Configuration d'un serveur de démarrage PXE sous SUSE Linux Enterprise Server 16.0

CONTENU

Configurez un serveur de démarrage PXE prenant en charge UEFI Secure Boot et le programme d'installation Agama.

MOTIF

Automatisez et rationalisez l'installation de plusieurs instances SUSE Linux Enterprise Server 16.0 sur le réseau.

EFFORT

Pour un administrateur de système ou de réseau, la lecture et la compréhension de cet article prennent généralement 30 à 45 minutes.

OBJECTIF

Disposer d'un serveur PXE fonctionnel qui peut démarrer plusieurs architectures dans le programme d'installation Agama.

CONDITIONS REQUISES

- Un système SUSE Linux Enterprise Server 16.0 doté de privilèges administratifs
- Une connexion Internet pour récupérer les images ISO
- Une configuration IP statique pour le serveur PXE

Date de publication : 11 déc 2025

Table des matières

1 Présentation du démarrage PXE avec SUSE Linux Enterprise Server 16.0

Le démarrage PXE permet aux machines de se lancer sur le réseau dans un environnement d'installation ou d'exécution sans stockage local. Cette section explique le fonctionnement de PXE dans le programme d'installation Agama de SUSE Linux Enterprise Server 16.0 et les images dynamiques de ce programme d'installation, en mettant l'accent sur GRUB 2.

1.1 Qu'est-ce que le démarrage PXE ?

PXE (Preboot Execution Environment) est une méthode qui permet aux systèmes de récupérer les chargeurs de démarrage et les programmes d'installation de système d'exploitation à partir d'un serveur réseau en utilisant DHCP et TFTP ou HTTP. Elle est largement utilisée pour provisionner des machines sans support physique ni système d'exploitation préinstallé.

1.2 Avantages du démarrage PXE

Le démarrage PXE simplifie l'approvisionnement en supprimant la nécessité d'un support d'installation local ou d'une configuration manuelle. Il offre les avantages suivants :

- Installation sans surveillance de nombreux systèmes sur le réseau
- Gestion centralisée des versions du programme d'installation et des configurations de démarrage
- Prise en charge de divers types d'architectures et de microprogrammes, y compris UEFI Secure Boot
- Sélection dynamique des programmes d'installation ou des paramètres d'installation à l'aide des menus GRUB 2

1.3 Fonctionnement du démarrage PXE dans SUSE Linux Enterprise Server 16.0

Le démarrage PXE dans SUSE Linux Enterprise Server 16.0 utilise GRUB 2 comme chargeur de démarrage et le programme d'installation Agama comme interface d'installation. Les chargeurs de démarrage et les fichiers du programme d'installation sont fournis sur le réseau à l'aide de HTTP ou TFTP, GRUB 2 récupérant le kernel Linux, l'unité RAM initiale (initrd) et l'image dynamique. Les clients PXE peuvent utiliser une variété de microprogrammes (notamment les plus courants tels que BIOS ou UEFI), d'exécutables de chargeur de démarrage ou de formats d'image, en fonction de leur architecture, par exemple AMD64/Intel 64, AArch64, ppc64le et s390x. En outre, ils doivent fonctionner à la fois sur les réseaux IPv4 et IPv6.

Le chargeur de démarrage transmet les paramètres du kernel Linux, tels que `root=live:`, pour charger le système de fichiers racine basé sur squashfs à partir d'une image ISO dynamique, en démarrant l'interface Agama soit localement, soit en tant que service Web pour une interface utilisateur Web distante.

1.3.1 Compatibilité avec les versions précédentes SLES 15.x

Les informations contenues dans cet article s'appliquent principalement à SUSE Linux Enterprise Server 16.0 et versions ultérieures. Il se concentre sur les flux de travail de démarrage PXE qui s'intègrent au programme d'installation Agama et s'appuient sur des images d'installation dynamiques. Dans le contexte et la portée de cet article, SLES 16.0 et les versions ultérieures diffèrent de SLES 15.x comme suit :

Programme d'installation

Utilise `dracut` et Agama au lieu de `linuxrc` et YaST.

Serveur DHCP

L'utilisation de DHCP ISC est abandonnée (fin de service 2022). Pour un serveur DHCP, utilisez plutôt Kea ou dnsmasq.

Paramètres de démarrage

Utilise le paramètre `root=live:` pour charger l'image du programme d'installation Agama et le paramètre facultatif `inst.install_url=` pour le dépôt d'installation non par défaut, au lieu du paramètre `install=`.

Le choix du chargeur de démarrage (GRUB 2, pxelinux, etc.) reste flexible et ne dépend pas de la version.

1.3.2 Différentes configurations et étapes possibles

Cet article présente les étapes de configuration obligatoires et les configurations facultatives ou alternatives. Ne suivez que les sections pertinentes pour votre déploiement et ignorez les alternatives qui ne s'appliquent pas à votre déploiement.

Obligatoire

Les tâches telles que l'installation des composants, la préparation de l'image du programme d'installation, la configuration de GRUB 2 et la validation du serveur doivent être effectuées dans toutes les configurations.

Méthode de distribution des fichiers

Un serveur HTTP (recommandé avec Agama) comme `nginx` et/ou un serveur TFTP comme `tftp` ou `dnsmasq`.

Serveur DHCP

Choisissez Kea ou dnsmasq.

Remarque : limites et caractéristiques de la méthode choisie

- Utilisez **Kea**, le nouveau serveur DHCP d'ISC, comme remplacement moderne de DHCP ISC. Pour plus d'informations sur Kea, reportez-vous au document https://www.isc.org/kea/. Pour l'avis de fin de service de DHCP ISC, reportez-vous au document https://www.isc.org/dhcp/. Kea est un serveur DHCP et nécessite un logiciel de serveur TFTP séparé. Le serveur DHCP Kea prend en charge les options de démarrage TFTP/PXE via IPv4 et IPv6 ainsi que le démarrage HTTP via IPv4. Le démarrage HTTP via IPv6 nécessite que le serveur DHCPv6 puisse renvoyer au client la valeur `Vendor Class Option` (voir `RFC3315, Section 22.16`), censée être utilisée « par un client pour identifier le fournisseur, » et n'est actuellement pas pris en charge.
- **dnsmasq** en tant que combinaison d'un serveur DNS, d'un serveur DHCP et d'un serveur TFTP. Vous pouvez l'utiliser pour servir le chargeur de démarrage, le kernel Linux, l'unité RAM initiale (et d'autres fichiers) via TFTP. Pour plus d'informations sur dnsmasq, reportez-vous au document https://thekelleys.org.uk/dnsmasq/doc.html. Le serveur DHCP dnsmasq prend en charge les options de démarrage TFTP/PXE via IPv4 et IPv6 ainsi que le démarrage HTTP via IPv4. Le démarrage HTTP via IPv6 nécessite que le serveur DHCPv6

puisse renvoyer au client la valeur `Vendor Class Option` (voir `RFC3315, Section 22.16`), censée être utilisée « par un client pour identifier le fournisseur, » et n'est actuellement pas pris en charge.

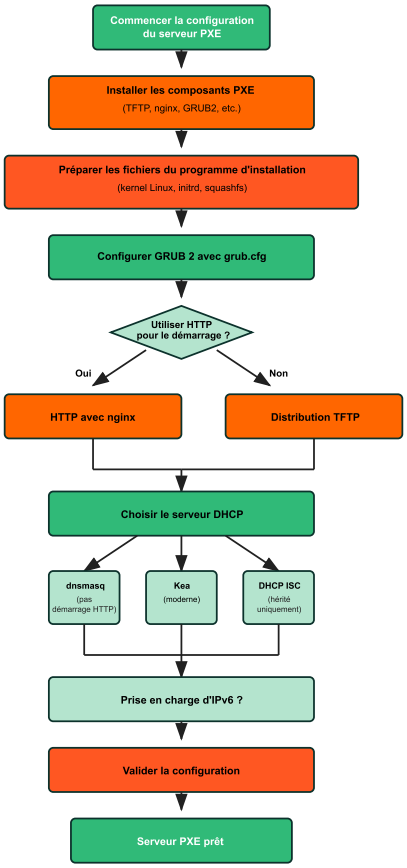

FIGURE 1 : EXEMPLE DE FLUX DE TRAVAIL POUR LA CONFIGURATION D'UN SERVEUR PXE

2 Préparation du réseau pour les services de démarrage PXE

Ce module décrit les exigences en matière d'infrastructure réseau pour le déploiement des services de démarrage PXE sur SUSE Linux Enterprise Server 16.0.

2.1 Introduction

Un serveur PXE comprend trois serveurs : un serveur DHCP qui fournit l'adresse et l'emplacement du fichier de démarrage (chargeur de démarrage) et un serveur TFTP et/ou HTTP pour récupérer les fichiers. En outre, il peut y avoir un serveur DNS, un serveur NTP et un routeur prenant en charge IPv6 ; ceux-ci sont généralement séparés du serveur PXE dans un réseau de production. Un serveur PXE exécutant SUSE Linux Enterprise Server 16.0 peut également nécessiter une configuration spécifique de l'interface réseau, l'ajout de certaines règles persistantes au pare-feu et certaines autorisations dans `SELinux`. Cette section présente un exemple de réseau avec des plages d'adresses IP appropriées et les règles nécessaires pour le pare-feu et SELinux.

2.2 Hypothèses et exemple de configuration du réseau

Dans cet article, nous partons des hypothèses suivantes :

- Le serveur PXE est en cours d'exécution sur l'interface réseau `eno1` avec la configuration réseau suivante :

  TABLEAU 1 : EXEMPLE DE CONFIGURATION DE RÉSEAU PXE

	IPv4	IPv6	Nom DNS
Réseau PXE	192.168.1.0/24	2001:db8:0:1::/64	example.net
Serveur PXE	192.168.1.200	2001:db8:0:1::200	pxe.example.net
Passerelle PXE	192.168.1.1	2001:db8:0:1::1	
Serveur DNS	192.168.1.200	2001:db8:0:1::200	
Serveur NTP	192.168.1.1	2001:db8:0:1::1	

- Par défaut, les serveurs routeur, NTP et DNS sont externes et s'exécutent sur une autre machine. Cet article fournit quelques conseils, mais ne couvre pas leur configuration complète.

2.3 Configuration de l'interface réseau, du pare-feu et de SELinux pour les services PXE

Configurez l'interface réseau et le pare-feu pour autoriser les services réseau requis par le serveur PXE. Ajustez les paramètres `SELinux` pour permettre les tests d'installation et définir des stratégies locales persistantes.

1. Vérifiez l'interface réseau PXE et assignez-la à la zone firewalld appropriée.
    a. Vérifiez les zones actuellement actives et les interfaces qui leur sont assignées :

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

    b. Si `eno1` n'est pas assigné à la zone `public`, faites-le :

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

    c. Faites en sorte que l'assignation de l'interface persiste après les redémarrages :

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

2. Configurez le pare-feu pour l'accès au service DNS.
    a. Autorisez le service DNS pour la session en cours :

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

    b. Rendez la modification permanente :

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

3. Configurez le pare-feu pour l'accès au service NTP.
    a. Autorisez le service NTP pour la session en cours :

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

    b. Rendez la modification permanente :

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

4. Configurez le pare-feu pour l'accès au service DHCP (IPv4).

a. Autorisez le service DHCP pour la session en cours :

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

b. Rendez la modification permanente :

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

5. Configurez le pare-feu pour l'accès au service DHCPv6.

a. Autorisez le service DHCPv6 pour la session en cours :

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

b. Rendez la modification permanente :

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

6. Configurez le pare-feu pour l'accès au service TFTP.

a. Autorisez le service TFTP pour la session en cours :

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

b. Rendez la modification permanente :

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

7. Configurez le pare-feu pour l'accès au service HTTP.

a. Autorisez le service HTTP pour la session en cours :

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

b. Rendez la modification permanente :

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

8. Configurez le pare-feu pour l'accès au service HTTPS.

a. Autorisez le service HTTPS pour la session en cours :

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

b. Rendez la modification permanente :

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

9. Désactivez temporairement SELinux pour les tests de configuration.

a. Définissez SELinux sur le mode permissif :

```
> sudo setenforce 0
```

b. Vérifiez le statut de SELinux :

```
> sudo sestatus
```

10. Générez et installez des modules de stratégie SELinux locaux pour les services liés à PXE.

a. Créez et installez un module pour nginx :

```
> sudo if test `ausearch -c 'nginx' --raw | wc -l` -gt 0 ; then
> sudo   ausearch -c 'nginx' --raw | audit2allow -a -M local-nginx
> sudo   semodule -i local-nginx.pp
> sudo fi
```

b. Créez et installez un module pour dnsmasq :

```
> sudo if test `ausearch -c 'dnsmasq' --raw | wc -l` -gt 0 ; then
> sudo   ausearch -c 'dnsmasq' --raw | audit2allow -a -M local-dnsmasq
> sudo   semodule -i local-dnsmasq.pp
> sudo fi
```

c. Créez et installez un module pour in.tftpd :

```
> sudo if test `ausearch -c 'in.tftpd' --raw | wc -l` -gt 0 ; then
> sudo   ausearch -c 'in.tftpd' --raw | audit2allow -a -M local-tftpd
> sudo   semodule -i local-tftpd.pp
```

```
> sudo fi
```

11. Réactivez le mode d'application de SELinux.

    a. Réglez SELinux sur le mode d'application :

    ```
    > sudo setenforce 1
    ```

    b. Vérifiez le statut de SELinux :

    ```
    > sudo sestatus
    ```

2.4 Résumé

Cette procédure a permis de s'assurer que l'interface réseau du serveur PXE, le pare-feu et la stratégie SELinux étaient correctement configurés pour un fonctionnement sûr et opérationnel.

- L'interface de service PXE (`eno1` dans cet exemple) a été vérifiée et assignée à la zone firewalld `public`.
- Les services de pare-feu requis pour le fonctionnement de PXE, notamment `dns`, `ntp`, `dhcp`, `dhcpv6`, `tftp`, `http`, et `https`, ont été ouverts.
- SELinux a été temporairement mis en mode `permissive` afin de faciliter les tests de service et d'enregistrer les refus AVC.
- Les commandes **`ausearch`** et **`audit2allow`** ont été utilisées pour générer et installer des modules de stratégie SELinux personnalisés pour des services tels que `nginx`, `dnsmasq` et `in.tftpd`.
- SELinux a été restauré en mode `enforcing` pour sécuriser le système en vue de son utilisation en production.

Une fois ces étapes terminées, le serveur PXE est configuré de manière sécurisée et prêt à servir des machines clientes sur le réseau en utilisant IPv4 ou IPv6.

3 Installation des composants requis pour le serveur PXE

Cette section explique comment installer les paquets nécessaires à la prise en charge du démarrage PXE dans SUSE Linux Enterprise Server 16.0, y compris les composants GRUB 2, DHCP, TFTP et/ou HTTP.

3.1 Introduction

Pour configurer un serveur de démarrage PXE sous SUSE Linux Enterprise Server 16.0, vous devez installer plusieurs services et outils. En fonction de votre configuration, vous pouvez avoir besoin des éléments suivants :

- Le paquet `dnsmasq` fournit une combinaison d'un serveur DNS, d'un serveur TFTP et d'un serveur DHCP (DHCPv4 et DHCPv6) avec une prise en charge limitée des annonces de routeur (RA) IPv6. Il fournit les éléments suivants :
  - Serveur DHCP dnsmasq : prend en charge la distribution conditionnelle d'options DHCP en fonction de la demande et de l'architecture du client pour :
    - les demandes de démarrage PXE à l'aide de DHCPv4 et DHCPv6 ;
    - les demandes de démarrage HTTP à l'aide de DHCPv4.

      

      ### Remarque : limites de dnsmasq pour le démarrage HTTP via DHCPv6

      À l'heure actuelle, dnsmasq ne prend pas en charge l'envoi de l'option DHCPv6 `vendor-class` requise.

  - Serveur TFTP dnsmasq : fournit les fichiers du chargeur de démarrage, le kernel Linux et l'unité RAM initiale via TFTP pendant le démarrage PXE.

- Serveur DNS dnsmasq : fournit une résolution récursive des noms de domaine et des adresses IP pour les micrologiciels clients et `/etc/resolv.conf` dans le programme d'installation/système d'exploitation.
- Annonces de routeur IPv6 dnsmasq : prennent en charge l'envoi d'annonces de routeur (RA) IPv6 lorsque le serveur PXE fait également office de routeur (configurabilité limitée à un « modèle RA commun »).

- Le paquet `kea` est un serveur DHCP et un successeur au serveur DHCP ISC. Il prend en charge la distribution conditionnelle d'options DHCP en fonction de la demande et de l'architecture du client pour :
  - les demandes de démarrage PXE à l'aide de DHCPv4 et DHCPv6 ;
  - les demandes de démarrage HTTP à l'aide de DHCPv4.

  

  ### Remarque : limites de Kea pour le démarrage HTTP via DHCPv6

  À l'heure actuelle, Kea ne prend pas en charge l'envoi de l'option DHCPv6 `vendor-class` requise. Pour plus d'informations, reportez-vous au document https://kea.readthedocs.io/en/latest/arm/dhcp6-srv.html#id4.

- Un serveur TFTP distribue les fichiers du chargeur de démarrage, le kernel Linux et l'unité RAM initiale via TFTP, tandis que le démarrage PXE avec Kea est fourni par le paquet `tftp` et n'est pas nécessaire pour le démarrage HTTP. Si vous utilisez `dnsmasq`, vous n'avez pas besoin du paquet `tftp`.
- Un serveur Web tel que le paquet `nginx` fournit les images du programme d'installation via HTTP.

Remarque : nécessité des serveurs HTTP

Un serveur HTTP/HTTPS comme nginx est presque toujours requis. Son utilisation s'étend au-delà du démarrage HTTP. En particulier, vous pouvez en avoir besoin dans les cas suivants :

- Il s'agit d'une exigence de base pour le démarrage HTTP.
- Il est recommandé pour la fourniture de `squashfs.img`. Vous pouvez utiliser `root=live:tftp://.../squashfs.img` dans la ligne de commande de démarrage.
- Il est également recommandé pour la fourniture de RPM à Agama dans le paramètre de ligne de commande de démarrage `inst.install_url=http://.../install/` sur un fichier `SLES-16.0-Full-*.inline.iso`, ainsi qu'avec des profils d'installation et d'autres fichiers pour une installation sans surveillance.

- Les paquets du chargeur d'amorçage GRUB 2 permettent le démarrage du réseau pour les architectures et les méthodes prises en charge. Par exemple, l'architecture AMD64/Intel 64 propose deux méthodes de démarrage du réseau : BIOS et UEFI. En outre, UEFI prend généralement en charge le démarrage PXE (TFTP) et HTTP. D'autres chargeurs de démarrage, tels que pxelinux, ne prennent pas en charge UEFI et le démarrage HTTP.
- Un daemon d'annonce de routeur pour IPv6, tel que le paquet `radvd`, peut éventuellement être fourni. Il est nécessaire sous SLES s'il sert également de routeur pour un réseau de programme d'installation afin d'effectuer les tâches suivantes :
  - Configurer le routage sur un réseau pour les clients de démarrage PXE ou HTTP.
  - Activer l'utilisation de DHCPv6 sur un réseau pour les clients de démarrage PXE ou HTTP.

3.2 Configuration requise

- Un système exécutant SUSE Linux Enterprise Server 16.0 avec des privilèges administratifs, enregistré auprès du SUSE Customer Center et configuré avec un accès aux dépôts en ligne appropriés à l'aide de SUSEConnect.
- Des modules SLE activés : module Server Applications, module Legacy et module Base System.
- Un accès aux dépôts de modules SLE pour les services de réseau et les chargeurs de démarrage.
- Une connexion Internet opérationnelle pour récupérer les paquets.

3.3 Installation des paquets

Procédez comme suit pour installer les paquets de base nécessaires au serveur de démarrage PXE.

PROCÉDURE 1 : INSTALLATION DES PAQUETS NÉCESSAIRES POUR UN SERVEUR DE DÉMARRAGE PXE

1. Installez le chargeur de démarrage GRUB 2 et le serveur HTTP nginx en tant qu'exigences communes.

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

2. Exécutez l'une des commandes suivantes pour installer les paquets essentiels à votre approche :

   - `kea` pour le serveur DHCP, `tftp` pour le serveur TFTP

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

   - `dnsmasq` en tant que fournisseur commun pour les serveurs DHCP, DNS et TFTP

```
> sudo zypper install dnsmasq
```

Remarque : limites des serveurs DHCP fournis par Kea et dnsmasq

Le démarrage HTTP via IPv6 n'est *actuellement* pas pris en charge par les serveurs DHCP fournis par les paquets `kea` et `dnsmasq`. Il ne permet pas de renvoyer l'option `vendor-class` au client HTTP, comme l'exige la spécification UEFI.

3. Vous pouvez éventuellement installer des cibles GRUB 2 supplémentaires spécifiques à l'architecture si vous prévoyez de prendre en charge d'autres plates-formes.

   - Pour l'architecture AMD64/Intel 64 :

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

   - Pour l'architecture AArch64 :

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

   - Pour l'architecture ppc64le :

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

   

   ### Remarque : mode de fourniture de paquets GRUB 2 par le serveur PXE à des clients dont l'architecture est différente de celle de la machine serveur

   Les paquets `noarch.rpm` spécifiques à l'architecture de GRUB 2 sont inclus dans le sous-répertoire `noarch` du média/dépôt d'installation, quelle que soit l'architecture de la machine sur laquelle le serveur PXE est configuré. En d'autres termes, vous pouvez installer les paquets `grub2-arm64-efi` et `grub2-powerpc-ieee1275` sur un serveur PXE s'exécutant sur une machine AMD64/Intel 64, afin de prendre en charge les clients dotés d'autres architectures.

4. Vous pouvez éventuellement installer le paquet `shim` si vous avez besoin du mode UEFI Secure Boot pour AMD64/Intel 64 ou AArch64, mais que vous ne souhaitez pas utiliser les fichiers de l'image ISO du support d'installation.

   ```
   > sudo zypper install shim
   ```

5. Vous pouvez éventuellement installer le daemon d'annonce de routeur `radvd` si vous souhaitez utiliser le serveur PXE comme routeur (non recommandé pour les réseaux de production).

   ```
   > sudo zypper install radvd
   ```

6. Installez l'utilitaire `rsync` pour copier ou synchroniser facilement l'image ISO et l'arborescence Annuaire.

```
> sudo zypper install rsync
```

7. Assurez-vous que les services sont installés, mais qu'ils n'ont pas encore démarré. La configuration sera abordée dans des sections ultérieures.

4 Création des répertoires NetBoot de GRUB 2 pour le serveur PXE

Cette section décrit comment créer des répertoires NetBoot de GRUB 2 pour les serveurs PXE à l'aide de **`grub2-mknetdir`**, qui génère des répertoires spécifiques à l'architecture pour les systèmes AMD64/Intel 64 (UEFI et BIOS), AArch64 et ppc64le. Pour la prise en charge du mode UEFI Secure Boot, les administrateurs doivent copier les fichiers EFI signés à partir du support d'installation ou utiliser le paquet `shim` pour remplacer les fichiers par défaut non signés du chargeur de démarrage.

4.1 Introduction

Cette section décrit comment configurer les répertoires NetBoot de GRUB 2 pour le déploiement d'un serveur PXE sur plusieurs architectures. La commande **`grub2-mknetdir`** crée des répertoires spécifiques à l'architecture sous `/srv/tftpboot/boot/grub2/` pour différentes plateformes. Par exemple, les systèmes AMD64/Intel 64 génèrent à la fois des répertoires UEFI (`x86_64-efi`) et du BIOS hérité (`i386-pc`), tandis que les systèmes AArch64 et ppc64le créent leurs répertoires UEFI respectifs (`arm64-efi` et `powerpc-ieee1275`).

Pour la prise en charge du mode UEFI Secure Boot, qui n'est pas assurée par les fichiers `core.efi` par défaut non signés, les administrateurs peuvent soit copier des fichiers EFI signés à partir du support d'installation, soit installer le paquet `shim` et copier manuellement les fichiers de chargeur de démarrage requis (`shim.efi`, `grub.efi`, `MokManager.efi`) dans les répertoires d'architecture appropriés, en veillant à une résolution correcte des liens symboliques afin de conserver tous les fichiers dans le répertoire racine TFTP.

4.2 Configuration requise

- Assurez-vous d'avoir installé les paquets suivants : `grub2`, `tftp` et tout autre paquet GRUB 2 spécifique à l'architecture, tel que `grub2-x86_64-efi` et `grub2-i386-pc`.
- Assurez-vous que le support d'installation (ISO) est disponible pour le montage ou que le paquet `shim` est installé sur le système. Vous pouvez télécharger le support d'installation (ISO) pour votre architecture cible à partir du SUSE Customer Center.

4.3 Préparation des répertoires NetBoot et du mode UEFI Secure Boot

Cette procédure crée la structure de répertoire GRUB 2 requise pour le démarrage réseau PXE et configure éventuellement la prise en charge du mode UEFI Secure Boot sur plusieurs architectures.

1. Créez une structure de répertoire NetBoot de GRUB 2.

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

   Cela crée des répertoires spécifiques à l'architecture :

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

   

   Avertissement

   N'écrasez pas manuellement le fichier `grub.cfg` créé par **`grub2-mknetdir`**.

2. Copiez sur le serveur TFTP les autres répertoires indépendants de l'architecture, tels que `fonts/` et `locale/`, qui sont disponibles sous le répertoire `/srv/tftpboot/boot/grub2/`.

3. Vous pouvez également utiliser le fichier `/srv/tftpboot/boot/grub2/ARCH-efi/core.efi` installé par la commande **`grub2-mknetdir`** pour les architectures AMD64/Intel 64 ou AArch64 pour UEFI PXE. Cependant, ils ne sont *pas signés* et ne prennent pas en charge UEFI Secure Boot. Pour activer éventuellement UEFI Secure Boot pour les architectures AMD64/Intel 64 et AArch64 prises en charge, effectuez l'une des étapes suivantes :

   - Copiez les fichiers nécessaires à partir de l'image ISO du support d'installation :

     a. Montez l'image ISO.

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

     b. Copiez les fichiers EFI.

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

     (1) Remplacez *ARCH*`-efi` par `x86_64-efi` ou `arm64-efi`, les architectures prises en charge pour UEFI Secure Boot.

     c. Testez l'image ISO du support d'installation.

     ```
     > sudo umount /mnt
     ```

   - Utilisez le paquet `shim` si vous ne souhaitez pas utiliser les fichiers de l'image ISO du support d'installation :

     a. Si ce n'est déjà fait, installez le paquet `shim`.

     ```
     > sudo zypper install shim
     ```

     b. Copiez les fichiers signés du chargeur de démarrage pour l'architecture requise :

        i. Copiez le fichier `shim.efi`.

           - Pour l'architecture AMD64/Intel 64 :

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

- Pour l'architecture AArch64 :

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

ii. Copiez le fichier `grub.efi`.

- Pour l'architecture AMD64/Intel 64 :

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

- Pour l'architecture AArch64 :

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

iii. Copiez le fichier `MokManager.efi`.

- Pour l'architecture AMD64/Intel 64 :

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

- Pour l'architecture AArch64 :

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

Remarque

L'indicateur `-L` résout les liens symboliques pour s'assurer que les fichiers restent à la racine TFTP.

5 Préparation du contenu de l'image du programme d'installation

Cette section décrit comment extraire les fichiers du programme d'installation à partir du support d'installation de SUSE Linux Enterprise Server 16.0 et comment les organiser pour les environnements de démarrage PXE. Il couvre à la fois les images `.install.iso` et les paquets RPM, avec des instructions spécifiques pour différents types d'installation et architectures.

5.1 Introduction

SUSE Linux Enterprise Server 16.0 fournit des fichiers de programme d'installation dans plusieurs formats afin de prendre en charge différents scénarios de démarrage PXE. Le programme d'installation Agama nécessite trois fichiers essentiels : l'image du kernel Linux (`linux`), l'unité RAM initiale (`initrd`) et le système de fichiers racine compressé (`squashfs.img`). Ces fichiers doivent être extraits à partir du support d'installation et organisés dans une structure de répertoires accessible via TFTP et HTTP.

Cette section couvre les méthodes de préparation à la fois des images `.install.iso` et des paquets RPM, afin d'assurer la compatibilité avec les différents types d'installation et architectures pris en charge par SUSE Linux Enterprise Server 16.0.

5.2 Configuration requise

- Support d'installation de SUSE Linux Enterprise Server 16.0 tel que disponible dans le SUSE Customer Center. Choix possibles :
  - Image ISO en ligne : programme d'installation uniquement pour les installations réseau (`SLES-16.0-Online-`*`ARCH-BUILD`*`.install.iso`)
  - Image ISO complète : programme d'installation avec dépôt d'installation (`SLES-16.0-Full-`*`ARCH-BUILD`*`.install.iso`)
  - Paquets RPM : `tftpboot-agama-installer-SUSE_SLE_16_PXE-`*`ARCH`*
- Un point de montage temporaire, tel que `/mnt`.

- Espace disque suffisant sous `/srv/tftpboot` et `/srv/install` pour la méthode d'installation choisie.
- Privilèges administratifs permettant de créer des répertoires et de copier des fichiers.

5.3 Préparation des fichiers du programme d'installation à partir d'images ISO

Les images ISO constituent une méthode simple pour extraire les fichiers du programme d'installation. Les procédures suivantes couvrent à la fois les types Image ISO en ligne et Image ISO complète pour différentes architectures.

5.3.1 Utilisation d'images ISO en ligne

Les images ISO en ligne ne contiennent que les composants du programme d'installation, ce qui nécessite un accès réseau aux dépôts d'installation lors de l'installation du système. Cela correspond à l'entrée du menu de démarrage `SLES-16.0 Online Installation` dans GRUB.

PROCÉDURE 2 : EXTRACTION DE FICHIERS À PARTIR D'UNE IMAGE ISO EN LIGNE (X86_64 ET AARCH64)

1. Créez la structure de répertoires pour les fichiers du programme d'installation :

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

2. Montez l'images ISO en ligne :

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

3. Copiez les fichiers du kernel Linux et initrd :

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

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

4. Copiez le système de fichiers racine compressé :

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

5. Montez l'image ISO :

```
> sudo umount /mnt
```

PROCÉDURE 3 : EXTRACTION DE FICHIERS À PARTIR D'UNE IMAGE ISO EN LIGNE (PPC64LE)

1. Créez la structure de répertoire :

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

2. Montez l'image ISO :

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

3. Copiez les fichiers du kernel Linux et initrd (notez la structure de chemin différente pour ppc64le) :

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

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

4. Copiez le système de fichiers racine compressé :

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

5. Montez l'image ISO :

```
> sudo umount /mnt
```

5.3.2 Utilisation d'images ISO complètes

Les images ISO complètes comprennent à la fois le programme d'installation et les dépôts d'installation, ce qui permet des installations locales sans dépendances réseau externes. Cela correspond à l'entrée du menu de démarrage `SLES-16.0 Local Installation` dans GRUB avec le paramètre supplémentaire `inst.install_url=http://pxe.example.net/install/SLES-16.0/${arch}`.

PROCÉDURE 4 : EXTRACTION DE FICHIERS À PARTIR D'UNE IMAGE ISO COMPLÈTE

1. Créez des répertoires à la fois pour les fichiers du programme d'installation et pour le dépôt d'installation :

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

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

2. Montez l'image ISO complète :

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

3. Copiez les fichiers du kernel Linux et initrd (ajustez les chemins pour ppc64le comme indiqué dans les procédures précédentes) :

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

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

4. Copiez le système de fichiers racine compressé :

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

5. Copier le dépôt d'installation pour l'accès au serveur HTTP local :

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

6. Montez l'image ISO :

```
> sudo umount /mnt
```

5.4 Préparation des fichiers du programme d'installation à partir de paquets RPM

Les paquets RPM constituent une méthode alternative pour obtenir les fichiers du programme d'installation en ligne.

PROCÉDURE 5 : INSTALLATION ET UTILISATION DES PAQUETS RPM TFTPBOOT

1. Installez les paquets requis :

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

2. Copiez les fichiers linux, initrd et squashfs.img dans tftpboot :

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

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

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

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

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

5.5 Structure de répertoires recommandée

Organisez les fichiers extraits selon la disposition de répertoires suivante afin de garantir la cohérence et la facilité de maintenance. Cette structure prend en charge plusieurs types d'installation et architectures.

EXEMPLE 1 : DISPOSITION COMPLÈTE DES RÉPERTOIRES DU SERVEUR PXE

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

❶ Image du kernel Linux extraite du support d'installation

2. Image de l'unité RAM initiale
3. Système de fichiers racine compressé pour le programme d'installation Agama
4. Dépôt d'installation à partir du répertoire `install` de l'image ISO complète (facultatif)

5.6 Vérification de l'installation

Après avoir extrait et organisé les fichiers du programme d'installation, vérifiez que tous les composants requis sont présents et accessibles.

PROCÉDURE 6 : ÉTAPES DE VÉRIFICATION

1. Vérifiez que les fichiers essentiels sont présents :

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

2. Veillez à ce que les autorisations d'accès aux fichiers soient correctes :

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

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

Important : accessibilité des fichiers

Assurez-vous que tous les fichiers extraits sont lisibles par les services TFTP et HTTP. Les clients PXE accéderont aux fichiers au cours du processus de démarrage. Il est donc essentiel de disposer d'autorisations et d'une configuration de service adéquates pour que les déploiements réussissent.

5.7 Étapes suivantes

Une fois les fichiers du programme d'installation correctement préparés et organisés, vous pouvez poursuivre avec les tâches suivantes :

- Configurer GRUB 2 pour le démarrage PXE avec des entrées de menu faisant référence à ces fichiers
- Configurer les services HTTP et TFTP pour desservir le contenu extrait
- Configurer DHCP pour diriger les clients PXE vers les chargeurs de démarrage appropriés

Les fichiers extraits seront référencés dans la configuration GRUB 2 à l'aide de chemins tels que `root=live:http://pxe.example.net/boot/images/SLES-16.0/ARCH/squashfs.img`.

6 Configuration de GRUB 2 pour le démarrage PXE

Cette section décrit comment configurer le chargeur de démarrage GRUB 2 pour un démarrage basé sur PXE sous SUSE Linux Enterprise Server 16.0. Elle couvre la création de la structure de répertoires de démarrage du réseau, la configuration de chargeurs de démarrage spécifiques à l'architecture et l'implémentation d'un système de configuration flexible qui prend en charge plusieurs architectures et scénarios d'installation.

6.1 Introduction

GRUB 2 fait office de chargeur de démarrage réseau pour les clients PXE, en chargeant les fichiers du noyau Linux et initrd pour lancer le programme d'installation Agama. Cette section montre comment créer une configuration GRUB 2 sophistiquée qui détecte automatiquement l'architecture du client, gère la sélection de l'interface réseau et fournit un menu de démarrage unifié prenant en charge plusieurs types d'installation et architectures cibles.

L'approche de la configuration utilise une conception modulaire avec des fichiers séparés pour la détection de l'architecture, les définitions de variables et les entrées du menu de démarrage. Cela permet de prendre en charge des configurations spécifiques aux machines et des profils d'installation automatisés, tout en maintenant la cohérence entre les différentes plates-formes matérielles.

6.2 Configuration requise

- Assurez-vous que la structure du répertoire de démarrage du réseau GRUB 2 est en place, comme décrit dans les sections précédentes.
- Assurez-vous que les fichiers du programme d'installation sont correctement organisés comme décrit dans les sections précédentes.

- Les paquets GRUB 2 pour toutes les architectures cibles doivent être installés : `grub2-x86_64-efi`, `grub2-i386-pc`, `grub2-aarch64-efi` et `grub2-ppc64le-ieee1275`.
- Le paquet `shim` pour la prise en charge du mode UEFI Secure Boot (facultatif).
- Un accès administratif à `/srv/tftpboot` ou à la racine PXE équivalente.

6.3 Création de la configuration GRUB 2

Le fichier de configuration GRUB 2 gère trois tâches principales : la détection de l'architecture du client, la gestion des interfaces réseau et le chargement d'autres fichiers de configuration. Cette approche modulaire permet de s'adapter à différents scénarios de déploiement.

PROCÉDURE 7 : CONFIGURATION DU PRINCIPAL FICHIER `grub.cfg`

- Créez le fichier de configuration GRUB 2 principal à l'emplacement `/srv/tftpboot/boot/grub2/grub.cfg` :

```
> sudo cat > /srv/tftpboot/boot/grub2/grub.cfg << 'EOF'
# Architecture detection and mapping
if [ "$grub_cpu" == "i386" ]; then
  set arch='x86_64'
elif [ "$grub_cpu" == "x86_64" ]; then
  set arch='x86_64'
elif [ "$grub_cpu" == "arm64" ]; then
  set arch='aarch64'
elif [ "$grub_cpu" == "powerpc" ]; then
  set arch='ppc64le'
fi

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


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

```
set ifcfg="ifcfg=${net_default_mac}=dhcp"
export ifcfg

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

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

ÉLÉMENTS CLÉS DE LA CONFIGURATION

Détection de l'architecture

Associe les types de processeur de GRUB 2 aux architectures de distribution, ce qui permet de créer des entrées de menu unifiées fonctionnant sur différentes plates-formes matérielles.

Gestion de l'interface réseau

Définit une variable `${ipcfg}` utilisant la variable grub2 `${net_default_mac}` pour activer DHCP uniquement sur l'interface de démarrage PXE nommée `pxe0`, évitant ainsi les problèmes de sondage du réseau sur les systèmes multi-interfaces.

Définitions des utilitaires

Définit une variable type `${sconsole}` avec des paramètres de console série.

Configuration spécifique à la machine

Charge les fichiers de configuration facultatifs par machine en fonction de l'adresse MAC, ce qui permet de personnaliser les paramètres de démarrage par machine et d'automatiser les profils d'installation.

6.4 Création du menu de démarrage unifié

Le menu de démarrage utilise les variables de la configuration principale pour fournir des entrées de menu indépendantes de l'architecture qui s'adaptent automatiquement aux différentes plates-formes matérielles et aux différents types d'installation.

PROCÉDURE 8 : CONFIGURATION DU FICHIER MENU.CFG

- Créez un menu de démarrage unifié dans `/srv/tftpboot/boot/grub2/menu.cfg` :

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

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

Remarque : flexibilité de l'entrée de menu

Les entrées de menu utilisent des variables qui sont automatiquement remplies en fonction de l'architecture et de la configuration du client. La variable `${arch}` permet de s'assurer que les bons fichiers sont chargés.

La variable facultative `${ipcfg}` permet de configurer uniquement l'interface réseau sélectionnée par PXE.

La variable facultative `${sconsole}` permet d'activer une console série sur le système du programme d'installation.

6.5 Configurations spécifiques à la machine

Pour les déploiements avancés, vous pouvez créer des fichiers de configuration spécifiques à la machine qui remplacent les paramètres par défaut ou fournissent des paramètres d'installation automatisés.

PROCÉDURE 9 : CRÉATION D'UNE CONFIGURATION SPÉCIFIQUE À LA MACHINE

1. Créez un répertoire pour les configurations spécifiques à la machine :

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

2. Pour une machine avec une adresse MAC `aa:bb:cc:dd:ee:ff`, créez une configuration spécifique :

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

3. Créez le fichier `grub.cfg` spécifique à la machine :

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

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

# Use know predictable network interface name
set ipcfg="ip=eno1:dhcp"

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

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

Vous pouvez éventuellement fournir une entrée de menu propre dans le fichier `grub.cfg` spécifique à l'hôte (par exemple, généré pour une tentative de démarrage spécifique) :

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

menuentry 'SLES-16.0 Auto-Installation' {
  linux  /boot/images/SLES-16.0/${arch}/linux showopts root=live:http://
pxe.example.net/boot/images/SLES-16.0/${arch}/squashfs.img inst.install_url=http://
pxe.example.net/install/SLES-16.0/${arch} inst.auto=http://pxe.example.net/install/
profiles/${net_default_mac}/sles16.json ip=eno1:dhcp
  initrd /boot/images/SLES-16.0/${arch}/initrd
}
EOF
```

EXEMPLE 2 : PARAMÈTRES COURANTS SPÉCIFIQUES À LA MACHINE

`default`
: Spécifie l'entrée de menu pour démarrer automatiquement.

`timeout`
: Définit le timeout de démarrage en secondes.

`ipcfg`
: Remplace la configuration de l'interface réseau pour un matériel spécifique.

`autoinstall`
: Fournit des URL de profil d'installation automatisé spécifiques à la machine

6.6 Vérification de la configuration GRUB 2

Après avoir créé les fichiers de configuration, vérifiez que la configuration est correcte et que tous les fichiers requis sont en place.

PROCÉDURE 10 : ÉTAPES DE VÉRIFICATION

1. Vérifiez la structure de répertoires GRUB 2 :

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

2. Vérifiez la syntaxe du fichier de configuration en la testant à l'aide des outils GRUB 2 :

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

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

3. Veillez à ce que les autorisations d'accès aux fichiers soient correctes :

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

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

Important : test de la configuration

Testez la configuration GRUB 2 avec des clients PXE réels pour vous assurer de la détection de l'architecture et le menu fonctionnent correctement. La variable `${net_default_mac}` n'est disponible que dans les scénarios de démarrage réseau réels.

6.7 Dépannage de la configuration GRUB 2

Problèmes courants et leurs solutions lors de l'utilisation de configurations PXE GRUB 2. Chaque problème comprend des étapes de diagnostic et des commandes spécifiques pour résoudre le problème.

6.7.1 Échec de la détection de l'architecture

Lorsque GRUB 2 ne détecte pas l'architecture correcte, les clients risquent de démarrer avec des fichiers binaires incorrects ou de ne rien pouvoir charger.

PROCÉDURE 11 : DÉBOGAGE DE LA DÉTECTION DE L'ARCHITECTURE

1. Ajoutez une sortie de débogage à la configuration GRUB 2 pour afficher les valeurs détectées :

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

2. Testez la syntaxe de la configuration :

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

3. Si l'assignation de l'architecture est incomplète, étendez la logique de détection :

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

4. Vérifiez que les répertoires spécifiques à l'architecture existent :

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

6.7.2 Interface réseau introuvable

Certaines implémentations de microprogrammes peuvent ne pas définir correctement la variable `${net_default_mac}`, ce qui entraîne des échecs de configuration du réseau.

PROCÉDURE 12 : DIAGNOSTIC DES PROBLÈMES LIÉS À L'INTERFACE RÉSEAU

1. Ajoutez une sortie de débogage pour vérifier les variables réseau :

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

2. Créez une configuration réseau de secours :

```
> sudo cat >> /srv/tftpboot/boot/grub2/grub.cfg << 'EOF'

# Fallback network configuration if net_default_mac is empty
if [ "X${net_default_mac}" == "X" ]; then
  set ipcfg="ip=dhcp"
  set ifcfg="ifcfg=*=dhcp"
  echo "WARNING: Using fallback network configuration"
  sleep 2
fi
EOF
```

3. Testez la configuration réseau avec une interface spécifique :

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

4. Vérifiez les noms des interfaces réseau sur le système cible :

```
> ip link show
```

6.7.3 Chemins d'accès aux fichiers introuvables

Des chemins d'accès incorrects empêchent GRUB 2 de charger les fichiers de kernel Linux et initrd, ce qui provoque des échecs de démarrage.

PROCÉDURE 13 : VÉRIFICATION DE L'ACCESSIBILITÉ DES CHEMINS DES FICHIERS

1. Vérifiez si les fichiers du programme d'installation existent aux emplacements prévus :

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

2. Vérifiez l'accès TFTP aux fichiers de démarrage :

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

3. Testez l'accès HTTP aux fichiers du programme d'installation :

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

4. Vérifiez les autorisations et la propriété des fichiers :

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

5. Corrigez les autorisations si nécessaire :

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

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

6. Vérifiez que les liens symboliques ne sont pas rompus :

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

6.7.4 Échecs des démarrages EFI

Des problèmes liés à EFI et Secure Boot peuvent empêcher l'initialisation correcte du chargeur de démarrage ou provoquer des échecs d'authentification.

PROCÉDURE 14 : DIAGNOSTIC DES PROBLÈMES LIÉS AU DÉMARRAGE EFI

1. Vérifiez que les fichiers Secure Boot sont présents :

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

2. Vérifiez que les fichiers shim (bootx64.efi ou shim.efi), grub.efi et MokManager.efi sont correctement copiés :

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

3. Vérifiez l'intégrité du fichier EFI :

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

4. Testez si les fichiers sont accessibles via TFTP :

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

5. Pour les systèmes aarch64, vérifiez les fichiers EFI ARM64 :

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

6. Vérifiez que la configuration DHCP fournit les bons chemins d'accès au chargeur de démarrage :

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

7. Si des fichiers sont manquants, recopiez-les à partir de l'image ISO montée dans /mnt ou à partir des fichiers du paquet shim :

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

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

6.7.5 Non-chargement des entrées de menu

Lorsque GRUB 2 se charge, mais que les entrées de menu échouent ou affichent des erreurs, le problème est souvent lié à l'expansion des variables ou aux références de fichiers.

PROCÉDURE 15 : DÉBOGAGE DES PROBLÈMES LIÉS AUX ENTRÉES DE MENU

1. Testez la syntaxe de la configuration de menu :

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

2. Ajoutez une sortie de débogage aux entrées de menu :

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

3. Vérifiez que l'expansion des variables fonctionne correctement :

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

4. Effectuez un test avec une entrée de menu simplifiée :

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

5. Chargez temporairement le menu de test :

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

6. Restaurez le menu d'origine après le test :

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

6.7.6 Activation de la journalisation détaillée

Pour les problèmes persistants, activez la journalisation complète afin de capturer des informations détaillées sur le processus de démarrage.

PROCÉDURE 16 : CONFIGURATION DE LA JOURNALISATION DE DÉBOGAGE DE GRUB 2

1. Créez une version de débogage de la configuration principale :

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

2. Ajoutez une sortie de débogage complète :

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

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

3. Incluez la configuration de débogage dans le fichier principal :

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

4. Surveillez les journaux TFTP pendant les tentatives de démarrage :

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

5. Surveillez les journaux DHCP pour les requêtes PXE :

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

6. Désactivez le mode de débogage après le dépannage :

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

6.8 Étapes suivantes

Une fois GRUB 2 correctement configuré, vous pouvez passer aux tâches suivantes :

- Configurer les services HTTP et TFTP pour desservir les fichiers de démarrage et le contenu du programme d'installation.
- Configurer les services DHCP pour diriger les clients PXE vers les chargeurs de démarrage appropriés.
- Tester le processus complet de démarrage PXE sur le matériel cible.

Le système de configuration flexible GRUB 2 fournit une base pour des scénarios de déploiement PXE sophistiqués, prenant en charge de multiples architectures et types d'installation par le biais d'une interface unifiée.

7 Configuration de TFTP pour le démarrage PXE

Cette section explique comment configurer les services TFTP pour desservir les chargeurs de démarrage GRUB 2 et le contenu de démarrage PXE pour les installations SUSE Linux Enterprise Server 16.0. Elle couvre le serveur traditionnel `in.tftpd` et la fonctionnalité TFTP intégrée fournie par `dnsmasq`.

7.1 Introduction

TFTP fournit des fichiers de chargeur de démarrage aux clients PXE pendant le processus de démarrage du réseau. SUSE Linux Enterprise Server 16.0 prend en charge deux implémentations de serveur TFTP : le serveur traditionnel `in.tftpd` du paquet `tftp` et la fonctionnalité TFTP intégrée dans `dnsmasq`.

7.2 Configuration requise

- Le paquet `tftp` ou le paquet `dnsmasq` est installé.
- Les fichiers de démarrage PXE sont organisés sous `/srv/tftpboot`.
- Des privilèges administratifs sont disponibles pour configurer les services.

7.3 Configuration du serveur in.tftpd

Le serveur `in.tftpd` utilise le fichier de configuration `/etc/sysconfig/tftp` pour définir le répertoire racine TFTP et les options du serveur.

PROCÉDURE 17 : CONFIGURATION DU SERVEUR TFTP IN.TFTPD

1. Vous pouvez éventuellement activer la journalisation verbeuse en définissant les options TFTP :

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

   L'option `-v` active la journalisation verbeuse afin de consigner les noms des fichiers récupérés via TFTP.

2. Activez et démarrez le service TFTP :

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

7.4 Configuration du serveur TFTP dnsmasq

`dnsmasq` fournit un serveur TFTP intégré qui peut être activé et configuré pour utiliser le répertoire `/srv/tftpboot`.

PROCÉDURE 18 : CONFIGURATION DE LA FONCTIONNALITÉ TFTP DE DNSMASQ

1. Créez le fichier de configuration TFTP :

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

2. Activez et démarrez le service dnsmasq :

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

7.5 Vérification de la configuration TFTP

Testez la fonctionnalité du serveur TFTP pour vous assurer qu'il peut fournir des fichiers aux clients PXE.

PROCÉDURE 19 : TEST DE LA FONCTIONNALITÉ DU SERVEUR TFTP

1. Créez un fichier de test :

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

2. Récupérez le fichier de test via TFTP :

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

3. Vérifiez que le fichier a bien été récupéré :

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

4. Nettoyez les fichiers de test :

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

7.6 Dépannage de la configuration TFTP

Problèmes courants lors de la configuration des services TFTP pour les environnements de démarrage PXE.

7.6.1 Conflits de services sur le port 69

`in.tftpd` et `dnsmasq` utilisent tous deux le port UDP 69 pour les services TFTP et ne peuvent pas s'exécuter simultanément.

PROCÉDURE 20 : RÉSOLUTION DES CONFLITS DE SERVICES TFTP

1. Vérifiez quels sont les services en cours d'exécution :

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

2. Vérifiez ce qui utilise le port 69 :

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

3. Arrêtez le service en conflit (exemple pour dnsmasq) :

```
> sudo systemctl stop dnsmasq
```

4. Démarrez votre service TFTP préféré :

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

7.6.2 Problèmes liés au répertoire TFTP

Des problèmes d'accès au répertoire racine TFTP peuvent empêcher la distribution des fichiers.

PROCÉDURE 21 : VÉRIFICATION DE LA CONFIGURATION DU RÉPERTOIRE TFTP

1. Vérifiez la configuration du répertoire TFTP pour in.tftpd :

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

2. Vérifiez la configuration du répertoire TFTP pour dnsmasq :

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

3. Vérifiez si le répertoire existe :

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

4. S'il est manquant, créez le répertoire :

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

7.6.3 Activation de la journalisation TFTP

La journalisation verbeuse permet d'identifier les problèmes d'accès aux fichiers lors des transferts TFTP.

PROCÉDURE 22 : ACTIVATION DE LA JOURNALISATION TFTP VERBEUSE

1. Vérifiez les options TFTP actuelles :

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

2. Activez la journalisation verbeuse :

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

3. Redémarrez le service TFTP :

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

4. Surveillez les journaux TFTP :

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

7.7 Étapes suivantes

Une fois TFTP configuré, vous pouvez passer à la configuration des services HTTP pour desservir les fichiers du programme d'installation et les services DHCP de manière à diriger les clients PXE vers les chargeurs de démarrage appropriés.

8 Configuration de nginx pour la distribution HTTP

Cette section explique comment configurer nginx pour qu'il desserve le contenu du démarrage PXE via HTTP, de manière à permettre aux clients de charger des fichiers du programme d'installation, tels que les images du kernel Linux, initrd et squashfs, à partir d'un emplacement central. La distribution HTTP offre de meilleures performances que TFTP pour les fichiers volumineux et est requise pour les installations de SUSE Linux Enterprise Server 16.0 à l'aide d'Agama.

8.1 Introduction

nginx sert de serveur HTTP pour les environnements de démarrage PXE et permet d'accéder aux fichiers du programme d'installation par le biais d'une distribution basée sur le Web. Le serveur HTTP expose le répertoire de démarrage TFTP et les dépôts d'installation, ce qui permet aux clients PXE de télécharger les images du kernel Linux, les fichiers initrd et les composants du programme d'installation Agama via HTTP plutôt que via le protocole TFTP, qui est plus lent.

8.2 Configuration requise

- Le paquet `nginx` est installé.
- Les fichiers de démarrage PXE sont organisés sous `/srv/tftpboot/boot`.
- Les dépôts d'installation sont disponibles sous `/srv/install`.
- Des privilèges administratifs sont disponibles pour modifier la configuration nginx.

8.3 Configuration de nginx pour le démarrage PXE

La configuration de nginx définit des alias d'emplacement qui exposent le répertoire de démarrage TFTP et les dépôts d'installation par le biais d'URL HTTP.

PROCÉDURE 23 : CONFIGURATION DU SERVEUR HTTP NGINX

1. Éditez le fichier de configuration nginx :

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

2. Configurez le bloc du serveur HTTP dans la section `http` :

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

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

    charset             utf-8;
    sendfile            on;
    keepalive_timeout   65;
```

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

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

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

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

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

events {
    worker_connections  1024;
}
EOF
```

3. Testez la syntaxe de la configuration nginx :

```
> sudo nginx -t
```

4. Activez et démarrez le service nginx :

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

8.4 Vérification de la configuration nginx

Testez la fonctionnalité du serveur HTTP pour vous assurer qu'il peut desservir les fichiers de démarrage PXE et le contenu de l'installation aux clients.

PROCÉDURE 24 : TEST DU SERVEUR HTTP NGINX

1. Testez l'accès HTTP aux fichiers de démarrage :

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

2. Testez l'accès au répertoire d'installation :

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

3. Vérifiez qu'un fichier spécifique du programme d'installation est accessible :

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

8.5 Dépannage de la configuration nginx

Problèmes courants lors de la configuration de nginx pour la distribution HTTP au démarrage PXE.

8.5.1 Erreurs de syntaxe de la configuration

Une syntaxe de configuration nginx incorrecte empêche le service de démarrer ou de se recharger correctement.

PROCÉDURE 25 : RÉSOLUTION DES PROBLÈMES LIÉS À LA CONFIGURATION NGINX

1. Testez la syntaxe de la configuration :

```
> sudo nginx -t
```

2. Vérifiez le statut du service nginx si le démarrage échoue :

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

3. Affichez les journaux d'erreurs détaillés :

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

4. Vérifiez le fichier journal des erreurs de nginx :

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

8.5.2 Problèmes liés à l'accès aux fichiers et aux autorisations

nginx peut ne pas parvenir à desservir des fichiers en raison d'autorisations incorrectes ou de répertoires manquants.

PROCÉDURE 26 : RÉSOLUTION DES PROBLÈMES LIÉS À L'ACCÈS AUX FICHIERS

1. Vérifiez que le répertoire de démarrage existe et qu'il est accessible :

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

2. Vérifiez si le répertoire d'installation existe :

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

3. Vérifiez que nginx peut lire les répertoires :

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

4. Créez les répertoires manquants le cas échéant :

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

5. Définissez les autorisations appropriées :

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

8.5.3 Conflits de liaison de port

nginx peut ne pas parvenir à démarrer si un autre service utilise le port 80.

PROCÉDURE 27 : RÉSOLUTION DES CONFLITS DE PORT

1. Vérifiez ce qui utilise le port 80 :

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

2. Arrêtez les services en conflit le cas échéant :

```
> sudo systemctl stop apache2
```

3. Redémarrez le service nginx :

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

4. Vérifiez que nginx écoute sur le port 80 :

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

8.6 Étapes suivantes

Une fois nginx configuré pour la distribution HTTP, vous pouvez passer à la configuration des services DHCP de manière à diriger les clients PXE vers les chargeurs de démarrage et les ressources HTTP appropriés.

9 Configuration d'un serveur DNS à l'aide de dnsmasq

Cette section explique comment configurer les services DNS à l'aide de dnsmasq afin d'assurer la résolution des noms d'hôte pour les clients PXE qui accèdent aux ressources d'installation de SUSE Linux Enterprise Server 16.0. La configuration DNS permet aux clients d'utiliser des noms d'hôtes au lieu d'adresses IP dans les URL de démarrage et les configurations DHCP.

9.1 Introduction

Les services DNS permettent aux clients PXE de résoudre les noms d'hôtes dans les URL de démarrage et les sources d'installation. Bien que la configuration complète d'un serveur DNS dépasse le cadre de ce document, cette section présente une configuration DNS de base utilisant dnsmasq qui permet aux clients de résoudre le nom d'hôte du serveur PXE (*PXE.EXAMPLE.NET*) en adresses IP.

Sans configuration DNS, les URL de démarrage doivent utiliser directement des adresses IP, telles que `http://192.168.1.200/` ou `http://[2001:db8:0:1::200]/`. Certaines implémentations de microprogrammes BIOS/UEFI ne prennent pas en charge les noms d'hôtes dans les URL TFTP DHCP et requièrent des adresses IP telles que `tftp://[2001:db8:0:1::200]/`.

9.2 Configuration requise

- Le paquet `dnsmasq` est installé.
- Des adresses IP statiques sont configurées pour le serveur PXE.
- Des privilèges administratifs sont disponibles pour configurer les services DNS.

9.3 Configuration de services DNS dnsmasq

La configuration DNS dnsmasq assure la résolution des noms d'hôtes locaux et utilise des serveurs de noms en amont pour les requêtes externes.

PROCÉDURE 28 : CONFIGURATION D'UN SERVEUR DNS DNSMASQ

1. Créez le fichier de configuration DNS pour dnsmasq :

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

# Log DNS queries
log-queries

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

# Never forward A or AAAA queries for plain names to upstream name servers
domain-needed

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

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

2. Ajoutez des entrées de noms d'hôtes au fichier des hôtes (hosts) du système :

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

```
EOF
```

3. Testez la configuration dnsmasq :

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

4. Activez et démarrez le service dnsmasq :

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

Remarque : comportement du transfert DNS

Par défaut, dnsmasq utilise les serveurs de noms de `/etc/resolv.conf` comme redirecteurs et fournit des enregistrements à partir de `/etc/hosts`. Cela permet au serveur PXE de résoudre les noms d'hôtes externes tout en fournissant une résolution locale pour les services liés à PXE.

9.4 Vérification de la configuration DNS

Testez la fonctionnalité du serveur DNS pour vous assurer que la résolution du nom d'hôte fonctionne pour les clients PXE.

PROCÉDURE 29 : TEST DE LA FONCTIONNALITÉ DU SERVEUR DNS

1. Testez la résolution du nom d'hôte IPv4 :

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

2. Testez la résolution du nom d'hôte IPv6 :

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

3. Testez la recherche DNS inversée pour IPv4 :

```
> nslookup 192.168.1.200 localhost
```

4. Vérifiez que le transfert DNS externe fonctionne toujours :

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

9.5 Dépannage de la configuration DNS

Problèmes courants lors de la configuration de dnsmasq pour les services DNS dans les environnements PXE.

9.5.1 Problèmes de configuration et de service

dnsmasq peut ne pas démarrer en raison d'erreurs de configuration ou de conflits de ports.

PROCÉDURE 30 : RÉSOLUTION DES PROBLÈMES DE CONFIGURATION DNS

1. Testez la syntaxe de la configuration dnsmasq :

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

2. Vérifiez le statut du service dnsmasq :

```
> systemctl status dnsmasq
```

3. Vérifiez ce qui utilise le port DNS 53 :

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

4. Consultez les journaux dnsmasq pour vérifier s'il y a des erreurs :

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

5. Arrêtez les services DNS en conflit le cas échéant :

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

9.5.2 Échecs de la résolution de nom d'hôte

Les requêtes DNS peuvent échouer en raison d'une configuration incorrecte ou d'entrées de noms d'hôtes manquantes.

PROCÉDURE 31 : DIAGNOSTIC DES PROBLÈMES DE RÉSOLUTION DNS

1. Vérifiez si les entrées de noms d'hôtes existent dans le fichier hosts :

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

2. Vérifiez la configuration du domaine dans dnsmasq :

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

3. Testez une requête DNS avec sortie verbeuse :

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

4. Surveillez les journaux de requêtes dnsmasq :

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

5. Redémarrez dnsmasq pour recharger la configuration :

```
> sudo systemctl restart dnsmasq
```

9.5.3 Problèmes de transfert DNS

Les requêtes DNS externes peuvent échouer si la configuration du serveur de noms en amont est incorrecte.

PROCÉDURE 32 : DÉPANNAGE DES PROBLÈMES DE TRANSFERT DNS

1. Vérifiez la configuration du serveur de noms en amont :

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

2. Testez une requête directe auprès du serveur de noms en amont :

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

3. Vérifiez la configuration du transfert dnsmasq :

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

4. Ajoutez un serveur de noms spécifique en amont le cas échéant :

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

5. Redémarrez le service dnsmasq :

```
> sudo systemctl restart dnsmasq
```

9.6 Étapes suivantes

Une fois les services DNS configurés, les clients PXE peuvent résoudre les noms d'hôtes dans les URL de démarrage et les sources d'installation. Vous pouvez procéder à la configuration des services DHCP qui font référence au serveur DNS pour la configuration du client.

10 Configuration d'un serveur NTP à l'aide de chrony

Cette section explique comment configurer les services NTP à l'aide de `chrony` afin d'assurer une synchronisation horaire précise pour les clients PXE pendant les installations de SUSE Linux Enterprise Server 16.0. Une synchronisation horaire correcte est essentielle pour la validation des certificats et la journalisation système lors d'installations basées sur le réseau.

10.1 Introduction

Les services NTP assurent une synchronisation horaire précise dans l'ensemble de l'infrastructure réseau. Pour les environnements de démarrage PXE, la synchronisation horaire est cruciale pour la validation des certificats lors des connexions HTTPS, l'horodatage correct des journaux et les opérations système coordonnées. Cette section présente la configuration de base du serveur NTP à l'aide de `chrony`.

10.2 Configuration requise

- Le paquet `chrony` est installé.

  ```
  > sudo zypper install chrony
  ```

- La connectivité réseau est assurée vers les serveurs NTP en amont.
- Des privilèges administratifs sont disponibles pour configurer les services NTP.

10.3 Configuration du service NTP chrony

Le service `chrony` fournit une fonctionnalité NTP avec une synchronisation horaire automatique avec les serveurs en amont et des fonctionnalités d'heure locale pour les clients du réseau.

PROCÉDURE 33 : CONFIGURATION DU SERVEUR NTP `chrony`

- Activez et démarrez le service `chrony` :

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

10.4 Vérification de la configuration NTP

Testez la fonctionnalité du service NTP pour vous assurer que la synchronisation horaire fonctionne correctement.

PROCÉDURE 34 : TEST DE LA FONCTIONNALITÉ DU SERVEUR NTP

1. Vérifiez le statut du service `chrony` :

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

2. Affichez le statut actuel de la synchronisation horaire :

```
> chronyc tracking
```

3. Listez les sources NTP configurées :

```
> chronyc sources
```

4. Vérifiez les statistiques du serveur NTP :

```
> chronyc sourcestats
```

10.5 Dépannage de la configuration NTP

Problèmes courants lors de la configuration de `chrony` pour les services NTP dans les environnements PXE.

10.5.1 Problème de démarrage du service

Le service `chrony` peut ne pas démarrer en raison d'erreurs de configuration ou de problèmes de connectivité réseau.

PROCÉDURE 35 : RÉSOLUTION DES PROBLÈMES DU SERVICE NTP

1. Vérifiez le statut du service `chrony` et ses journaux :

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

2. Affichez les journaux détaillés du service :

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

3. Testez la configuration `chrony` :

```
> sudo chronyd -Q
```

4. Redémarrez le service le cas échéant :

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

10.5.2 Échecs de synchronisation horaire

La synchronisation horaire peut échouer en raison de problèmes de réseau ou d'une mauvaise configuration du serveur.

PROCÉDURE 36 : DIAGNOSTIC DES PROBLÈMES DE SYNCHRONISATION HORAIRE

1. Vérifiez le statut actuel de la synchronisation :

```
> chronyc tracking
```

2. Vérifiez la connectivité de la source NTP :

```
> chronyc sources -v
```

3. Forcez une synchronisation immédiate :

```
> sudo chronyc makestep
```

4. Vérifiez l'heure système par rapport à l'horloge matérielle :

```
> timedatectl status
```

5. Vérifiez la connectivité réseau vers les serveurs NTP :

```
> chronyc activity
```

10.5.3 Pare-feu et problèmes de réseau

Le trafic NTP peut être bloqué par des règles de pare-feu, ce qui empêche la synchronisation horaire.

PROCÉDURE 37 : RÉSOLUTION DES PROBLÈMES DE CONNECTIVITÉ RÉSEAU NTP

1. Vérifiez si le port NTP est ouvert dans le pare-feu :

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

2. Ajoutez le service NTP au pare-feu le cas échéant :

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

3. Rechargez la configuration du pare-feu :

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

4. Testez manuellement la connectivité NTP :

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

5. Vérifiez l'utilisation du port `chrony` :

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

10.6 Étapes suivantes

Si les services NTP sont configurés, le serveur et les clients PXE maintiendront une synchronisation horaire précise. Cela garantit une validation correcte des certificats et une coordination des opérations système lors d'installations basées sur le réseau.

11 Configuration des annonces de routeur IPv6

Cette section décrit comment configurer la fonctionnalité d'annonces de routeur IPv6 afin de fournir des annonces de routeur adéquates aux clients PXE. Les annonces de routeur IPv6 permettent la configuration du routage IPv6 et la configuration automatique des adresses DHCPv6 avec état pour les installations SUSE Linux Enterprise Server 16.0.

11.1 Introduction

Les annonces de routeur (RA) IPv6 fournissent des informations essentielles sur la configuration du réseau aux clients PXE, notamment les paramètres de routage IPv6 et de configuration automatique de l'adresse DHCPv6. Cette section suppose qu'un routeur IPv6 est configuré pour fournir des annonces de routeur adéquates afin de configurer le routage IPv6 vers le réseau et la route par défaut, et d'activer la configuration automatique de l'adresse DHCPv6 avec état à l'aide de `AdvManagedFlag on`.

11.2 Configuration requise

- Le paquet `radvd` est installé.
- Configuration du réseau IPv6 sur l'interface du serveur
- Des privilèges administratifs sont disponibles pour configurer les services d'annonces de routeur.

11.3 Configuration de `radvd` pour les annonces de routeur IPv6

Le service `radvd` fournit une fonctionnalité d'annonce de routeur IPv6 utilisant la configuration définie dans `/etc/radvd.conf`.

PROCÉDURE 38 : CONFIGURATION DES ANNONCES DE ROUTEUR IPV6 `radvd`

1. Configurez le service `radvd` :

```
> sudo cat > /etc/radvd.conf << 'EOF'
interface eno1
{
    # radvd options
    IgnoreIfMissing on;                # Do not fail and exit when interface is
 missed
    AdvSendAdvert on;                  # Sending RAs on the interface is not
 disabled

    # Configuration settings

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

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

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

2. Activez et démarrez le service `radvd` :

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

11.4 Vérification des annonces de routeur IPv6

Testez la fonctionnalité d'annonces de routeur IPv6 (IPv6 RA) pour garantir sa bonne configuration et son fonctionnement correct.

PROCÉDURE 39 : TEST DES ANNONCES DE ROUTEUR IPV6

1. Vérifiez le statut du service `radvd` :

```
> systemctl status radvd
```

2. Passez en revue et vérifiez les paramètres IPv6 RA à l'aide de **`ravdump`** :

```
> radvdump
```

   L'utilitaire **`radvdump`** affiche les paramètres IPv6 RA envoyés par le routeur IPv6 toutes les quelques minutes.

11.5 Configuration du transfert IP pour la fonctionnalité de routeur

Si le serveur PXE fait également office de routeur, le transfert IP doit être activé pour permettre au système de remplir un rôle de routeur.

PROCÉDURE 40 : ACTIVATION DU TRANSFERT IP SUR LE SERVEUR PXE

1. Créez le fichier de configuration réseau :

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

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

2. Appliquez les paramètres de configuration réseau :

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

Remarque : considérations relatives à la configuration du routeur

Par défaut, un routeur ne traite pas les annonces de routeur IPv6 pour la configuration automatique de l'hôte. Pour accepter les annonces de routeur IPv6 sur une interface de liaison montante de routeur, le paramètre sysctl `accept_ra = 2` est requis. Consultez la section Configuration du réseau du Guide d'administration pour plus de détails sur la configuration du routeur, y compris les réglages du pare-feu et les autres étapes nécessaires.

11.6 Dépannage des annonces de routeur IPv6

Problèmes courants lors de la configuration des annonces de routeur IPv6 pour les environnements PXE.

11.6.1 Problèmes liés au service `radvd`

Le service `radvd` peut ne pas démarrer en raison d'erreurs de configuration ou de problèmes d'interface.

PROCÉDURE 41 : RÉSOLUTION DES PROBLÈMES LIÉS AU SERVICE `radvd`

1. Vérifiez le statut du service `radvd` et ses journaux :

```
> systemctl status radvd
```

2. Affichez les journaux détaillés du service :

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

3. Testez la syntaxe de la configuration `radvd` :

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

4. Vérifiez si l'interface spécifiée existe :

```
> ip link show eno1
```

5. Redémarrez le service après avoir corrigé la configuration :

```
> sudo systemctl restart radvd
```

11.6.2 Problèmes liés à la configuration du transfert IP

Des paramètres de transfert IP incorrects peuvent empêcher le bon déroulement de la fonctionnalité de routeur.

PROCÉDURE 42 : DIAGNOSTIC DES PROBLÈMES LIÉS AU TRANSFERT IP

1. Vérifiez le statut actuel du transfert IP :

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

2. Vérifiez le statut du transfert IPv6 :

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

3. Vérifiez le fichier de configuration sysctl :

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

4. Appliquez la configuration si les valeurs sont incorrectes :

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

5. Vérifiez le paramètre accept_ra sur l'interface de liaison montante :

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

11.6.3 Problèmes liés à la réception des annonces de routeur

Les clients peuvent ne pas recevoir ou traiter correctement les annonces de routeur IPv6.

PROCÉDURE 43 : DÉPANNAGE DES PROBLÈMES LIÉS À LA RÉCEPTION DES ANNONCES DE ROUTEUR

1. Surveillez les annonces des routeurs à l'aide de **ravdump** :

```
> radvdump -d
```

2. Vérifiez la configuration de l'interface IPv6 sur les clients :

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

3. Vérifiez la table de routage IPv6 sur les clients :

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

4. Testez la connectivité IPv6 avec le routeur :

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

5. Vérifiez les règles de pare-feu pour ICMPv6 :

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

11.7 Étapes suivantes

Si l'annonce de routeur IPv6 est configurée, les clients PXE peuvent recevoir une configuration réseau IPv6 correcte. Cela active la fonctionnalité DHCPv6 et la connectivité IPv6 pour les installations basées sur le réseau.

12 Configuration d'un serveur DHCP à l'aide de dnsmasq

Cette section explique comment configurer les services DHCP à l'aide de dnsmasq afin de fournir les informations de configuration réseau et de démarrage PXE pour les installations SUSE Linux Enterprise Server 16.0. Le serveur DHCP dnsmasq utilise la configuration basée sur les balises pour prendre en charge les clients PXE IPv4 et IPv6 avec des fonctionnalités de démarrage UEFI et BIOS.

12.1 Introduction

Le serveur DHCP dnsmasq fournit des informations sur la configuration réseau et le fichier de démarrage aux clients PXE à l'aide d'un système basé sur les balises afin d'établir une correspondance avec les types de clients et de fournir les chargeurs de démarrage appropriés. Cette configuration prend en charge les correspondances PXEClient et HTTPClient qui fonctionnent pour DHCPv4 et DHCPv6, permettant le démarrage via les systèmes UEFI et BIOS sur de multiples architectures.

Important : limites HTTPClient dans dnsmasq

Les versions 2.90 et antérieures de dnsmasq ne prennent pas en charge l'envoi de l'option de classe de fournisseur (vendor-class) 6:16 aux clients DHCPv6 pour les configurations HTTPClient. Pour une prise en charge complète de HTTPClient, envisagez d'utiliser des serveurs DHCP Kea ou ISC.

12.2 Configuration requise

- Le paquet `dnsmasq` est installé.
- Les fichiers de démarrage PXE sont correctement organisés sous `/srv/tftpboot`.
- L'interface réseau est configurée pour le service DHCP.
- Des privilèges administratifs sont disponibles pour configurer les services DHCP.

12.3 Configuration des services DHCP dnsmasq

La configuration DHCP dnsmasq comprend la mise en correspondance des types de clients, les plages réseau et les affectations de fichiers de démarrage pour les réseaux IPv4 et IPv6.

PROCÉDURE 44 : CONFIGURATION D'UN SERVEUR DHCP DNSMASQ

1. Créez le fichier de configuration DHCP pour dnsmasq :

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

# Log DHCP processing
log-dhcp

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

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

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

# IPv6 PXE/HTTP boot client matches (enterprise:343 intel)
# Match client type in PXEClient:Arch and map to a tag
dhcp-vendorclass=set:tftp_bios_x86_pc,enterprise:343,PXEClient:Arch:00000
dhcp-vendorclass=set:tftp_uefi_x86_64,enterprise:343,PXEClient:Arch:00007
dhcp-vendorclass=set:tftp_ieee_ppc_64,enterprise:343,PXEClient:Arch:0000e
dhcp-vendorclass=set:tftp_uefi_arm_64,enterprise:343,PXEClient:Arch:00011
# Match client type in HTTPClient:Arch and map to a tag
dhcp-vendorclass=set:http_uefi_x86_64,enterprise:343,HTTPClient:Arch:00016
dhcp-vendorclass=set:http_uefi_arm_64,enterprise:343,HTTPClient:Arch:00019
EOF
```

2. Configurez la plage et les options DHCP IPv4 :

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

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

3. Configurez les options de démarrage PXE IPv4 :

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

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

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

4. Configurez la plage et les options DHCP IPv6 :

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

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

5. Configurez les options de démarrage PXE IPv6 :

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

# IPv6 PXEClient boot
```

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

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

6. Testez la configuration dnsmasq :

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

7. Activez et démarrez le service dnsmasq :

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

12.4 Vérification de la configuration DHCP

Testez la fonctionnalité de serveur DHCP pour vous assurer que la configuration réseau est correcte et que le fichier de démarrage adéquat est distribué aux clients PXE.

PROCÉDURE 45 : TEST DU SERVEUR DHCP DNSMASQ

1. Vérifiez le statut du service dnsmasq :

```
> systemctl status dnsmasq
```

2. Vérifiez la liaison de port DHCP :

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

3. Surveillez les assignations de baux DHCP :

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

4. Vérifiez les baux DHCP actifs :

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

12.5 Dépannage de la configuration DHCP dnsmasq

Problèmes courants lors de la configuration de dnsmasq pour les services DHCP dans les environnements PXE.

12.5.1 Problèmes liés à la configuration et au démarrage de services

dnsmasq peut ne pas démarrer en raison d'erreurs de configuration ou de conflits de ports avec d'autres services DHCP.

PROCÉDURE 46 : RÉSOLUTION DES PROBLÈMES DE SERVICE DHCP DNSMASQ

1. Testez la syntaxe de la configuration dnsmasq :

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

2. Recherchez les éventuels conflits de ports DHCP :

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

3. Arrêtez les services DHCP conflictuels :

```
> sudo systemctl stop dhcpd
```

4. Affichez les journaux détaillés du service :

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

5. Redémarrez dnsmasq après avoir résolu les conflits :

```
> sudo systemctl restart dnsmasq
```

12.5.2 Problèmes liés aux assignations de baux DHCP

Les clients peuvent ne pas recevoir d'adresses IP en raison de problèmes de configuration de plage ou de connectivité réseau.

PROCÉDURE 47 : DIAGNOSTIC DES PROBLÈMES LIÉS AUX BAUX DHCP

1. Vérifiez la configuration de la plage DHCP :

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

2. Surveillez les demandes DHCP en temps réel :

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

3. Vérifiez le statut de l'interface réseau :

```
> ip addr show
```

4. Vérifiez le paramètre DHCP faisant autorité :

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

5. Testez la réponse DHCP avec dhcping :

```
> dhcping -s 192.168.1.200
```

12.5.3 Problèmes liés à la distribution du fichier de démarrage PXE

Les clients PXE peuvent recevoir des adresses IP mais ne pas démarrer en raison d'une configuration incorrecte du fichier de démarrage ou de problèmes liés à la correspondance des types de clients.

PROCÉDURE 48 : DÉPANNAGE DE LA CONFIGURATION DU DÉMARRAGE PXE

1. Vérifiez la correspondance de la classe de fournisseur du client :

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

2. Vérifiez les chemins d'accès au fichier de démarrage :

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

3. Testez l'accès TFTP aux fichiers de démarrage :

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

4. Surveillez les journaux DHCP spécifiques à PXE :

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

5. Vérifiez l'assignation des balises dans les journaux :

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

12.5.4 Problèmes liés à la configuration DHCP IPv6

Les clients DHCP IPv6 nécessitent une configuration correcte des annonces de routeur et peuvent avoir des exigences d'adressage différentes de celles d'IPv4.

PROCÉDURE 49 : RÉSOLUTION DES PROBLÈMES LIÉS À DHCP IPV6

1. Vérifiez la configuration de la plage DHCP IPv6 :

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

2. Vérifiez le statut des annonces de routeur IPv6 :

```
> systemctl status radvd
```

3. Surveillez les requêtes DHCPv6 :

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

4. Testez la connectivité IPv6 :

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

5. Vérifiez la configuration de l'option IPv6 :

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

12.6 Étapes suivantes

Avec les services DHCP dnsmasq configurés, les clients PXE peuvent recevoir des informations sur la configuration réseau et le fichier de démarrage à la fois pour les environnements IPv4 et IPv6. Le système basé sur les balises permet une assignation flexible des fichiers de démarrage en fonction de l'architecture du client et des exigences de la méthode de démarrage.

13 Configuration d'un serveur DHCP à l'aide de Kea

Cette section explique comment configurer les services DHCP à l'aide de Kea afin de fournir les informations de configuration réseau et de démarrage PXE pour les installations SUSE Linux Enterprise Server 16.0. Kea est un serveur DHCP moderne qui prend en charge à la fois IPv4 et IPv6 avec une mise en correspondance de la classe du client pour les scénarios de démarrage PXE et HTTP.

13.1 Introduction

Kea est le serveur DHCP moderne développé par ISC pour succéder au serveur DHCP ISC hérité. Il assure une prise en charge robuste à la fois de DHCPv4 et de DHCPv6 avec des fonctionnalités de classification des clients qui permettent de distribuer un fichier de démarrage approprié en fonction de l'architecture et de la méthode de démarrage de ces derniers. Kea utilise des fichiers de configuration basés sur JSON et prend en charge des fonctionnalités avancées telles que l'identification de la classe du fournisseur pour le démarrage HTTP.

13.2 Configuration requise

- Les paquets DHCP Kea `kea-dhcp4` et `kea-dhcp6` sont installés.
- Les fichiers de démarrage PXE sont correctement organisés sous `/srv/tftpboot`.
- L'interface réseau est configurée pour le service DHCP.
- Des privilèges administratifs sont disponibles pour configurer les services DHCP.

13.3 Configuration du serveur DHCPv4 Kea

La configuration DHCPv4 Kea utilise des classes de clients pour mettre en correspondance les types de clients PXE et HTTP et fournir des fichiers de démarrage appropriés pour différentes architectures.

PROCÉDURE 50 : CONFIGURATION DU SERVEUR DHCPV4 KEA

1. Configurez le serveur DHCPv4 Kea :

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

```
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [
        "eno1"
      ]
    },
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea4-ctrl-socket"
    },
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/lib/kea/dhcp4.leases",
      "lfc-interval": 3600
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250,
      "unwarned-reclaim-cycles": 5
    },
    "renew-timer": 1800,
    "rebind-timer": 3150,
    "valid-lifetime": 3600,
    "option-data": [],
    "client-classes": [
      {
        "name": "pxeclients#00000",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:00000'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/i386-pc/core.0"
      },
      {
        "name": "pxeclients#00007",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:00007'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/x86_64-efi/bootx64.efi"
      },
      {
        "name": "pxeclients#0000e",
        "test": "substring(option[60].hex,0,20) == 'PXEClient:Arch:0000e'",
        "next-server": "192.168.1.200",
        "boot-file-name": "/boot/grub2/powerpc-ieee1275/core.elf"
```

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

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

2. Créez le répertoire pour les journaux de Kea :

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

3. Testez la configuration DHCPv4 Kea :

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

4. Activez et démarrez le service DHCPv4 Kea :

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

13.4 Configuration du serveur DHCPv6 Kea

La configuration DHCPv6 Kea assure l'assignation d'adresses IPv6 et la fourniture des informations sur le fichier de démarrage à l'aide de la mise en correspondance de la classe de fournisseur pour différentes architectures de clients.

PROCÉDURE 51 : CONFIGURATION DU SERVEUR DHCPV6 KEA

1. Configurez le serveur DHCPv6 Kea :

```
> sudo cat > /etc/kea/kea-dhcp6.conf << 'EOF'
{
  "Dhcp6": {
    "interfaces-config": {
      "interfaces": [
        "eno1"
      ]
    },
    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/tmp/kea6-ctrl-socket"
    },
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/lib/kea/dhcp6.leases",
      "lfc-interval": 3600
    },
    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250,
      "unwarned-reclaim-cycles": 5
    },
    "renew-timer": 1800,
    "rebind-timer": 2880,
    "preferred-lifetime": 3600,
    "valid-lifetime": 7200,
    "option-data": [],
    "option-def": [],
    "client-classes": [
      {
        "name": "pxeclients#00000",
        "test": "substring(option[16].hex,6,20) == 'PXEClient:Arch:00000'",
        "option-data": [
```

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

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

2. Testez la configuration DHCPv6 Kea :

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

3. Activez et démarrez le service DHCPv6 Kea :

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

13.5 Vérification de la configuration DHCP Kea

Testez la fonctionnalité du serveur DHCP Kea pour vous assurer que la configuration réseau est correcte et que le fichier de démarrage adéquat est distribué aux clients PXE.

PROCÉDURE 52 : TEST DES SERVEURS DHCP KEA.

1. Vérifiez le statut du service DHCPv4 Kea :

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

2. Vérifiez le statut du service DHCPv6 Kea :

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

3. Vérifiez la liaison de port DHCP :

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

4. Surveillez les journaux DHCPv4 :

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

5. Surveillez les journaux DHCPv6 :

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

6. Vérifiez les baux DHCP actifs :

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

13.6 Dépannage de la configuration DHCP Kea

Problèmes courants lors de la configuration des serveurs DHCP Kea pour les environnements de démarrage PXE.

13.6.1 Problèmes de configuration et de service

Les services Kea peuvent ne pas démarrer en raison d'erreurs de configuration JSON ou de problèmes d'interface réseau.

PROCÉDURE 53 : RÉSOLUTION DES PROBLÈMES DE CONFIGURATION KEA

1. Testez la syntaxe de la configuration DHCPv4 :

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

2. Testez la syntaxe de la configuration DHCPv6 :

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

3. Recherchez les éventuelles erreurs de syntaxe JSON :

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

4. Vérifiez la configuration de l'interface réseau :

```
> ip addr show eno1
```

5. Vérifiez les journaux du service Kea :

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

13.6.2 Problèmes liés aux assignations de baux DHCP

Les clients peuvent ne pas recevoir d'adresses IP en raison de problèmes de configuration de sous-réseau ou d'épuisement du pool.

PROCÉDURE 54 : DIAGNOSTIC DES PROBLÈMES LIÉS AUX BAUX KEA

1. Vérifiez la configuration du sous-réseau et du pool :

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

2. Surveillez les assignations de baux en temps réel :

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

3. Recherchez les éventuels conflits dans la base de données des baux :

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

4. Vérifiez la liaison de l'interface :

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

5. Effacez la base de données des baux le cas échéant :

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

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

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

13.6.3 Problèmes de mise en correspondance de la classe des clients PXE

Les clients PXE peuvent recevoir des adresses IP mais ne pas obtenir le bon fichier de démarrage en raison de problèmes de configuration de la classe des clients.

PROCÉDURE 55 : DÉPANNAGE DE LA CLASSIFICATION DES CLIENTS KEA

1. Vérifiez les définitions de classes des clients :

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

2. Surveillez la mise en correspondance de la classe des clients dans les journaux :

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

3. Vérifiez les modèles d'identificateur de classe de client :

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

4. Testez l'accessibilité du fichier de démarrage :

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

5. Activez la journalisation de débogage pour une analyse détaillée du client :

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

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

13.6.4 Problèmes spécifiques à DHCPv6

Les clients DHCP IPv6 nécessitent une configuration correcte des annonces de routeur et gèrent l'option de classe de fournisseur différemment des clients IPv4.

PROCÉDURE 56 : RÉSOLUTION DES PROBLÈMES DHCPV6 KEA

1. Vérifiez la configuration de sous-réseau DHCPv6 :

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

2. Vérifiez le statut des annonces de routeur IPv6 :

```
> systemctl status radvd
```

3. Vérifiez la correspondance de la classe de fournisseur DHCPv6 :

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

4. Vérifiez le format de l'option bootfile-url IPv6 :

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

5. Testez la connectivité IPv6 vers le serveur de démarrage :

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

13.7 Étapes suivantes

Avec les services DHCP Kea configurés, les clients PXE peuvent recevoir des informations complètes sur la configuration réseau et le fichier de démarrage à la fois pour les environnements IPv4 et IPv6. Le système de classification des clients permet une assignation précise des fichiers de démarrage en fonction de l'architecture du client et prend en charge à la fois les méthodes traditionnelles de démarrage PXE et les méthodes modernes de démarrage HTTP.

14 Configuration d'un serveur DHCP avec DHCP ISC

Cette section explique comment configurer le serveur DHCP ISC afin de fournir les informations de configuration réseau et de démarrage PXE pour les installations SUSE Linux Enterprise Server 15. Le paquet dhcp-server ISC n'est plus disponible sous SUSE Linux Enterprise Server 16.0. DHCP ISC utilise la mise en correspondance des classes et des sous-classes pour prendre en charge les scénarios de démarrage PXE et HTTP dans différentes architectures de clients.

14.1 Introduction

DHCP ISC est le serveur DHCP traditionnel qui fournit les informations sur la configuration réseau et le fichier de démarrage aux clients PXE à l'aide d'un système de classes et de sous-classes. Bien qu'ISC ait déclaré ce serveur en fin de vie à partir de 2022, il reste largement utilisé dans les déploiements existants et offre une prise en charge solide des scénarios de démarrage PXE et HTTP avec identification de la classe du fournisseur.

Important : statut de fin de vie de DHCP ISC

DHCP ISC a été déclaré en fin de vie par ISC en 2022. Pour les nouveaux déploiements, envisagez d'utiliser Kea ou dnsmasq à la place. Cette configuration est fournie pour assurer la compatibilité avec les installations DHCP ISC existantes.

14.2 Configuration requise

- Les paquets DHCP ISC `dhcp-server` sont installés.
- Les fichiers de démarrage PXE sont correctement organisés sous `/srv/tftpboot`.
- L'interface réseau est configurée pour le service DHCP.
- Des privilèges administratifs sont disponibles pour configurer les services DHCP.

14.3 Configuration du serveur DHCPv4 ISC

La configuration DHCPv4 ISC utilise des déclarations de classes et de sous-classes pour mettre en correspondance les types de clients PXE et HTTP et fournir des fichiers de démarrage appropriés pour différentes architectures.

PROCÉDURE 57 : CONFIGURATION DU SERVEUR DHCPV4 KEA

1. Configurez le serveur DHCPv4 ISC :

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

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

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

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

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

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

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

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

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

        range  dynamic-bootp            192.168.1.100 192.168.1.199;

        option subnet-mask              255.255.255.0;

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

2. Configurez l'interface DHCP dans sysconfig :

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

3. Testez la configuration DHCPv4 :

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

4. Activez et démarrez le service DHCPv4 ISC :

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

14.4 Configuration du serveur DHCPv6 ISC

La configuration DHCPv6 ISC assure l'assignation d'adresses IPv6 et la fourniture des informations sur le fichier de démarrage à l'aide de la mise en correspondance de la classe de fournisseur avec la gestion adéquate des options DHCPv6.

PROCÉDURE 58 : CONFIGURATION DU SERVEUR DHCPV6 ISC

1. Configurez le serveur DHCPv6 ISC :

```
> sudo cat > /etc/dhcpd6.conf << 'EOF'
# /etc/dhcpd6.conf
#
# Sample DHCPv6 configuration file for ISC dhcpd
#
# *** PLEASE CONFIGURE IT FIRST ***
#
# Don't forget to set the DHCPD6_INTERFACE in the
# /etc/sysconfig/dhcpd file.
#

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

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

# IPv6 address valid lifetime
#  (at the end the address is no longer usable by the client)
#  (set to 30 days, the usual IPv6 default)
default-lease-time 7200;

# IPv6 address preferred lifetime
#  (at the end the address is deprecated, i.e., the client should use
#   other addresses for new connections)
#  (set to 7 days, the usual IPv6 default)
preferred-lifetime 3600;

##
## PXE / HTTP boot option declarations
##

# The dhcp6 option 16 is in fact an:
#   { uint32 enterprise-number, array of { uint16 len, string tag} vendor-class-
data }
# this declaration is using the whole option data as string for substring match:
```

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

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

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

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

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

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

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

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

2. Configurez l'interface DHCPv6 dans sysconfig :

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

3. Testez la configuration DHCPv6 :

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

4. Activez et démarrez le service DHCPv6 ISC :

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

14.5 Vérification de la configuration DHCP ISC

Testez la fonctionnalité du serveur DHCP ISC pour vous assurer que la configuration réseau est correcte et que le fichier de démarrage adéquat est distribué aux clients PXE.

PROCÉDURE 59 : TEST DES SERVEURS DHCP ISC

1. Vérifiez le statut du service DHCPv4 ISC :

```
> systemctl status dhcpd
```

2. Vérifiez le statut du service DHCPv6 ISC :

```
> systemctl status dhcpd6
```

3. Vérifiez la liaison de port DHCP :

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

4. Surveillez les journaux DHCP :

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

5. Vérifiez les baux DHCP actifs :

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

6. Surveillez l'activité DHCPv6 :

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

14.6 Dépannage de la configuration DHCP ISC

Problèmes courants lors de la configuration des serveurs DHCP ISC pour les environnements de démarrage PXE.

14.6.1 Problèmes de configuration et de service

Les services DHCP ISC peuvent ne pas démarrer en raison d'erreurs de syntaxe de la configuration ou de problèmes de liaison d'interface.

PROCÉDURE 60 : RÉSOLUTION DES PROBLÈMES DE CONFIGURATION DHCP ISC

1. Testez la syntaxe de la configuration DHCPv4 :

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

2. Testez la syntaxe de la configuration DHCPv6 :

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

3. Vérifiez la configuration de l'interface :

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

4. Vérifiez le statut de l'interface réseau :

```
> ip addr show eno1
```

5. Recherchez les éventuels conflits de ports :

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

6. Affichez les journaux détaillés du service :

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

14.6.2 Problèmes liés aux assignations de baux DHCP

Les clients peuvent ne pas recevoir d'adresses IP en raison de problèmes d'autorisation ou de configuration de sous-réseau.

PROCÉDURE 61 : DIAGNOSTIC DES PROBLÈMES LIÉS AUX BAUX DHCP ISC

1. Vérifiez la configuration du sous-réseau et de la plage :

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

2. Vérifiez le paramètre faisant autorité :

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

3. Surveillez les assignations de baux en temps réel :

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

4. Recherchez les éventuelles erreurs dans la base de données des baux :

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

5. Testez la réponse DHCP manuellement :

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

14.6.3 Problèmes de mise en correspondance des classes et sous-classes

Les clients PXE peuvent recevoir des adresses IP mais ne pas obtenir les fichiers de démarrage appropriés en raison de problèmes de configuration de la mise en correspondance des classes.

PROCÉDURE 62 : DÉPANNAGE DE LA MISE EN CORRESPONDANCE DES CLASSES DHCP ISC

1. Vérifiez les définitions de classe :

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

2. Vérifiez les entrées de sous-classe :

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

3. Surveillez l'identification des classes de fournisseurs :

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

4. Testez l'accessibilité du fichier de démarrage :

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

5. Activez la journalisation détaillée :

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

```
> sudo systemctl restart dhcpd
```

14.6.4 Problèmes liés à l'option de classe de fournisseur DHCPv6

Les clients DHCP IPv6 présentent une gestion complexe de l'option de classe fournisseur qui peut nécessiter une configuration spécifique pour une prise en charge correcte du démarrage PXE.

PROCÉDURE 63 : RÉSOLUTION DES PROBLÈMES DHCPV6 ISC

1. Vérifiez les définitions des options DHCPv6 :

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

2. Vérifiez l'analyse des chaînes de classes de fournisseurs :

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

3. Vérifiez la correspondance de la classe de fournisseur DHCPv6 :

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

4. Vérifiez le format de l'option bootfile-url IPv6 :

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

5. Vérifiez la dépendance des annonces de routeur :

```
> systemctl status radvd
```

6. Testez la connectivité IPv6 :

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

14.7 Étapes suivantes

Lorsque les services DHCP ISC sont configurés, les clients PXE peuvent recevoir des informations sur la configuration réseau et le fichier de démarrage à l'aide du système traditionnel de classes et de sous-classes. Bien que DHCP ISC soit en fin de vie, cette configuration assure la compatibilité pour les déploiements existants qui nécessitent des fonctionnalités de démarrage PXE et HTTP sur plusieurs architectures de clients.

15 Validation de la configuration du serveur PXE

Cette section décrit comment valider et tester la configuration complète du serveur PXE afin de s'assurer que tous les composants fonctionnent correctement pour les installations réseau de SUSE Linux Enterprise Server 16.0. Il couvre la vérification des services, les tests de connectivité du réseau et la validation du démarrage PXE de bout en bout.

15.1 Introduction

Après avoir configuré tous les composants du serveur PXE, y compris les services TFTP, HTTP, DNS, DHCP et de chargeur de démarrage GRUB 2, il est essentiel de valider le bon fonctionnement de l'ensemble du système. Cette validation garantit que les clients PXE peuvent démarrer avec succès dans le programme d'installation Agama et effectuer des installations basées sur le réseau de SUSE Linux Enterprise Server 16.0.

15.2 Configuration requise

- Tous les composants du serveur PXE sont configurés et opérationnels.
- Des systèmes clients de test capables d'effectuer des démarrages PXE sont disponibles.

- Une connectivité réseau est assurée entre le serveur PXE et les clients.
- Un accès administratif est disponible pour surveiller les services du serveur.

15.3 Validation des services du serveur PXE

Vérifiez que tous les services essentiels du serveur PXE sont en cours d'exécution et sont correctement configurés avant de les tester avec les clients PXE.

PROCÉDURE 64 : VÉRIFICATION DU STATUT DU SERVICE DU SERVEUR PXE

1. Vérifiez le statut du service TFTP :

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

   Résultat attendu : le service doit être actif et écouter sur le port 69.

2. Vérifiez le service HTTP nginx :

   ```
   > systemctl status nginx
   ```

   Résultat attendu : le service doit être actif et écouter sur le port 80.

3. Vérifiez le service DNS (si vous utilisez dnsmasq) :

   ```
   > systemctl status dnsmasq
   ```

   Résultat attendu : le service doit être actif et écouter sur le port 53.

4. Vérifiez le statut du service DHCP (choisissez le service approprié) :

   ```
   > systemctl status dhcpd
   ```

   Pour DHCP dnsmasq :

   ```
   > systemctl status dnsmasq
   ```

   Pour DHCP Kea :

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

   Résultat attendu : le service DHCP doit être actif et écouter sur les ports appropriés.

5. Vérifiez les annonces de routeur IPv6 (si configurées) :

```
> systemctl status radvd
```

Résultat attendu : le service doit être actif pour les environnements IPv6.

6. Vérifiez le service NTP :

```
> systemctl status chronyd
```

Résultat attendu : le service doit être actif et synchronisé.

15.4 Test de la connectivité réseau et de l'accès aux fichiers

Vérifiez que les clients PXE peuvent accéder aux fichiers de démarrage et au contenu de l'installation sur le réseau à l'aide des protocoles TFTP et HTTP.

PROCÉDURE 65 : TEST DE L'ACCÈS AUX FICHIERS DU RÉSEAU

1. Testez l'accès TFTP aux fichiers de chargeur de démarrage :

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

Vérifiez que le fichier a bien été récupéré :

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

Nettoyez les fichiers de test :

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

2. Testez l'accès HTTP à la configuration GRUB 2 :

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

Résultat attendu : réponse HTTP 200 OK.

3. Vérifiez l'accès HTTP aux fichiers du programme d'installation :

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

Résultat attendu : réponse HTTP 200 OK avec une longueur de contenu appropriée.

4. Testez la résolution DNS (si le DNS local est configuré) :

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

   Résultat attendu : résolution correcte des enregistrements A et AAAA.

5. Vérifiez la navigation dans les répertoires pour les emplacements d'autoindex :

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

   Résultat attendu : liste de répertoires montrant les fichiers de démarrage.

15.5 Validation de la fonctionnalité DHCP

Testez les réponses du serveur DHCP et vérifiez que les informations de démarrage appropriées sont fournies aux différents types de clients.

PROCÉDURE 66 : TEST DES RÉPONSES DU SERVEUR DHCP

1. Vérifiez la liaison de port DHCP :

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

   Résultat attendu : services DHCP écoutant sur les ports 67 (IPv4) et 547 (IPv6).

2. Surveillez les demandes DHCP en temps réel :

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

   Ou pour dnsmasq :

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

   Laissez cette commande s'exécuter pour observer l'activité DHCP pendant le test.

3. Testez la réponse DHCP à l'aide de dhcping (si disponible) :

```
> dhcping -s 192.168.1.200
```

   Résultat attendu : réponse DHCP réussie du serveur.

4. Vérifiez les baux DHCP actifs :

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

Ou pour Kea :

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

Résultat attendu : entrées de baux pour les clients tests.

15.6 Test de démarrage PXE de bout en bout

Effectuez des tests complets de démarrage PXE avec des systèmes clients réels pour valider l'ensemble du processus de démarrage, depuis DHCP jusqu'au démarrage du programme d'installation Agama.

PROCÉDURE 67 : TEST DU PROCESSUS COMPLET DE DÉMARRAGE PXE

1. Préparez un système client de test :
   - Configurez le BIOS/UEFI pour permettre le démarrage réseau.
   - Définissez le démarrage réseau comme première priorité de démarrage.
   - Connectez le client au même réseau que le serveur PXE.
2. Surveillez les journaux du serveur PXE pendant le démarrage du client :

   ```
   > journalctl -f | grep -E "dhcp|tftp|nginx"
   ```
3. Démarrez le client de test et observez la séquence suivante :
   1. Le client devrait recevoir une adresse IP via DHCP.
   2. Le client devrait télécharger le chargeur de démarrage via TFTP.
   3. Le menu GRUB 2 devrait apparaître avec les options d'installation.
   4. Le kernel Linux et l'unité RAM initiale (initrd) devraient se charger via HTTP.
   5. Le programme d'installation Agama devrait démarrer correctement.

4. Vérifiez la détection de l'architecture du client en testant différents types de clients :
    - Systèmes BIOS x86_64 hérités (devraient obtenir le fichier core.0)
    - Systèmes UEFI x86_64 (devraient obtenir le fichier bootx64.efi)
    - Systèmes UEFI aarch64 (devraient obtenir le fichier bootaa64.efi)
5. Testez le démarrage PXE IPv6 (si IPv6 est configuré) :
    - Activez la configuration réseau IPv6 uniquement sur le client de test.
    - Vérifiez l'assignation d'adresses DHCPv6.
    - Vérifiez la distribution de bootfile-url IPv6.

15.7 Validation des fonctionnalités du programme d'installation Agama

Vérifiez que le programme d'installation Agama démarre correctement et qu'il peut accéder aux sources d'installation pour effectuer les installations de SUSE Linux Enterprise Server 16.0.

PROCÉDURE 68 : TEST DU DÉMARRAGE DU PROGRAMME D'INSTALLATION AGAMA

1. Vérifiez l'accessibilité de l'interface Web d'Agama :
   Lors du démarrage du client, notez l'adresse IP assignée et l'accès :

   ```
   http://CLIENT_IP_ADDRESS
   ```

   Résultat attendu : l'interface Web Agama devrait se charger correctement.
2. Vérifiez les journaux du programme d'installation Agama sur le client :
   Basculez vers la console (Alt + F2) et exécutez :

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

   Résultat attendu : aucune erreur critique ne doit se produire au démarrage d'Agama.
3. Vérifiez l'accessibilité de la source d'installation :
   Pour les installations ISO complètes, vérifiez l'accès au dépôt :

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

   Résultat attendu : réponse HTTP 200 OK avec la liste du dépôt.

4. Testez la fonctionnalité d'installation de paquet :
   Dans l'interface Agama, vérifiez que :

   - le système peut détecter les disques disponibles ;
   - la configuration réseau est conservée ;
   - le dépôt de paquets est accessible ;
   - l'installation peut se poursuivre jusqu'à son terme.

15.8 Dépannage des échecs de validation

Problèmes courants lors de la validation du serveur PXE et leurs étapes de résolution.

15.8.1 Échecs de l'assignation DHCP

Les clients ne reçoivent pas d'adresses IP pendant le démarrage PXE.

PROCÉDURE 69 : RÉSOLUTION DES PROBLÈMES DE VALIDATION DHCP

1. Recherchez les éventuels conflits de service DHCP :

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

2. Vérifiez que l'interface réseau est opérationnelle :

```
> ip addr show eno1
```

3. Vérifiez la disponibilité de la plage DHCP :

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

4. Surveillez les journaux DHCP pour repérer les éventuelles erreurs :

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

15.8.2 Échecs de distribution des fichiers de démarrage

Les clients reçoivent des adresses IP, mais ne parviennent pas à télécharger les fichiers de démarrage.

PROCÉDURE 70 : RÉSOLUTION DES PROBLÈMES LIÉS AUX FICHIERS DE DÉMARRAGE

1. Vérifiez l'accessibilité du service TFTP :

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

2. Vérifiez les autorisations des fichiers :

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

3. Surveillez les journaux d'accès TFTP :

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

4. Vérifiez la détection de l'architecture des clients :

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

15.8.3 Échecs du démarrage du programme d'installation Agama

Les fichiers de démarrage se chargent correctement, mais le programme d'installation Agama ne démarre pas.

PROCÉDURE 71 : RÉSOLUTION DES PROBLÈMES DE DÉMARRAGE D'AGAMA

1. Vérifiez l'accès HTTP aux fichiers du programme d'installation :

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

2. Vérifiez la syntaxe des paramètres du kernel Linux dans la configuration GRUB 2 :

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

3. Surveillez le processus de démarrage des clients :

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

4. Vérifiez la persistance de la configuration réseau :

```
# ip addr show
```

15.9 Liste de contrôle pour la validation du serveur PXE

Cette liste de contrôle vous permet de vérifier systématiquement tous les aspects de la configuration de votre serveur PXE.

TABLEAU 2 : LISTE DE CONTRÔLE POUR LA VALIDATION DU SERVEUR PXE

Composant	Étape de validation	Statut
TFTP Service	Service actif, écoute sur le port 69, fichiers accessibles	☐
Service HTTP	nginx actif, écoute sur le port 80, fichiers du programme d'installation accessibles	☐
Service DNS	Résolution du nom d'hôte opérationnelle, écoute sur le port 53	☐
Service DHCP	Assignation d'adresses IP opérationnelle, options de démarrage distribuées	☐
Configuration GRUB 2	Le menu se charge ; la détection de l'architecture fonctionne	☐
Prise en charge d'IPv6	Annonces de routeur actives, DHCPv6 opérationnel	☐
Démarrage PXE	Le client démarre correctement et reçoit un chargeur de démarrage correct	☐
Programme d'installation Agama	Le programme d'installation démarre ; l'interface Web est accessible	☐
Source d'installation	Dépôt accessible, paquets installables	☐
Persistance du réseau	Maintien de la configuration réseau pendant l'installation	☐

15.10 Conclusion de la validation

Un serveur PXE correctement validé devrait présenter une fonctionnalité correcte de bout en bout, depuis le démarrage du réseau du client jusqu'au démarrage du programme d'installation Agama. Tous les services devraient fonctionner sans erreur et les clients devraient être en mesure

d'effectuer des installations de SUSE Linux Enterprise Server 16.0 sur le réseau. Des tests de validation réguliers garantissent la fiabilité continue de l'infrastructure PXE pour les déploiements automatisés.

16 Mentions légales

A GNU Free Documentation License

0. PREAMBLE

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

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

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

1. APPLICABILITY AND DEFINITIONS

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

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

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

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

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

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

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

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

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

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

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions

whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

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

3. COPYING IN QUANTITY

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

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

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

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

4. MODIFICATIONS

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

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

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

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

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

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

5. COMBINING DOCUMENTS

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

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

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

6. COLLECTIONS OF DOCUMENTS

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

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

7. AGGREGATION WITH INDEPENDENT WORKS

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

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

8. TRANSLATION

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

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

9. TERMINATION

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

10. FUTURE REVISIONS OF THIS LICENSE

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

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

ADDENDUM: How to use this License for your documents

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

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

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

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

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