

本文使用 pxe 自动安装技术进行大规模裸机（物理机与虚拟机）安装部署 linux 系统。

本系统合集目标

1. 降低新手门槛，可以从更高的技术平台起步
2. 节约专业人员时间，把时间专注于高水准技术
3. 降低系统基础设施维护和安全防护成本

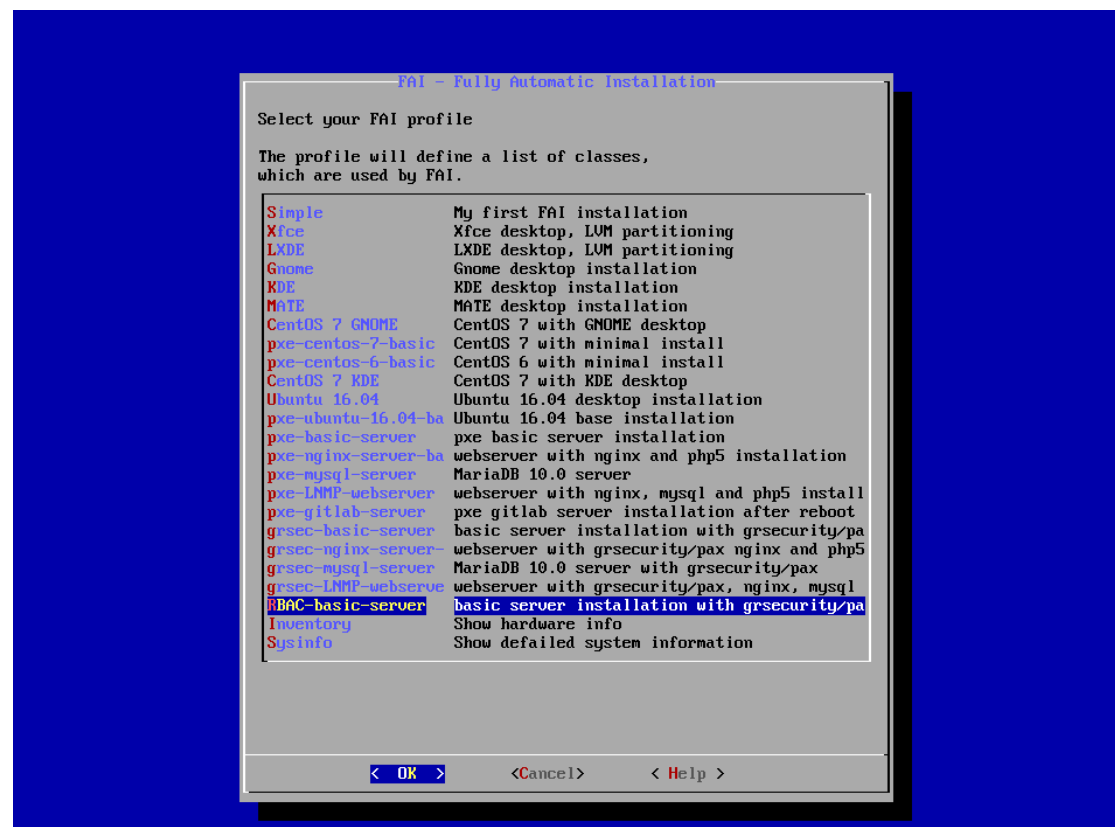
使用要求：

局域网需要 DHCP，安装过程保持网络畅通，否则无法更新，以及部分模板会安装失败。

大规模安装方式：光盘安装 fai-server 作为安装服务器，然后配置 pxe 服务，配置安装源代理服务，完成后其他主机设置 bios 网卡 pxe 启动从 fai-server 批量安装系统。

提供可启动光盘 ISO 镜像，用于单机安装。

当前支持系统及配置模板



一．原版系统

用户名 demo 密码 fai 用户名 root 密码 fai

Dedbian8 原版基本系统，XFCE 桌面，LXDE 桌面，GNOME 桌面，KDE 桌面，MATE 桌面

Ubuntu 14.04 原版基本系统

Ubuntu 16.04 原版桌面 Unity

二．定制系统

菜单选项：pxe 前缀 用户名 huserpwd 密码 huser 用户名 root 密码 rootpwd 性能调优，部分配置增强，安全改进

Centos6 定制基本系统

Centos7 定制基本系统，GNOME 桌面环境，KDE 桌面环境

Dedbian8 定制基本系统，Mysql 服务器，web 后端（LNP），web 服务器（LNMP）

Ubuntu 14.04 定制基本系统

Ubuntu 16.04 定制基本系统

三．安全加固系统

在定制系统基础上，启用 grsecurity/pax 加固内核，初始系统未启用 RBAC，仅支持 DAC 自主访问控制，制作配置 RBAC 规则后，才能达到最高安全等级（以下第四类）。

菜单选项：grsec 前缀

用户名 hmuser 密码 hmuserpwd 用户名 root 密码 rootpwd

Dedbian8 grsecurity 安全加固基本系统, Mysql 服务器, web 后端(LNP), web 服务器(LNMP)

四．安全加固系统 启用 RBAC 角色访问控制 目标具备实用价值的高级安全系统

在上述 grsecurity/pax 安全系统基础上，进一步启用 RBAC 角色访问控制，默认就是最高安全防护级别。

菜单选项 RBAC 前缀

用户名 hmuser 密码 hmuserpwd 用户名 root 密码 rootpwd

RBAC 访问控制规则密码：rbacpwd

RBAC 管理员角色 admin 密码：adminpwd

RBAC 管理员角色（仅关闭和重启操作系统）shutdown 密码：shutdownpwd

Dedbian8 grsecurity 安全加固基本系统 启用角色访问控制规则，无差别严格管制系统中每个用户每个程序的行为，取消 root 用户特权，对抗各种未知内存溢出漏洞，对抗 root 提权，缓解或者消除木马与后门威胁。

支持秘密审计记录系统中用户行为，确保记录机制无法被发现，无法逃脱。

内置 RBAC 规则集可以用于保生产环境安全 nginx, apache, php, nfs, openvpn, sshd, rsyslog 等。

Debian 系列是本光盘合集作者生产环境服务器部署的系统，各种先进特性予以优先支持，包括 grsecurity 内核与 RBAC，bcc-tools 动态追踪。