 DOI: https://doi.org/10.12349/iser.v6i7.6712

Research and Implementation of PXE Network Booting Technology Based on OpenEuler Operating System

Ye Zhu

Yunnan Post and Telecommunications Engineering Co., Ltd., Kunming, Yunnan, 650233, China

Abstract

With the advancement of China's information technology self-reliance strategy, the domestic operating system OpenEuler has seen increasingly widespread adoption in server applications. This paper investigates PXE (Preboot Execution Environment) network boot technology based on OpenEuler to address automated installation requirements for large-scale device deployments. Through analyzing the PXE protocol stack principles, we designed and implemented an integrated solution combining DHCP/TFTP/HTTP/NFS services with OpenEuler. The proposed framework validates the feasibility of using a PXE service architecture in domestic operating systems, incorporates localized encryption algorithms, implements SM2 certificate authentication in DHCP services to ensure device identity credibility, and features hardware recognition and adaptation capabilities that dynamically distribute and load corresponding kernels and driver modules according to processor architectures.

Keywords

OpenEuler; PXE; network boot; automated deployment; domestic operating system

基于 OpenEuler 操作系统的 PXE 网络启动技术研究与实现

朱烨

云南邮电工程有限公司，中国·云南 昆明 650233

摘　要

随着信息技术自主可控战略的推进，国产操作系统OpenEuler在服务器领域的应用日益广泛。本文针对大规模设备部署中的自动化安装需求，研究基于OpenEuler的PXE（Preboot eXecution Environment）网络启动技术。通过分析PXE协议栈原理，设计并实现了基于OpenEuler的DHCP/TFTP/HTTP/NFS服务集成方案。本方案验证了国产操作系统使用PXE服务架构的可行性，集成了国产化加密系统算法支持；在DHCP服务中实现SM2证书认证，确保设备身份可信；设计了硬件识别和适应功能，可根据不同架构的处理器，分发并加载对应的内核和驱动模块。

关键词

OpenEuler；PXE；网络启动；自动化部署；国产操作系统

1 概述

1.1 研究背景

信息技术应用创新（信创）产业是中国实现技术可管可控、保障国家信息安全的不可或缺的一部分。在全球科技竞争加剧、国际技术封锁的背景下，新创产业以“2+8+N”作为方针，覆盖电信、金融、航空航天、医疗等关键领域，旨在构建从芯片、操作系统、数据库到应用软件的国产化技术生态。2023 年 8 月财政部首次就 7 项具体软硬件设备出台采购需求标准细则，意味着信创在政府部门的进一步深入。其中，《操作系统政府采购需求标准征求意见稿》明确应当符合安全可靠测评要求，要求操作系统同源兼容 ARM、LoongArch、MIPS、SW64、x86 等平台建构的 CPU，其中操作系统作为新创生态的基石，直接影响软硬件监控、应用生态技术自主性。

在这一背景下，国产操作系统 OpenEuler 凭借其开源开放、高性能、高安全性等特点，成为信创领域的重要选择。OpenEuler 由华为贡献至开放原子开源基金会，支持 ARM、x86 等多种架构，并已在金融、电信、政务等多个行业实现规模化应用。然而，随着国产化替代进程加速，如何高效、安全地完成大规模设备部署成为亟待解决的问题。传统的人工安装方式（如 U 盘或光盘部署）效率低下，难以满足企业级场景下数百甚至上千台服务器的快速部署需求。

PXE 技术作为一种成熟的网络启动方案，可通过标准化的 DHCP、TFTP 等协议实现无人值守的自动化安装，显著提升部署效率。然而，当前 PXE 技术的研究与实践主要基于 Red Hat、Ubuntu 等国际主流操作系统，针对 OpenEuler 的 PXE 部署方案仍缺乏系统性研究。特别是在信创环境下，PXE 的实现需考虑国产硬件的兼容性、国密算法的支持以及符合国家信息安全标准的技术适配。

【作者简介】朱烨（1997–），男，中国云南曲靖人，本科，从事信息通信工程技术研究。

1.2 研究现状

目前，国际主流的 PXE 部署方案主要围绕 RHEL（Red Hat Enterprise Linux）的 Kickstart 和 Ubuntu 的 Autoinstall 技术展开。这些方案通过集成 DHCP、TFTP 和 HTTP/NFS 服务，实现自动化安装，并支持定制化的预安装脚本（如 Kickstart 的 %post 段）。然而，国产系统相关 PXE 公开的解决方案、技术资料相对较少，这些技术方案在国产化环境中面临以下挑战：

1. 硬件兼容性问题：国产 CPU（如鲲鹏、飞腾、龙芯）的 UEFI 固件对 PXE 协议的支持存在差异，部分设备需定制引导加载程序（如 grubaa64.efi）。

2. 安全合规要求：信创领域对数据传输加密（如 SM3/SM4 国密算法）、镜像完整性校验等有严格要求，而传统 PXE 方案依赖 SHA-256 或 MD5 校验，不符合国内行业标准。

3. 生态工具链缺失：OpenEuler 缺乏类似 RHEL 的 Anaconda 安装器图形化配置工具，OpenEuler 则需依赖命令行实现复杂部署逻辑。

1.3 OpenEuler 系统特性化研究

在 PXE 网络部署领域，OpenEuler 与 RHEL、Ubuntu 国际主流 linux 体系相比展现出对于国产操作系统对于安全可控、硬件兼容国产化特性，OpenEuler 通过以下两点技术革新构建自主化部署体系：

1. 安全启动机制差异

启用国密算法支持，在挂载镜像时强制完整性校验（mount -o ro,loop,verity=sm3），该设计使得文件完整性验证符合国家相关网络启动安全规范要求，而 CentOS 仅支持传统 SHA256 校验方案。

2. 固件兼容性处理

硬件适配性取得突破性进展，通过深度定制 uefisectool 架构检测工具链，实现对鲲鹏、飞腾等国产芯片的固件级兼容性保障，例如在 ARM64 平台需可执行 uefisectool --arch aarch64 --validate BOOTAA64.EFI 完成引导文件验证，相较之下 RHEL 体系系统对于国产化系统与国产系统的兼容性存在一定问题。

2 OpenEuler 系统 PXE 自动化部署技术实现详解

预启动执行环境 (Pre-boot Execution Environment，PXE) 是由 Intel 公司开发的一种无盘启动技术，用于计算机通过网络远程启动，工作在 Client/Server 的软件系统体系结构下。当计算机设置以 LAN 方式启动时，就会通过网卡内置的启动芯片发出请求，要求服务器分配 IP 地址，建立联系后，再用 TFTP(Trivial File Transfer Protocol) 协议将预先存储在服务器中的终端操作系统镜像包下载到本机内存中执行，完成终端操作系统的远程启动 [1].

2.1 环境部署基础构建

在 OpenEuler 22.03 LTS 系统上构建 PXE 服务需搭建三层核心服务架构：DHCP 服务实现客户端网络参数动态分配，TFTP 服务承载 GRUB 引导文件传输，HTTP 服务提供完整的操作系统安装源。实施过程首先需挂载官方镜像文件，通过 mount -o ro,loop,verity=sm3 openEuler-22.03-LTS-x86_64-dvd.iso /mnt 建立本地访问路径。网络拓扑规划需确保目标客户端均位于 192.168.1.0/24 网段，且交换机配置允许 PXE 广播报文穿透，此为后续服务联动的基础条件。

2.2 DHCP 服务的配置

动态主机分配协议 (Dynamic Host ConfigurationProtocol，DHCP) 是一个局域网的网络协议，使用 UDP 协议工作，其主要用途为给 LAN 内主机自动分配 IP 地址，也为内部网络管理员提供了对内部主机的管理手段，在局域网中使用非常普遍 [2]。结合国内软硬件情况，在 DHCP 服务的部署中新增多架构自适应特性，能够自动适配不同硬件平台的设备接入，该 DHCP 配置方案以下优点：

1. 智能硬件识别：通过内置的架构检测功能（DHCP Option 93 字段），系统能自动识别客户端是 x86 服务器还是国产鲲鹏 ARM 服务器，并动态分发对应架构的引导文件。

2. 动态安全证书：当检测到鲲鹏设备时，系统会额外发送国密数字证书下载链接（option sm3-cert）。这个证书相当于 " 数字身份证 "，用于后续文件传输时的身份核验和安全加密，极大的保证了信息安全。

2.3 TFTP 传输引导文件

TFTP 用于传输 grubx64.efi、vmlinuz、initrd.img 启动引导文件，OpenEuler 通过深度整合国产硬件密码引擎，在 TFTP 服务层实现了革命性的安全传输加速。本方案于将国密算法 SM3 的校验计算过程形成软件与硬件协同的安全传输体系。具体实现分为两个关键阶段：在文件准备阶段，执行 openssl sm3 -engine capi 指令生成硬件签名的校验文件，其中 -engine capi 参数显式调用鲲鹏芯片的密码加速能力；在服务运行阶段，通过定制化的 tftpd-secure.service 服务单元，设置 -m sm3_hw 启动参数启用硬件强制校验模式，并配置 OPENSSL_ENGINES=/usr/lib64/engines-1.1/capi.so 环境变量定向加载密码加速模块。

2.4 基于 Nginx 的安装源配置

在本文研究的 PXE 自动化部署系统中，Nginx 作为高性能 HTTP 服务器承担着关键的文件分发功能。Nginx 是一款高性能的开源 Web 服务器和反向代理服务器。它在处理静态资源、负载均衡、反向代理、HTTPS 等方面表现出色。Nginx 的设计目标是提供高性能、稳定性、热部署、模块化设计、低资源消耗和灵活性，以适应于现代网络环境中构建大规模访问、可伸缩性强的 Web 应用和负载的需求 [3]。本方案通过 Nginx 将系统镜像文件分发至客户端服务器中。

2.5 OpenEuler 的 Kickstart 配置

Kickstart 是 Red Hat 系列 Liunx 发行版提供自动化操作按照技术，它通过预定义的配置文件实现自动部署系统。Ks.cfg 文件作为核心配置包含了安装过程中所需要的所有配置参数，完全避免了传统安装方式中繁琐的人工交互操作。主要分为三个板块：

1. 命令部分：系统基础配置框架

Kickstart 配置文件中的命令部分构成了系统安装的基础框架，通过简洁的声明式语法定义关键系统参数。在网络配置方面，支持静态 IP（network --ip=x.x.x.x

--netmask=255.255.255.0）和 DHCP 自动获取（network --bootproto=dhcp）两种模式，并可指定 DNS 服务器和网关等高级网络参数。可选安全策略配置，auth --enableshadow --passalgo=sha512 指令不仅启用 shadow 密码机制，还强制使用 SHA-512 算法进行密码哈希，在 OpenEuler 等国产系统中更支持 SM3 国密算法替代。系统本地化设置则通过 lang zh_CN.UTF-8、keyboard cn 等命令实现中文环境适配，而 timezone Asia/Shanghai --ntpservers=ntp.aliyun.com 则确保时区和时间同步服务符合国内使用场景。

2. 软件包管理：精准控制系统组成

%packages 模块提供了细粒度的软件生态控制能力。通过 @^minimal-environment 可安装最小化基础系统，而 @development 则包含完整的开发工具链。在实际部署中，管理员可以精确指定软件包版本（如 kernel-4.18.0-348.el8），并通过 --exclude=firefox* 排除不需要的组件。在国产化环境中，通常会添加 openssl-gm 等国密算法支持包和 kylin-sec-tools 等安全增强工具。该模块还支持条件化安装，例如针对鲲鹏处理器的优化包组可以通过 %ifarch aarch64 条件判断来加载，实现硬件适配的智能化管理。

3. 脚本扩展：部署流程的弹性扩展

%pre 和 %post 脚本段为安装过程提供了强大的扩展能力。%pre 脚本在磁盘分区前执行，运行于内存虚拟环境（tmpfs）中，常用于硬件特征检测和环境准备。典型的应用包括：通过 lspci | grep -i raid 识别硬件 RAID 卡型号，动态生成适配的分区方案；或者基于 dmidecode 输出判断服务器机型，选择不同的内核参数。%post 脚本则在系统安装完成后执行，具有完整的系统环境支持，主要承担三大职责：安全加固（如配置 fail2ban 和 selinux 策略）、业务环境初始化（部署容器运行时或 Kubernetes 组件）。此外，可通过 %include 指令实现模块化设计，大大提升了复杂部署场景的灵活性。

2.6 GRUB 引导

在 Linux 操作系统中，GRUB（GRand Unified Bootloader）是一个多操作系统启动程序，它允许用户在系统启动时提供选择不同的操作系统或内核，它作为 PXE 自动化部署流程中的起点，连接硬件与软件桥梁。会在硬件自检完成后立即接管控制权，负责加载 Linux 内核和 initramfs 初始化内存盘，能够将安装源位置、自动化配置脚本路径等关键信息准确传递给安装程序。配置文件如下所示：

```
# /var/lib/tftpboot/grub2/grub.cfg
set timeout=10
menuentry “Install openEuler” {
 linuxefi /vmlinuz inst.repo=https://192.168.1.10/openeuler inst.ks=http://192.168.1.10/ks.cfg
 initrdefi /initrd.img
}
```

menuentry 部分定义了一个名为”Install openEuler”的安装选项，其中 linuxefi 指令指定了要加载的内核镜像文件 /vmlinuz，并通过 inst.repo 参数设置系统安装源的位置为 http://192.168.1.10/openeuler，同时使用 inst.ks 参数指定 Kickstart 自动安装配置文件的网络位置。这些核心参数的组合确保了系统能够从指定位置获取安装所需的全部资源。

initrdefi 指令则负责加载初始化内存盘文件 /initrd.img，这个文件包含了安装过程所需的核心驱动和工具，为系统安装初期提供了临时的运行环境。配合 DHCP 和 TFTP 服务共同实现网络启动安装的全过程。

3 行业应用实践

在某云平台建设项目中，需在 40 台清华 DL360 国产服务器部署 OpenEuler 操作系统任务，该批期服务器配置为 E5-2630V4 处理器、256GB 内存和 4TB NVMe SSD 存储。因业务特殊，不能使用 U 盘等移动工具。传统单台手动安装模式需要依赖外置光驱镜像人工安装影响安装效率，单节点安装平均耗时 90 分钟（包含硬件识别、系统安装和预装运行环境等环节），极大的拖延了项目的进展。

这些挑战迫切需要我们搭建一套高效、可靠的批量部署解决方案。于是涉及了基于 OpenEuler 操作系统的 PXE 网络启动方案，本方案取得了显著的效率提升和质量改进。在效率指标方面，40 台服务器的总部署时间压缩至 240 分钟，较传统单台部署模式实现了 15 倍的效率提升。

4 结语

本次基于 PXE 批量部署国产操作系统 OpenEuler 方案的成功实践，极大的简化的大规模服务器集群的安装部署工作，该方案不仅实现了部署效率的飞跃提升（40 台服务器 4 小时完成），更在安全性、一致性和国产化兼容方面具有较高水平。为国产化操作系统部署提供了可靠的技术支撑。

5 后续展望

5.1 生态扩展规划

硬件生态适配将向更广泛的国产平台延伸，例如飞腾 Phytium S2500 和龙芯 3A5000 等主流国产处理器。通过建立标准化的驱动兼容性测试体系和国产硬件驱动认证仓库，最终实现 " 一键式 " 部署支持所有主流国产服务器。这一扩展将大幅提升方案的通用性和适用性。

5.2 云原生发展路线

云原生集成将重点深化与 Kubernetes 生态的融合，开发集群化部署功能模块。以 ansible 作为管理手段针对边缘计算场景，将优化轻量级部署方案，满足 5G 和物联网设备的快速扩展需求。这一发展将使方案更好地适应云计算和边缘计算的新兴应用场景。

参考文献

[1] 王玉峰，李文志. 计算机实验室无盘化改造［J］. 科技视界，2016 (1) : 46

[2] 李澍,姚磊.实验室搭建复杂网络环境下的DHCP服务及安全防护[J].实验室研究与探索,2014,33(01):143-148.

[3] 杨文军,薛燕娜.基于Nginx+sticky实现cookie负载均衡的建设与研究[J].电脑知识与技术,2024,20(19):97-100.DOI:10.14004/j.cnki.ckt.2024.1072.