**Ubuntu服务器指南**

**Ubuntu服务器指南**

版权所有©2018本文件的贡献者

### 摘要

欢迎来到Ubuntu服务器指南！它包含如何在Ubuntu系统上安装和配置各种服务器应用程序以满足您的需要的信息。这是一个循序渐进、面向任务的指南，用于配置和自定义系统。

### 信用证和执照

本文档由Ubuntu文档团队维护(https://wiki.ubuntu.com/DocumentationTeam). 贡献者名单如下。

本文档在知识共享共享共享3.0许可证（CC-BY-SA）下提供。

您可以根据本许可证的条款自由修改、扩展和改进Ubuntu文档源代码。所有衍生作品必须根据本许可证发布。

分发本文件的目的是希望它有用，但不提供任何担保；甚至没有免责声明中所述的适销性或特定用途适用性的暗示保证。

许可证副本可在此处获得：Creative Commons ShareAlike许可证[1]。

本文件的作者包括：

•Ubuntu文档项目的成员[2]

•Ubuntu服务器团队成员[3]

•社区帮助维基的贡献者[4]

•其他贡献者可以在Launchpad上提供的serverguide[5]和ubuntu docs[6]bzr分支的修订历史中找到。

### 目录

1.       介绍1.

1.   支持2.

2.       安装3.

1.   准备安装。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。4.

2.   使用live server安装程序安装。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。6.

3.   使用debian安装程序安装。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。8.

4.   升级。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。11

5.   高级安装。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。12

6.   内核崩溃转储。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。21

3.       包装管理。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。27

1.   介绍28

2.   dpkg。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。29

3.   恰当的30

4.   资质32

5.   自动更新。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。34

6.   配置36

7.   参考文献。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。38

4.       网络。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。39

1.   网络配置。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。40

2.   TCP/IP协议。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。48

3.   动态主机配置协议（DHCP）。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。52

4.   时间同步。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。55

5.   数据平面开发工具包。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。60

5.       DM多路径。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。75

1.   设备映射器多路径。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。76

2.   多路径设备。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。79

3.   设置DM多路径概述。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。82

4.   DM多路径配置文件。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。86

5.   DM多路径管理和故障排除。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。98

6.       远程给药。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。103

1.   OpenSSH服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。104

2.   木偶107

3.   Zentyal。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。110

7.       网络认证。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。114

1.   OpenLDAP服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。115

2.   Samba和LDAP。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。140

3.   Kerberos。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。146

4.   Kerberos和LDAP。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。154

5.   SSSD和Active Directory。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。161

8.       域名服务（DNS）。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。166

Ubuntu服务器指南

1.   安装167

2.   配置168

3.   故障排除。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。174

4.   参考文献。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。178

9.       安全179

1.   用户管理。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。180

2.   控制台安全性。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。186

3.   防火墙。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。187

4.   公寓。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。194

5.   证书。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。198

6.   eCryptfs。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。203

10.   监测。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。205

1.   概述206

2.   纳吉奥斯。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。207

3.   穆宁。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。211

11.   网络服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。213

1.   HTTPD-Apache2 Web服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。214

2.   PHP-脚本语言。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。221

3.   Squid-代理服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。223

4.   Ruby on Rails。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。226

5.   Apache Tomcat。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。228

12.   数据库。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。232

1.   MySQL。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。233

2.   PostgreSQL。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。237

13.   灯具应用。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。240

1.   概述241

2.   莫因莫因。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。242

3.   phpMyAdmin。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。244

4.   WordPress。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。246

14.   文件服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。248

1.   FTP服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。249

2.   网络文件系统（NFS）。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。253

3.   iSCSI启动器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。255

4.   CUPS-打印服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。258

15.   电子邮件服务。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。261

1.   后缀。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。262

2.   Exim4。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。270

3.   多佛科特服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。273

4.   邮递员。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。275

5.   邮件过滤。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。281

16.   聊天应用程序。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。288

1.   概述289 Ubuntu服务器指南

2.   IRC服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。290

3.   Jabber即时消息服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。292

17.   版本控制系统。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。294

1.   集市295

2.   吉特。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。296

3.   颠覆。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。299

4.   参考文献。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。304

18.   桑巴。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。305

1.   介绍306

2.   文件服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。307

3.   打印服务器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。310

4.   保护文件和打印服务器的安全。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。312

5.   作为域控制器。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。317

6.   Active Directory集成。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。321

19.   备份。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。323

1.   Shell脚本。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。324

2.   档案轮换。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。328

3.   杆菌。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。331

20.   虚拟化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。336

1.   利比韦特。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。337

2.   Qemu。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。344

3.   云图像和uvtool。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。346

4.   Ubuntu云。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。350

5.   LXD。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。351

6.   LXC。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。362

21.   聚类。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。377

1.   DRBD。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。378

22.   虚拟专用网。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。381

1.   OpenVPN。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。382

23.   其他有用的应用。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。396

1.   帕姆·莫特。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。397

2.   埃切佩尔。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。399

3.   比奥布。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。401

A.附录。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。403

1.报告Ubuntu Server Edition中的错误。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。404

### 表格一览表

2.1. 建议的最低要求。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。4.

5.1. 优先级检查器转换。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。76

5.2. DM多路径组件。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。77

5.3. 多路径配置默认值。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。90

5.4. 多路径属性。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。93

5.5. 设备属性。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。95

5.6. 有用的多路径命令选项。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。101

17.1. 访问方法。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。300

# 第一章。介绍

欢迎来到Ubuntu服务器指南！

在这里，您可以找到有关如何安装和配置各种服务器应用程序的信息。这是一个循序渐进、面向任务的指南，用于配置和自定义系统。

本指南假设您对Ubuntu系统有基本了解。第2章，安装[3页]介绍了一些安装细节，但是如果您需要安装Ubuntu的详细说明，请参阅Ubuntu安装指南[7]。

该手册的HTML版本可在Ubuntu文档网站[8]上在线获取。

介绍

## 1.支持

Ubuntu Server Edition有两种不同的支持方式：商业支持和社区支持。主要的商业支持（和开发资金）可从Canonical，Ltd.获得。他们以每台台式机或每台服务器为基础提供价格合理的支持合同。有关更多信息，请参阅Ubuntu Advantage[9]页面。

社区支持也由致力于使Ubuntu成为最佳发行版的个人和公司提供。通过多个邮件列表、IRC频道、论坛、博客、Wiki等提供支持。大量可用信息可能会让人不知所措，但一个好的搜索引擎查询通常可以为您的问题提供答案。有关更多信息，请参见Ubuntu支持[10]页。

# 第二章。安装

本章简要介绍如何安装Ubuntu18.04 LTS服务器版。有关更详细的说明，请参阅Ubuntu安装指南[11]。

## 1.准备安装

本节说明在开始安装之前要考虑的各个方面。

#### 1.1. 系统要求

Ubuntu 18.04 LTS Server Edition支持四（4）种主要架构：AMD64、ARM、POWER8、LinuxONE和z系统（尽管本手册不包括LinuxONE或z系统的安装，请参阅专用指南[12]）。

UbuntuServer18.04LTS引入了一个新的安装程序，“live Server”安装程序（有时称为“Ubiquity for Servers”或简称为“subiquity”），它提供了更友好、更快的安装体验。在编写本文时，它仅支持amd64处理器，不支持LVM或RAID或其他更复杂的存储选项，也不支持重用正在安装的系统磁盘上的现有分区。它还需要访问Ubuntu存档，可能通过代理。如果这些限制意味着您不能使用live server安装程序，那么以前的基于debian安装程序的安装程序仍然可用。

下表列出了推荐的硬件规格。根据您的需要，您可以使用比这更少的资源进行管理。然而，如果忽视这些建议，大多数用户可能会感到沮丧。

##### **表2.1。建议的最低要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **安装类型** | **安装方法** | **中央处理器** | **内存** | **硬盘空间** | |
| **基本系统** | **已安装的所有任务** |
| 服务器  （标准） | debian安装程序 | 1千兆赫 | 512兆字节 | 1.5千兆字节 | 2.5千兆字节 |
| 实时服务器 | 1千兆赫  （仅限amd64） | 1G字节 | 1.5千兆字节 | 不适用 |
| 服务器  （最低限度） | debian安装程序 | 300兆赫 | 384兆字节 | 1.5千兆字节 | 2.5千兆字节 |

服务器版为各种服务器应用程序提供了一个公共基础。它是一种极简设计，为所需的服务提供了一个平台，如文件/打印服务、web托管、电子邮件托管等。

#### 1.2. 服务器和桌面差异

Ubuntu服务器版和Ubuntu桌面版之间有一些区别。应该注意的是，两个版本使用相同的apt存储库，这使得在桌面版上安装服务器应用程序与在服务器版上安装服务器应用程序一样容易。

这两个版本之间的区别在于服务器版本和安装过程中缺少X窗口环境。

1.2.1. 内核差异：

Ubuntu版本10.10和之前的版本实际上在服务器和桌面版本上有不同的内核。Ubuntu不再有单独的服务器和通用内核风格。这些已经被合并到一个单一的通用内核风格中，以帮助减少版本生命周期中的维护负担。

在64位处理器上运行64位版本的Ubuntu时，您不受内存寻址空间的限制。

要查看所有内核配置选项，可以查看/boot/config-4.14.0-server。此外，简单地说，Linux内核[13]是关于可用选项的一个很好的资源。

#### 1.3. 备份

•在安装Ubuntu Server Edition之前，您应该确保系统上的所有数据都已备份。有关备份选项，请参见第19章备份[p.323]。

如果这不是第一次在您的计算机上安装操作系统，那么您可能需要重新分区磁盘，为Ubuntu腾出空间。

无论何时对磁盘进行分区，如果在分区过程中出错或出现问题，您都应该准备好丢失磁盘上的所有内容。安装中使用的程序非常可靠，大多数都使用了多年，但它们也执行破坏性操作。

## 2.使用live server安装程序安装

安装Ubuntu Server Edition的基本步骤与安装任何操作系统的步骤相同。

与桌面版不同，服务器版不包括图形安装程序。Live Server安装程序使用在默认虚拟控制台上运行的基于文本的控制台界面。该界面可以完全由回车键、上下箭头键（偶尔输入）驱动。

如果在安装过程中需要随时切换到其他控制台（通过按Ctrl-AltF<n>或Ctrl-Alt-Right）以访问shell。在安装开始之前，您可以使用“后退”按钮返回到以前的屏幕并选择不同的选项。

•从Ubuntu网站下载适当的ISO文件[14]。

•从包含ISO文件的介质（如USB密钥）引导系统。

•在启动提示下，将要求您选择一种语言。

•在主引导菜单中，有一些附加选项可用于安装Ubuntu Server Edition。你可以安装一个基本的Ubuntu服务器，检查安装介质是否有缺陷，检查系统的RAM，或者从第一个硬盘启动。本节的其余部分将介绍基本的Ubuntu服务器安装。

•引导到安装程序后，它会询问您使用哪种语言。

•接下来，安装过程从询问键盘布局开始。您可以要求安装程序尝试自动检测，也可以从列表中手动选择。安装的后续阶段将要求您键入ASCII字符，因此，如果您选择的布局不允许输入ASCII字符，系统将提示您输入一个组合键，以便在允许输入的布局和您选择的布局之间切换。此操作的默认按键为Alt+Shift。

•接下来，安装程序可以选择将系统安装为普通Ubuntu服务器、MAAS[15]裸机云机架控制器或MAAS[16]区域控制器。如果您选择一个MAAS选项，系统将询问您一些详细信息。

•安装程序将网络配置为在每个网络接口上运行DHCP。如果这不足以访问internet，则应手动配置至少一个接口。选择一个接口来配置它。

•如果Ubuntu归档文件只能通过您环境中的代理访问，则可以在下一个屏幕上输入。如果不需要，请将该字段留空。

•然后，您可以选择让安装程序使用整个磁盘或手动配置分区。您在其上创建分区的第一个磁盘将被选择为引导磁盘，并在其上创建一个额外的分区以包含引导加载程序；您可以使用“选择为引导磁盘”按钮将引导分区移动到其他驱动器。

一旦您从此屏幕继续，安装过程将开始。无法移回此屏幕或以前的屏幕，并且您配置安装程序使用的磁盘上的任何数据都将丢失。

•下一个屏幕配置系统的初始用户。您可以从启动板或导入SSH密钥

但是仍然需要设置密码，因为此用户将通过sudo实用程序具有root访问权限。

•最终屏幕显示安装程序的进度。安装完成后，系统将提示您重新启动新安装的系统。

## 3.使用debian安装程序进行安装

安装Ubuntu Server Edition的基本步骤与安装任何操作系统的步骤相同。与桌面版不同，服务器版不包括图形安装程序。debianinstaller安装程序使用基于控制台菜单的过程。

•从Ubuntu网站下载适当的ISO文件[17]。

•从包含ISO文件的介质（如USB密钥）引导系统。

•在启动提示下，将要求您选择一种语言。

•在主引导菜单中，有一些附加选项可用于安装Ubuntu Server Edition。你可以安装一个基本的Ubuntu服务器，检查CD-ROM的缺陷，检查系统的RAM，从第一个硬盘引导，或者拯救一个坏了的系统。本节的其余部分将介绍基本的Ubuntu服务器安装。

•安装程序询问应使用哪种语言。之后，您将被要求选择您的位置。

•接下来，安装过程从询问键盘布局开始。您可以要求安装程序尝试自动检测，也可以从列表中手动选择。

•然后安装程序会发现您的硬件配置，并使用DHCP配置网络设置。如果您不希望在下一个屏幕上使用DHCP，请选择“返回”，您可以选择“手动配置网络”。

•接下来，安装程序询问系统的主机名。

•设置新用户；此用户将通过sudo实用程序具有root访问权限。

•完成用户设置后，系统会询问您是否要加密主目录。

•接下来，安装程序询问系统的时区。

•然后，您可以从多个选项中选择以配置硬盘驱动器布局。之后，系统会询问您要安装到哪个磁盘。根据磁盘布局，您可能会在重写分区表或设置LVM之前收到确认提示。如果选择LVM，将询问根逻辑卷的大小。有关高级磁盘选项，请参阅第5节“高级安装”[p.12]。

•然后安装Ubuntu基本系统。

•安装过程的下一步是决定如何更新系统。有三种选择：

•：这需要管理员登录计算机并手动安装更新。*没有自动更新*

•：这将安装无人值守升级包，该包将在无需管理员干预的情况下安装安全更新。有关更多详细信息，请参见第5节“自动更新”[p.34]。*自动安装安全更新*

•：景观是Canonical提供的一项付费服务，帮助管理您的Ubuntu机器。有关详细信息，请参见景观[18]网站。*用景观管理系统*

•您现在可以选择安装或不安装多个软件包任务。有关详细信息，请参见第3.1节“一揽子任务”[p.9]。此外，还可以选择启动aptitude来选择要安装的特定软件包。更多信息请参见第4节“能力倾向”[p.32]。

•最后，重新启动前的最后一步是将时钟设置为UTC。

如果在安装过程中的任何时候您对默认设置不满意，请在任何提示下使用“返回”功能，以进入详细的安装菜单，允许您修改默认设置。

在安装过程中的某些时候，您可能需要阅读安装系统提供的帮助屏幕。要执行此操作，请按F1。

同样，有关详细说明，请参阅Ubuntu安装指南[19]。

#### 3.1. 包任务

在Server Edition安装期间，您可以选择安装其他软件包。软件包按其提供的服务类型进行分组。

•DNS服务器：选择绑定DNS服务器及其文档。

•LAMP服务器：选择现成的Linux/Apache/MySQL/PHP服务器。

•邮件服务器：此任务选择对通用邮件服务器系统有用的各种包。

•OpenSSH服务器：选择OpenSSH服务器所需的包。

•PostgreSQL数据库：此任务为PostgreSQL数据库选择客户端和服务器包。

•打印服务器：此任务将您的系统设置为打印服务器。

•Samba文件服务器：此任务将您的系统设置为Samba文件服务器，特别适用于Windows和Linux系统的网络。

•Tomcat Java服务器：安装Apache Tomcat和所需的依赖项。

•虚拟机主机：包括运行KVM虚拟机所需的包。

•手动选择软件包：执行aptitude，允许您单独选择软件包。

使用tasksel实用程序完成软件包组的安装。Ubuntu（或Debian）和其他GNU/Linux发行版之间的一个重要区别是，在安装时，软件包也被配置为合理的默认值，最终会提示您提供所需的其他信息。同样，在安装任务时，不仅要安装包，还要配置包以提供完全集成的服务。

安装过程完成后，您可以通过在终端提示符下输入以下内容来查看可用任务的列表：

**tasksel——列出任务**

输出将列出其他基于Ubuntu的发行版（如Kubuntu和Edubuntu）的任务。请注意，您也可以自行调用tasksel命令，这将显示不同可用任务的菜单。

您可以使用--task packages选项查看随每个任务一起安装的包的列表。例如，要列出与DNS服务器任务一起安装的包，请输入以下内容：命令的输出应列出：**tasksel--任务包dns服务器**

bind9文件bind9utils bind9

如果您在安装过程中未安装其中一个任务，但您决定将新LAMP服务器也设为DNS服务器，只需插入安装介质并从终端：

**sudo tasksel安装dns服务器**

## 4.升级换代

有几种方法可以从一个Ubuntu版本升级到另一个Ubuntu版本。本节概述了推荐的升级方法。

#### 4.1. 发布升级吗

升级Server Edition安装的推荐方法是使用do release upgrade实用程序。作为update manager核心包的一部分，它没有任何图形依赖项，默认情况下安装。

基于Debian的系统也可以通过使用apt dist升级进行升级。但是，建议使用do release upgrade，因为它能够处理版本之间有时需要的系统配置更改。

要升级到较新版本，请在终端提示符下输入：**发布升级吗**

也可以使用do release upgrade升级到Ubuntu的开发版本。要完成此操作，请使用-d开关：

**是否发布升级-d**

对于生产环境，不建议升级到开发版本。

为了进一步提高LTS版本的稳定性，如果您当前运行的是LTS版本，则在行为上会有轻微的变化。LTS系统仅自动考虑通过do releaseupgrade与第一个点版本一起升级到下一个LTS。因此，例如14.04只会在16.04.1发布后升级。如果您想在之前进行更新，例如，在计算机子集上评估安装的LTS升级，则必须通过-d开关使用与升级到开发版本相同的参数。

## 5.高级安装

#### 5.1. 软件磁盘阵列

独立磁盘冗余阵列“RAID”是一种使用多个磁盘提供不同平衡以提高数据可靠性和/或提高输入/输出性能的方法，具体取决于所使用的RAID级别。RAID在软件（操作系统知道两个驱动器并积极维护它们）或硬件（特殊控制器使操作系统认为只有一个驱动器并“不可见地”维护驱动器）中实现。

当前版本的Linux（和Ubuntu）中包含的RAID软件基于“mdadm”驱动程序，运行良好，甚至比许多所谓的“硬件”RAID控制器都要好。本节将指导您使用两个物理硬盘上的两个RAID1分区安装Ubuntu Server Edition，一个用于/，另一个用于交换。

##### 5.1.1. 分割

按照安装步骤进行操作，直到进入分区磁盘步骤，然后：

1.         选择手动作为分区方法。

2.         选择第一个硬盘，并同意“在此设备上创建新的空分区表？”。

对希望成为RAID阵列一部分的每个驱动器重复此步骤。

3.         选择第一个驱动器上的“可用空间”，然后选择“创建新分区”。

4.         接下来，选择分区的大小。这个分区将是交换分区，交换大小的一般规则是RAM的两倍。输入分区大小，然后选择主分区，然后选择开始分区。

交换分区大小为可用RAM容量的两倍可能并不总是可取的，尤其是在具有大量RAM的系统上。计算服务器的交换分区大小在很大程度上取决于系统的使用方式。

5.         选择顶部的“使用方式：”行。默认情况下，这是“Ext4日志文件系统”，将其更改为“RAID物理卷”，然后“完成分区设置”。

6.         对于/分区，再次在第一个驱动器上选择“空闲空间”，然后选择“创建新分区”。

7.         使用驱动器上剩余的可用空间，然后选择“继续”，然后选择“主”。

8.         与交换分区一样，选择顶部的“使用方式：”行，将其更改为“RAID物理卷”。同时选择“可引导标志：”行将值更改为“开”。然后选择“完成分区设置”。

9.         对其他磁盘和分区重复步骤3到步骤8。

##### 5.1.2. RAID配置

通过分区设置，可以配置阵列：

1.         回到主“分区磁盘”页面，选择顶部的“配置软件RAID”。

2.         选择“是”将更改写入磁盘。

3.         选择“创建MD设备”。

4.         在本例中，选择“RAID1”，但如果使用不同的设置，请选择适当的类型（RAID0 RAID1 RAID5）。

要使用RAID5，您至少需要三个驱动器。使用RAID0或RAID1只需要两个驱动器。

5.         输入阵列的活动设备“2”的数量或硬盘驱动器的数量。然后选择“继续”。

6.         接下来，默认情况下输入备用设备的数量“0”，然后选择“继续”。

7.         选择要使用的分区。通常为sda1、sdb1、sdc1等。数字通常匹配，不同的字母对应不同的硬盘驱动器。

对于交换分区，选择sda1和sdb1。选择“继续”进入下一步。

8.         对/sda2和sdb2分区重复步骤三到七。

9.         完成后，选择“完成”。

##### 5.1.3. 格式化

现在应该有一个硬盘驱动器和RAID设备的列表。下一步是格式化和设置RAID设备的装载点。将RAID设备视为本地硬盘驱动器，进行相应的格式化和装载。

1.         在“RAID1设备#0”分区下选择“#1”。

2.         选择“用作：”。然后选择“交换区域”，然后选择“完成分区设置”。

3.         接下来，在“RAID1设备#1”分区下选择“#1”。

4.         选择“用作：”。然后选择“Ext4日志文件系统”。

5.         然后选择“装载点”并选择“/-根文件系统”。根据需要更改任何其他选项，然后选择“完成分区设置”。

6.         最后，选择“完成分区并将更改写入磁盘”。

如果选择将根分区放置在RAID阵列上，安装程序将询问您是否希望在降级状态下引导。有关更多详细信息，请参见第5.1.4节“降级RAID”[p.13]。

然后，安装过程将正常继续。

##### 5.1.4. 降级RAID

在计算机生命周期的某个时刻，可能会发生磁盘故障事件。发生这种情况时，操作系统将使用软件RAID将阵列置于所谓的降级状态。

如果阵列因数据损坏而降级，默认情况下Ubuntu Server Edition将在30秒后启动到initramfs。一旦initramfs启动，就会出现15秒的提示，让您可以选择继续启动系统，或者尝试手动恢复。引导到initramfs提示符可能是也可能不是所需的行为，特别是当机器位于远程位置时。可以通过多种方式配置引导到降级阵列：

•dpkg重新配置实用程序可用于配置默认行为，在此过程中，您将被询问与阵列相关的其他设置。如监控、电子邮件警报等。要重新配置mdadm，请输入以下内容：**sudo dpkg重新配置mdadm**

•dpkg重新配置mdadm过程将更改/etc/initramfs tools/conf.d/mdadm配置文件。该文件的优点是可以预先配置系统的行为，也可以手动编辑：

BOOT\_DEGRADED=true

可以使用内核参数覆盖配置文件。

•使用内核参数将允许系统引导到降级阵列：

•服务器启动时，按Shift键打开Grub菜单。

•按e键编辑内核命令选项。

•按下向下箭头以突出显示内核行。

•在行尾添加“bootdegraded=true”（不带引号）。

•按Ctrl+x键启动系统。

系统启动后，您可以修复阵列，有关详细信息，请参阅第5.1.5节“RAID维护”[p.14]，或者由于主要硬件故障将重要数据复制到另一台机器。

##### 5.1.5. RAID维护

mdadm实用程序可用于查看阵列的状态、向阵列添加磁盘、删除磁盘等：

•要查看阵列的状态，请在终端提示符下输入：**sudomdadm-D/dev/md0**

D告诉mdadm显示关于/dev/md0设备的详细信息。用适当的RAID设备替换/dev/md0。

•要查看阵列中磁盘的状态，请执行以下操作：**sudo mdadm-E/dev/sda1**

如果输出非常类似于mdadm-D命令，请为每个磁盘调整/dev/sda1。

•如果磁盘出现故障，需要从阵列中删除，请输入：

**sudomdadm--删除/dev/md0/dev/sda1**

将/dev/md0和/dev/sda1更改为适当的RAID设备和磁盘。

•同样，要添加新磁盘，请执行以下操作：**sudomdadm--添加/dev/md0/dev/sda1**

有时，磁盘可能会变为故障状态，即使驱动器在物理上没有任何问题。通常，从阵列中删除驱动器，然后重新添加驱动器是值得的。这将导致驱动器与阵列重新同步。如果驱动器无法与阵列同步，则表明硬件出现故障。

/proc/mdstat文件还包含有关系统RAID设备的有用信息：

**cat/proc/mdstat**个性：[linear][multipath][raid0][raid1][raid6][raid5][raid4][raid10]md0:active raid1 sda1[0]sdb1[1]10016384块[2/2][UU]

未使用的设备：<none>

以下命令非常适合监视同步驱动器的状态：**手表-n1 cat/proc/mdstat**

按Ctrl+c停止“监视”命令。

如果确实需要更换有故障的驱动器，则在更换并同步驱动器后，需要安装grub。要在新驱动器上安装grub，请输入以下内容：**sudogrub安装/dev/md0**

用适当的阵列设备名称替换/dev/md0。

##### 5.1.6. 资源

RAID阵列的主题是一个复杂的主题，因为可以配置RAID的方式太多了。有关更多信息，请参阅以下链接：

•关于RAID的Ubuntu Wiki文章[20]。

•软件RAID HOWTO[21][22]

•管理Linux12上的RAID

#### 5.2. 逻辑卷管理器（LVM）

逻辑卷管理器（LVM）允许管理员使用一个或多个物理硬盘创建逻辑卷。LVM卷可以在软件RAID分区和驻留在单个磁盘上的标准分区上创建。卷也可以扩展，在需求变化时为系统提供更大的灵活性。

##### 5.2.1. 概述

LVM的力量和灵活性的副作用是更大程度的复杂性。在深入了解LVM安装过程之前，最好先熟悉一些术语。

•物理硬盘、磁盘分区或软件RAID分区格式化为LVM PV。*物理体积（PV）：*

•由一个或多个物理卷组成。可以通过添加更多PV来扩展VG。VG就像一个虚拟磁盘驱动器，从中雕刻出一个或多个逻辑卷。*卷组（VG）：*

•类似于非LVM系统中的分区。LV使用所需的文件系统（EXT3、XFS、JFS等）进行格式化，然后可用于装载和数据存储。*逻辑卷（LV）：*

##### 5.2.2. 安装

作为一个例子，本节介绍在LVM卷上安装带有/srv的Ubuntu Server Edition。在初始安装期间，只有一个物理卷（PV）将是卷组（VG）的一部分。安装后将添加另一个PV，以演示如何扩展VG。

LVM有几个安装选项，“引导-使用整个磁盘并设置LVM”，这也允许您将一部分可用空间分配给LVM，“引导-使用整个磁盘并设置加密LVM”，或手动设置分区并配置LVM。此时，在安装过程中，配置同时具有LVM和标准分区的系统的唯一方法是使用手动方法。

1.         按照安装步骤进行操作，直到进入分区磁盘步骤，然后：

2.         在“分区磁盘”屏幕上选择“手动”。

3.         选择硬盘，然后在下一个屏幕上选择“是”以“在此设备上创建一个新的空分区表”。

4.         接下来，使用您喜欢的文件系统创建标准/引导、交换和/分区。

5.         对于LVM/srv，创建一个新的逻辑分区。然后将“用作”更改为“LVM的物理卷”，然后“完成分区设置”。

6.         现在选择顶部的“配置逻辑卷管理器”，然后选择“是”将更改写入磁盘。

7.         对于下一个屏幕上的“LVM配置操作”，请选择“创建卷组”。为VG输入名称，如vg01或更具描述性的名称。输入名称后，选择为LVM配置的分区，然后选择“继续”。

8.         回到“LVM配置操作”屏幕，选择“创建逻辑卷”。选择新创建的卷组，并输入新LV的名称，例如srv，因为这是预期的装载点。

然后选择一个大小，它可能是完整的分区，因为它以后总是可以扩展的。选择“完成”，你应该回到主“分区磁盘”屏幕。

9.         现在向新LVM添加一个文件系统。在“LVM VG vg01，LV srv”下选择分区，或者选择您选择的任何名称，选择Use as。将文件系统设置为普通，选择/srv作为装载点。完成后，选择“done setting the partition”。

10.      最后，选择“完成分区并将更改写入磁盘”。然后确认更改并继续其余的安装。

有一些有用的实用程序可以查看有关LVM的信息：

•显示有关物理卷的信息。*显示：*

•显示有关卷组的信息。*vgdisplay：*

•显示有关逻辑卷的信息。*lvdisplay：*

##### 5.2.3.扩展卷组

继续以srv作为LVM卷示例，本节介绍添加第二个硬盘、创建物理卷（PV）以及将其添加到卷组（VG）中，扩展逻辑卷srv，最后扩展文件系统。本例假设系统中添加了第二个硬盘。在本例中，该硬盘名为/dev/sdb，我们将整个磁盘用作物理卷（您可以选择创建分区并将其用作不同的物理卷）

在发出以下命令之前，请确保您没有现有的/dev/sdb。如果在非空磁盘上发出这些命令，可能会丢失一些数据。

1.         首先，在终端中创建物理卷执行：

**sudopvcreate/dev/sdb**

2.         现在扩展卷组（VG）：

**sudo vgextend vg01/dev/sdb**

3.         使用vgdisplay查找可用物理扩展数据块-可用PE/大小（您可以分配的大小）。我们假设可用大小为511 PE（相当于2GB，PE大小为4MB），我们将使用全部可用空间。使用您自己的PE和/或可用空间。

逻辑卷（LV）现在可以通过不同的方法进行扩展，我们将只了解如何使用PE来扩展LV：**sudo lvextend/dev/vg01/srv-l+511**

l选项允许使用PE扩展LV，-l选项允许使用Meg、Gig、Tera等字节扩展LV。

4.         即使您应该能够在不首先卸载的情况下扩展ext3或ext4文件系统，但最好还是卸载它并检查文件系统，这样您就不会在想要减少逻辑卷的那一天搞砸（在这种情况下，必须先卸载）。

以下命令适用于EXT3或EXT4文件系统。如果您正在使用另一个文件系统，可能还有其他可用的实用程序。

**sudo umount/srv sudo e2fsck-f/dev/vg01/srv**

e2fsck的-f选项强制检查，即使系统看起来很干净。

5.         最后，调整文件系统的大小：

**sudo resize2fs/dev/vg01/srv**

6.         现在安装分区并检查其大小。

**mount/dev/vg01/srv/srv&&df-h/srv**

##### 5.2.4.资源

•参见Ubuntu Wiki LVM文章[23]。

•有关更多信息，请参阅LVM HOWTO[24]。

•另一篇好文章是在O&apos;Reilly的linuxdevcenter.com网站上使用LVM[25][26]管理磁盘空间。

•有关fdisk的更多信息，请参阅fdisk手册第16页。

#### 5.3.iSCSI

iSCSI协议可用于在连接或不连接硬盘的系统上安装Ubuntu，而iBFT可用于在安装和引导时自动化iSCSI设置。

##### 5.3.1.安装在无盘系统上

无盘iSCSI安装的第一步与第3节“使用debianinstaller安装”[p.8]至“硬盘布局”部分相同。

1.         安装程序将显示带有以下消息的警告：

未检测到磁盘驱动器。如果您知道磁盘驱动器所需的驱动程序的名称，可以从列表中选择。

2.         在列表中选择名为“登录到iSCSI目标”的项目。

3.         系统将提示您输入一个IP地址以扫描iSCSI目标，其中包含地址格式的说明。请输入iSCSI目标位置的IP地址，然后导航到<continue>，然后按Enter键

4.         如果访问iSCSI设备需要身份验证，请在下一字段中提供用户名。

否则将其留空。

5.         如果您的系统能够连接到iSCSI提供程序，则应看到可安装操作系统的可用iSCSI目标的列表。该列表应类似于以下内容：

选择要使用的iSCSI目标。192.168.1.29:3260上的iSCSI目标：[]iqn.2016-03。TrustyS ISCSIT目标：storage.sys0

<返回><继续>

6.         选择要与空格键一起使用的iSCSI目标。使用箭头键导航到要选择的目标。

7.         导航到<Continue>，然后按ENTER键。

如果成功连接到iSCSI目标，系统将提示您[！！]分区磁盘安装菜单。其余过程与连接磁盘上的任何正常安装相同。安装完成后，系统将要求您重新启动。

##### 5.3.2.安装在连接有磁盘的系统上

同样，在连接了一个或多个磁盘的普通服务器上安装iSCSI与第3节“使用debian安装程序安装”[p.8]部分相同，直到我们到达磁盘分区菜单。我们需要执行以下步骤，而不是使用任何引导选择：

1.         导航到手动菜单项

2.         选择配置iSCSI卷菜单项

3.         选择登录到iSCSI目标

4.         系统将提示您输入一个IP地址以扫描iSCSI目标。其中包含地址格式的说明。输入IP地址并导航到<continue>，然后按Enter键

5.         如果访问iSCSI设备需要身份验证，请在下一字段中提供用户名或将其留空。

6.         如果您的系统能够连接到iSCSI提供程序，则应看到可安装操作系统的可用iSCSI目标的列表。该列表应类似于以下内容：

选择要使用的iSCSI目标。192.168.1.29:3260上的iSCSI目标：

[]iqn.2016-03.TrustyS ISSITARGET:storage.sys0

<返回><继续>

7.         选择要与空格键一起使用的iSCSI目标。使用箭头键导航到要选择的目标

8.         导航到<Continue>，然后按ENTER键。

9.         如果成功，您将返回菜单，要求您登录iSCSI目标。导航至“完成”，然后按ENTER键

新连接的iSCSI磁盘将作为前缀为SCSI的设备出现在概述部分。这是您应该选择作为安装磁盘的磁盘。一旦确定，您可以选择任何分区方法。

根据您的系统配置，可能有其他SCSI磁盘连接到系统。在继续安装之前，请非常小心地识别正确的设备。否则，在错误的磁盘上执行安装可能会导致不可逆转的数据丢失。

##### 5.3.3.带iBFT的安装

要在安装和启动时基于iBFT（iSCSI启动固件表）设置iSCSI，请在安装程序提示符处（或在已保存的文件中）附加以下选项：

磁盘检测/ibft/enable=true partman iscsi/iscsi\u auto=true

这应该探测iBFT信息，并在安装过程中相应地配置网络接口和iSCSI目标，并将系统引导（initramfs）配置为也这样做，以便找到根设备。

从2019年6月20日起，netboot映像上的debian安装程序提供了对iBFT的支持，18.04.3点版及更高版本的ISO映像上（预期）也提供了对iBFT的支持。

##### 5.3.4.重新启动到iSCSI目标

此过程特定于您的硬件平台。例如，以下是如何使用iPXE重新启动到iSCSI目标

iPXE>dhcp配置（net0 52:54:00:a4:f2:a9）…正常

iPXE>sanboot iscsi:192.168.1.29:：：iqn.2016-03.信任iscsitarget:storage.sys0

如果该过程成功，您应该会看到Grub菜单出现在屏幕上。

## 6.内核崩溃转储

#### 6.1.导言

内核崩溃转储是指在内核执行中断时复制到磁盘的易失性内存（RAM）内容的一部分。以下事件可能导致内核中断：

•内核恐慌

•不可屏蔽中断（NMI）

•机器检查异常（MCE）

•硬件故障

•人工干预

对于其中一些事件（恐慌、NMI）内核将自动作出反应，并通过kexec触发崩溃转储机制。在其他情况下，需要手动干预以捕获内存。每当发生上述事件之一时，找出根本原因以防止再次发生非常重要。可以通过检查复制内存内容。

#### 6.2.内核崩溃转储机制

当内核死机时，内核依靠kexec机制在系统启动时分配的内存的预保留部分（见下文）中快速重新启动内核的新实例。这允许现有内存区域保持不变，以便安全地将其内容复制到存储。

#### 6.3.安装

使用以下命令安装内核崩溃转储实用程序：**sudo apt安装linux crashdump**

从16.04开始，默认情况下启用内核崩溃转储机制。在安装过程中，将显示以下对话框提示您。除非另有选择，否则将启用kdump机制。

|------------------------|配置kdump工具|------------------------|

| |

| |

|如果选择此选项，将启用kdump工具机制。A|

|仍然需要重新启动才能启用crashkernel内核|

|参数|

| |

|默认情况下是否应该启用kdump工具|

| |

|<Yes><No>|

| | |---------------------------------------------------------------------------|

如果您需要手动启用该功能，您可以使用dpkg reconforme kdump tools命令并对问题回答Yes。您还可以通过包括以下行来编辑/etc/default/kdump tools：

使用\_KDUMP=1

如果在安装linux crashdump软件包后未重新启动，则需要重新启动以激活crashkernel=boot参数。重新启动后，kdump工具将启用并处于活动状态。

如果在重新启动后启用kdump工具，则只需发出kdump config load命令即可激活kdump机制。

#### 6.4.配置

除了本地转储之外，现在还可以使用远程转储功能，使用SSH或NFS协议将内核崩溃转储发送到远程服务器。

##### 6.4.1.本地内核崩溃转储

本地转储是自动配置的，除非选择远程协议，否则将继续使用。存在许多配置选项，并在/etc/default/kdump tools文件中详细记录。

##### 6.4.2.使用SSH协议进行远程内核崩溃转储

要使用SSH协议启用远程转储，必须以以下方式修改/etc/default/kdump工具：

#---------------------------------------------------------------------------------------远程转储设施：#SSH-将接收转储文件和dmesg文件的远程服务器的用户名和主机名。

#SSH#KEY—用于登录远程#服务器的SSH私钥的完整路径。使用kdump config propagate将公钥发送到

#远程服务器

#HOSTTAG—选择在向远程服务器发送文件时，是否将IP地址的主机名用作#时间戳目录的前缀。

#“ip”是默认值。SSH=”ubuntu@kdump-网络崩溃”

唯一必须定义的变量是SSH。它必须包含使用{username}@{remote server}格式的远程服务器的用户名和主机名。

SSH\_KEY可用于提供要使用的现有私钥。否则，kdump config propagate命令将创建新的密钥对。HOSTTAG变量可用于将系统主机名用作要创建的远程目录的前缀，而不是IP地址。

以下示例显示如何使用kdump config propagate创建新密钥对并将其传播到远程服务器：

**sudo kdump配置传播**需要生成新的ssh密钥。。。

无法确定主机“kdump netcrash（192.168.1.74）”的真实性。

ECDSA密钥指纹为SHA256:iMp+5Y28qhbd+tevFCWrEXykDd4dI3yN4OVlu3CBBQ4。是否确实要继续连接（是/否）？是ubuntu@kdump-netcrash的密码：

已将ssh密钥/root/.ssh/kdump\u id\u rsa传播到服务器ubuntu@kdump-网络崩溃

要将公钥成功发送到服务器，需要远程服务器上使用的帐户密码

kdump config show命令可用于确认kdump已正确配置为使用SSH协议：

**kdump配置显示**转储模式：kdump

使用\_KDUMP:1 KDUMP\_SYSCTL:kernel.panic\_on\_oops=1 KDUMP\_COREDIR:/var/crash crashkernel addr:0x2c000000/var/lib/KDUMP/vmlinuz：指向/boot/vmlinuz-4.4.0-10-generic KDUMP initrd:/var/lib/KDUMP/initrd.img的符号链接/var/lib/KDUMP/initrd.img-4.0-10-generic

**宋承宪：ubuntu@kdump-netcrash SSH\_KEY:/root/.SSH/kdump\_id\_rsa HOSTTAG:ip当前状态：准备好kdump**

##### 6.4.3. 使用NFS协议的远程内核崩溃转储

要使用NFS协议启用远程转储，必须按以下方式修改/etc/default/kdump工具：

#NFS—配置为接收崩溃转储的NFS服务器的主机名和装载点。语法必须为{HOSTNAME}:{MOUNTPOINT}#（例如remote:/var/crash）

#NFS=“kdump netcrash:/var/crash”

与SSH协议一样，可以使用HOSTTAG变量将IP地址替换为主机名作为远程目录的前缀。

kdump config show命令可用于确认kdump已正确配置为使用NFS协议：

**kdump配置显示**转储模式：kdump

使用\_KDUMP:1 KDUMP\_SYSCTL:kernel.panic\_on\_oops=1 KDUMP\_COREDIR:/var/crash crashkernel addr:0x2c000000/var/lib/KDUMP/vmlinuz：指向/boot/vmlinuz-4.4.0-10-generic KDUMP initrd:/var/lib/KDUMP/initrd.img的符号链接/var/lib/KDUMP/initrd.img-4.4.0-10-generic NFS:KDUMP netcrash:/var/crashHOSTTAG:hostname当前状态：准备好kdump

#### 6.5. 验证

要确认内核转储机制已启用，有几件事需要验证。首先，确认crashkernel boot参数存在（注意：以下行已拆分为两行，以适合本文档的格式：

**cat/proc/cmdline**

BOOT\_IMAGE=/vmlinuz-3.2.0-17-server root=/dev/mapper/PreciseS root-ro-crashkernel=384M-2G:64M，2G-:128M

crashkernel参数具有以下语法：

crashkernel=<range1>：<size1>，<range2>：<size2>，…][@offset]range=start-[end]“start”是包含的，“end”是独占的。

因此，对于在/proc/cmdline中找到的crashkernel参数，我们将得到：crashkernel=384M-2G:64M，2G-：128M

上述值表示：

•如果闸板小于384M，则不要保留任何东西（这是“救援”案例）

•如果RAM大小在386M和2G之间（不含），则保留64M

•如果RAM大小大于2G，则保留128M

其次，通过执行以下操作，验证内核是否为kdump内核保留了请求的内存区域：

**dmesg | grep-i崩溃**

...

[0.000000]在800MB时为crashkernel保留64MB内存（系统RAM:1023MB）

最后，如前所述，kdump config show命令显示kdump工具配置的当前状态：

kdump config show DUMP\_模式：kdump

使用\_KDUMP:1 KDUMP\_SYSCTL:kernel.panic\_on\_oops=1 KDUMP\_COREDIR:/var/crash crashkernel addr:0x2c000000/var/lib/KDUMP/vmlinuz：指向/boot/vmlinuz-4.4.0-10-generic KDUMP initrd:/var/lib/KDUMP/initrd.img的符号链接：指向/var/lib/KDUMP/initrd.img-4.4.0-10-generic当前状态：准备好进行KDUMP初始化

kexec command:/sbin/kexec-p--command-line=“BOOT\_IMAGE=/vmlinuz-4.4.0-10-generic root=/dev/mapper/livits--vg root ro debug break=init console=ttys0115200 irqpoll maxcpus=1 nousb systemd.unit=kdump tools.service”--initrd=/var/lib/kdump/initrd.img/var/lib/kdump/vmlinuz

#### 6.6.测试碰撞卸载机制

测试崩溃转储机制将导致系统重新启动。在某些情况下，如果系统负载较重，这可能会导致数据丢失。如果要测试该机制，请确保系统处于空闲状态或负载很轻。

通过查看/proc/sys/kernel/SysRQ kernel参数的值，验证是否启用了SysRQ机制：**cat/proc/sys/kernel/sysrq**

如果返回的值为0，则转储然后重新启动功能将被禁用。大于1的值表示启用了sysrq功能的子集。有关选项和默认值的详细说明，请参阅/etc/sysctl.d/10-magic-sysrq.conf。启用转储然后使用以下命令重新启动测试：**sudo sysctl-w kernel.sysrq=1**

完成此操作后，您必须成为root用户，因为仅使用sudo是不够的。作为root用户，您必须发出命令echo c>/proc/sysrq trigger。如果您使用的是网络连接，您将失去与系统的联系。这就是为什么在连接到系统控制台时进行测试更好的原因。

这具有使内核转储进程可见的优点。

典型的测试输出应如下所示：

**sudo-s**

ubuntu的[sudo]密码：

#echo c>/proc/sysrq触发器

[31.659002]SysRq:Trigger a crash[31.659749]错误：无法在（NULL）[31.662668]IP:[<ffffffff8139f166>]SysRq\_handle\_crash+0x16/0x20[31.662668]PGD 3bfb9067 PUD 368a7067 PMD 0[31.662668]Oops:0002[#1]SMP[31.662668]CPU 1。。。。

输出的其余部分被截断，但您应该看到系统正在重新启动，并且在日志的某个地方，您将看到以下行：

开始：从内核崩溃中保存vmcore。。。

完成后，系统将重新启动到其正常操作模式。然后，您将在/var/Crash目录中找到内核崩溃转储文件和相关子目录：

**ls/var/crash**201809240744 kexec\_cmd linux-image-4.15.0-34-generic-201809240744.crash

如果由于OOM（内存不足）错误导致转储无法工作，请尝试通过编辑/etc/default/grub.d/kdump-tools.cfg来增加保留内存量。例如，要保留512兆字节：

GRUB\_CMDLINE\_LINUX\_DEFAULT=“$GRUB\_CMDLINE\_LINUX\_DEFAULT crashkernel=384M-:512M”运行sudo update GRUB，然后重新启动，然后再次测试。

#### 6.7.资源

内核崩溃转储是一个庞大的主题，需要对linux内核有很好的了解。您可以在此处找到有关该主题的更多信息：

•Kdump内核文档[27]。

•碰撞工具[28]

•分析Linux内核崩溃[29]（基于Fedora，它仍然提供了内核转储分析的良好演练）

# 第三章包装管理

Ubuntu拥有一个全面的软件包管理系统，用于安装、升级、配置和删除软件。除了为您的Ubuntu计算机提供对45000多个软件包的访问外，软件包管理设施还具有依赖项解析功能和软件更新检查。

有几种工具可用于与Ubuntu的软件包管理系统交互，从简单的命令行实用程序（系统管理员可以轻松实现自动化）到简单的图形界面（Ubuntu新手可以轻松使用）。

## 1.导言

Ubuntu的软件包管理系统源自Debian GNU/Linux发行版使用的同一系统。软件包文件包含在Ubuntu计算机上实现特定功能或软件应用程序所需的所有文件、元数据和指令。

Debian软件包文件的扩展名通常为“.deb”，通常存在于存储库中，这些存储库是在各种媒体（如CD-ROM光盘）上或在线上找到的软件包的集合。软件包通常采用预编译的二进制格式；因此安装速度快，无需编译软件。

许多复杂的软件包使用依赖项。依赖项是主体软件包为正常运行所需的附加软件包。例如，语音合成软件包festival依赖于软件包libasound2，该软件包提供音频播放所需的ALSA音库。为了使festival正常运行，它需要必须安装它的所有依赖项。Ubuntu中的软件管理工具将自动完成这项工作。

## 2.dpkg

dpkg是基于Debian的系统的软件包管理器。它可以安装、删除和生成软件包，但与其他软件包管理系统不同，它不能自动下载和安装软件包或其依赖项。本节介绍使用dpkg管理本地安装的软件包：

•从终端提示类型列出系统上安装的所有软件包：**dpkg-l**

•根据您系统上的软件包数量，这可能会产生大量输出。通过grep传输输出以查看是否安装了特定的软件包：**dpkg-l| grep apache2**

用任何包名、包名的一部分或其他正则表达式替换apache2。

•要列出软件包（在本例中为ufw软件包）安装的文件，请输入：**dpkg-L ufw**

•如果您不确定哪个软件包安装了文件，dpkg-S可能会告诉您。例如：

**dpkg-S/etc/host.conf**基本文件：/etc/host.conf

输出显示/etc/host.conf属于基本文件包。

许多文件是在包安装过程中自动生成的，即使它们位于文件系统中，dpkg-S也可能不知道它们属于哪个包。

•您可以通过输入以下内容安装本地.deb文件：**sudo dpkg-i zip\_3.0-4\_i386.deb**

将zip\_3.0-4\_i386.deb更改为要安装的本地.deb文件的实际文件名。

•卸载软件包可以通过以下方式完成：**sudo dpkg-r拉链**

在大多数情况下，不建议使用dpkg卸载程序包。最好使用处理依赖项的程序包管理器，以确保系统处于一致状态。例如，使用dpkg-r zip将删除zip程序包，但依赖它的任何程序包仍将被安装，并且可能不再正常运行。

有关更多dpkg选项，请参阅手册页：man dpkg。

## 3.Apt

apt命令是一个强大的命令行工具，它与Ubuntu的高级打包工具（apt）配合使用，执行诸如安装新软件包、升级现有软件包、更新包列表索引，甚至升级整个Ubuntu系统等功能。

作为一个简单的命令行工具，apt比Ubuntu中其他服务器管理员可用的包管理工具有许多优势。其中一些优势包括比简单终端连接（SSH）更易于使用，以及在系统管理脚本中使用的功能，而这些脚本又可以由cron调度实用程序自动执行。

apt实用程序的一些常用示例：

•：使用apt工具安装软件包非常简单。例如，要安装网络扫描仪nmap，请键入以下内容：**安装软件包SUDO apt Install nmap**

•：删除软件包也很简单。要删除上一示例中安装的软件包，请键入以下内容：**移除一个包sudo apt Remove nmap**

**多个包**：您可以指定要安装或删除的多个软件包，并用空格分隔。

此外，将--purge选项添加到apt remove也将删除包配置文件。这可能是或可能不是期望的效果，因此请谨慎使用。

•：APT软件包索引本质上是一个数据库，包含/etc/APT/sources.list文件和/etc/APT/sources.list.d目录中定义的存储库中的可用软件包。要使用存储库中的最新更改更新本地软件包索引，请键入以下内容：**更新包索引sudo apt Update**

•：随着时间的推移，当前安装在您计算机上的软件包的更新版本可能会从软件包存储库中获得（例如，安全更新）。要升级您的系统，请首先按照上述说明更新软件包索引，然后键入：**升级包Sudo apt升级**

有关升级到新Ubuntu版本的信息，请参阅第4节“升级”[p.11]。

apt命令的操作（如安装和删除软件包）记录在/var/log/dpkg.log文件中。

有关APT使用的更多信息，请阅读全面的Debian APT用户手册[30]或键入：

**贴身帮助**

## 4.才能

在没有命令行选项的情况下启动Aptitude，将为您提供一个菜单驱动、基于文本的高级打包工具（APT）系统前端。许多常见的包管理功能，如安装、删除和升级，都可以在Aptitude中使用单键命令执行，这些命令通常是小写字母。

Aptitude最适合在非图形终端环境中使用，以确保命令键正常运行。您可以作为普通用户，在终端提示下键入以下命令，启动Aptitude的菜单驱动界面：**sudo能力倾向**

当Aptitude启动时，您将在屏幕顶部看到一个菜单栏，在菜单栏下方看到两个窗格。顶部窗格包含软件包类别，如新软件包和未安装软件包。底部窗格包含与软件包和软件包类别相关的信息。

使用Aptitude进行软件包管理相对简单，用户界面使常见任务易于执行。以下是在Aptitude中执行的常见软件包管理功能的示例：

•：要安装软件包，请使用键盘箭头键和回车键，通过“未安装软件包”类别找到软件包。突出显示所需的软件包，然后按+键。软件包条目应变为绿色，表示已标记要安装。现在按g键显示软件包摘要操作。再次按g键，将开始下载和安装软件包。完成后，按ENTER键返回菜单。**安装软件包**

•：要删除软件包，请使用键盘箭头键和回车键，通过已安装软件包类别找到软件包。突出显示要删除的所需软件包，然后按-键。软件包条目应变为粉红色，表示已标记为要删除。现在按g可显示软件包摘要ge操作。再次按g键，将开始移除软件包。完成后，按ENTER键返回菜单。**删除包**

•：要更新包裹索引，只需按u键。包裹索引的更新将开始。**更新包索引**

•：要升级软件包，请按上述详细说明更新软件包索引，然后按U键标记所有软件包的更新。现在按g键，您将看到软件包操作的摘要。再次按g键，下载和安装将开始。完成后，按ENTER键返回菜单。**升级包**

实际查看包时，顶部窗格中包列表中显示的第一列信息列出了包的当前状态，并使用以下键描述包的状态：

•：安装包**我**

•：未安装软件包，但软件包配置仍保留在系统上**C**

•：从系统中清除**P**

•：虚拟软件包**v**

•：包装破损**B**

•：未打包的文件，但尚未配置包**U**

•：半配置-配置失败，需要修复**C**

•：半安装-拆卸失败，需要修复**H**

要退出智能，只需按q键并确认您希望退出。按F10键可从智能菜单中获得许多其他功能。

#### 4.1.命令行能力

您还可以使用APTITE作为命令行工具，类似于apt。要安装具有所有必要依赖项的nmap包，如apt示例中所示，您将使用以下命令：**sudo智能安装nmap**

要删除相同的包，请使用以下命令：**sudo智能删除nmap**

有关Aptitude命令行选项的更多详细信息，请参阅手册页。

## 5.自动更新

无人值守升级软件包可用于自动安装更新的软件包，并可配置为更新所有软件包或仅安装安全更新。首先，通过在终端中输入以下内容来安装软件包：**sudo apt安装无人值守升级**

要配置无人值守升级，请编辑/etc/apt/apt.conf.d/50Understand-upgrades并调整以下内容以满足您的需要：

无人参与升级：：允许的来源{

“${distro\_id}:${distro\_codename}”；

“${distro\_id}:${distro\_codename}-安全”；

//“${distro\_id}:${distro\_codename}-更新”；

//“${distro\_id}:${distro\_codename}-建议”；/“${distro\_id}:${distro\_codename}-后端口”；

};

某些软件包也可能被列入黑名单，因此不会自动更新。若要将软件包列入黑名单，请将其添加到列表中：

无人参与升级：：软件包黑名单{

//“vim”；

//“libc6”；

//“libc6-dev”；/“libc6-i686”；

};

双精度“/”用作注释，因此“/”后面的内容将不会被计算。

要启用自动更新，请编辑/etc/apt/apt.conf.d/20auto-upgrades并设置适当的apt配置选项：

APT:：Periodic:：Update软件包列表“1”；APT:：Periodic:：下载可升级软件包“1”；

APT:：周期：：自动清理间隔“7”；

APT:：定期：：无人值守升级“1”；

上面的配置每天更新包列表、下载和安装可用的升级。本地下载存档每周清理一次。在升级到更新版本的Ubuntu的服务器上，根据您的响应，上面列出的文件可能不在那里。在这种情况下，创建此名称的新文件也应该有效。

您可以在/etc/cron.daily/apt-compat脚本头中阅读有关apt定期配置选项的更多信息。

无人参与升级的结果将记录到/var/log/untained upgrades。

#### 5.1.通知

配置无人值守升级：：Mail in/etc/apt/apt.conf.d/50unservated-upgrades将启用无人值守升级，以向管理员发送电子邮件，详细说明任何需要升级或有问题的软件包。

另一个有用的软件包是apticron。apticron将配置一个cron作业，通过电子邮件向管理员发送有关系统上具有可用更新的任何软件包的信息，以及每个软件包中更改的摘要。

要安装apticron软件包，请在终端中输入：**sudo apt安装apticron**

安装软件包后，编辑/etc/apticron/apticron.conf以设置电子邮件地址和其他选项：

电子邮件=”root@example.com"

## 6.配置

高级打包工具（APT）系统存储库的配置存储在/etc/APT/sources.list文件和/etc/APT/sources.list.d目录中。此处引用了该文件的一个示例，以及有关在该文件中添加或删除存储库引用的信息。

您可以编辑该文件以启用或禁用存储库。例如，要禁用每当包操作发生时插入Ubuntu CD-ROM的要求，只需注释掉CD-ROM的相应行，该行显示在文件顶部：

#请不要再提示使用CD-ROM了#deb cdrom:[Ubuntu 18.04"仿生海狸"-i386发行版（20111013.1）]/Bionic main restricted

#### 6.1.额外存储库

除了官方支持的Ubuntu软件包存储库外，还有其他社区维护的存储库，这些存储库为可能的安装增加了数千个软件包。其中两个最流行的是Universe和Multiverse存储库。这些存储库不受Ubuntu的官方支持，但因为它们是由社区重新维护，他们通常提供与Ubuntu计算机一起使用的安全软件包。

Multiverse存储库中的包通常存在许可问题，这些问题会阻止它们使用免费操作系统分发，并且它们在您所在的地区可能是非法的。

请注意，Universe或Multiverse存储库都不包含官方支持的包。特别是，这些包可能没有安全更新。

还有许多其他包源可用，有时甚至只提供一个包，就像单个应用程序的开发人员提供的包源一样。但是，在使用非标准包源时，您应该始终非常小心。在执行任何安装之前，请仔细研究源代码和软件包，因为某些软件包源代码及其软件包可能会导致系统在某些方面不稳定或无法正常工作。

默认情况下，Universe和Multiverse存储库处于启用状态，但如果要禁用它们，请编辑/etc/apt/sources.list并注释以下行：

黛布http://archive.ubuntu.com/ubuntu 仿生宇宙多重宇宙http://archive.ubuntu.com/ubuntu 仿生宇宙多元宇宙

黛布http://us.archive.ubuntu.com/ubuntu/ 仿生宇宙http://us.archive.ubuntu.com/ubuntu/ 仿生宇宙http://us.archive.ubuntu.com/ubuntu/ 仿生更新宇宙deb srchttp://us.archive.ubuntu.com/ubuntu/ 仿生更新宇宙

黛布http://us.archive.ubuntu.com/ubuntu/ 仿生多重宇宙

deb srchttp://us.archive.ubuntu.com/ubuntu/ 仿生多重宇宙http://us.archive.ubuntu.com/ubuntu/ 仿生更新多元宇宙deb srchttp://us.archive.ubuntu.com/ubuntu/ 仿生多元宇宙

黛布http://security.ubuntu.com/ubuntu 仿生安全宇宙http://security.ubuntu.com/ubuntu 仿生安全宇宙http://security.ubuntu.com/ubuntu 仿生安全多重宇宙http://security.ubuntu.com/ubuntu 仿生安全多元宇宙

## 7.工具书类

本章涵盖的大部分材料都有手册页，其中许多可在线获取。

•安装软件[31]Ubuntu wiki页面有更多信息。

•有关dpkg的更多详细信息，请参阅dpkg手册页[32]。

•APT指南[33]和APT手册页[34]包含有关APT使用的有用信息。

•更多能力倾向选项，请参见能力倾向手册[35]。

•添加存储库HOWTO（Ubuntu Wiki）[36]页面包含更多关于添加存储库的详细信息。

# 第四章。网络

网络由两个或多个设备组成，如计算机系统、打印机和相关设备，通过物理电缆或无线链路连接，以便在连接的设备之间共享和分发信息。

本节提供有关网络的一般和特定信息，包括网络概念概述和流行网络协议的详细讨论。

## 1.网络配置

Ubuntu附带了许多图形工具来配置您的网络设备。本文档面向服务器管理员，重点介绍在命令行上管理网络。

#### 1.1. 以太网接口

以太网接口由系统使用可预测的网络接口名称标识。这些名称可以显示为eno1或enp0s25。但是，在某些情况下，接口可能仍然使用内核eth#风格的命名。

##### 1.1.1. 识别以太网接口

要快速识别所有可用的以太网接口，可以使用ip命令，如下所示。

**ip a**1:lo:<LOOPBACK，UP，LOWER\u UP>mtu 65536 qdisc noqueue state未知组默认qlen 1000链接/LOOPBACK 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8作用域主机lo有效\u lft forever首选\u lft forever inet6:：1/128作用域主机

有效的永远首选永远2:enp0s25:<广播，多播，向上，向下\u向上>mtu 1500 qdisc noqueue状态向上组默认qlen 1000

链接/以太00:16:3e:e2:52:42 brd ff:ff:ff:ff:ff:ff:ff链接网络ID 0 inet 10.102.66.200/24 brd 10.102.66.255作用域全局动态eth0有效\u lft 3257秒首选\u lft 3257秒inet6 fe80:：216:3eff:fee2:5242/64作用域链接有效\u lft永远首选\u lft永远首选\u lft

另一个可以帮助识别系统可用的所有网络接口的应用程序是lshw命令。此命令提供有关特定适配器的硬件功能的更多详细信息。在下面的示例中，lshw显示了一个逻辑名称为eth0的以太网接口，以及总线信息、驱动程序详细信息和所有支持的功能。

**sudolshw类网络**\*-网络

描述：以太网接口

产品：MT26448[ConnectX EN 10GigE，PCIe 2.0 5GT/s]供应商：Mellanox Technologies物理标识：0总线信息：pci@0004：01:00.0逻辑名称：eth4版本：b0

序列号：e4:1d:2d:67:83:56插槽：U78CB.001.WZS09KB-P1-C6-T1大小：10Gbit/s容量：10Gbit/s宽度：64位时钟：33MHz

功能：pm vpd msix pciexpress总线\u主cap \u列表以太网物理光纤10000bt fd

配置：自动协商=关闭广播=是驱动程序=mlx4\u en驱动服务器版本=4.0-0双工=完整固件=2.9.1326 ip=192.168.1.1延迟=0链路=是多播=是端口=光纤速度=10Gbit/s

资源：iomemory:24000-23fff irq:481内存：3fe200000000-3fe2000fffff内存：240000000000-240007FFFF

##### 1.1.2. 以太网接口逻辑名称

接口逻辑名称也可以通过网络计划配置进行配置。如果要控制哪个接口接收特定的逻辑名称，请使用匹配和设置名称键。match键用于根据MAC地址、驱动程序等条件查找适配器。然后，set name键可用于将设备更改为所需的逻辑名称。

网络：

版本：2渲染器：网络以太网络：eth\_lan0:

dhcp4:真正匹配：

地址：00:11:22:33:44:55集合名称：eth\_lan0

##### 1.1.3. 以太网接口设置

ethtool是一个显示和更改以太网卡设置的程序，如自动协商、端口速度、双工模式和LAN唤醒。以下是如何查看以太网接口的支持功能和配置设置的示例。

**sudo ethtool eth4**eth4的设置：

支持的端口：[光纤]

支持的链接模式：10000baseT/完整

支持的暂停帧使用：否

支持自动协商：否

支持的FEC模式：未报告

广告链接模式：10000baseT/完整

广告暂停帧用途：否

播发的自动协商：无播发的FEC模式：未报告

速度：10000Mb/s

双工：全

端口：光纤

物理量：0

收发器：内部

自动协商：关闭

支持唤醒：d

醒来：d

当前消息级别：0x00000014（20）链接如果检测到向下链接：是

#### 1.2. 定址方式

以下部分描述了配置在局域网和Internet上通信所需的系统IP地址和默认网关的过程。

##### 1.2.1. 临时IP地址分配

对于临时网络配置，您可以使用ip命令，该命令也可以在大多数其他GNU/Linux操作系统上找到。ip命令允许您配置立即生效的设置，但是这些设置不是持久的，在重新启动后将丢失。

要临时配置IP地址，可以按以下方式使用IP命令。修改IP地址和子网掩码以符合您的网络要求。然后可以使用ip设置链路的上行或下行。**sudo ip地址添加10.102.66.200/24开发enp0s25**

**ip链路设置dev enp0s25向上ip链路设置dev enp0s25向下**

要验证enp0s25的IP地址配置，可以按以下方式使用IP命令。

**ip地址显示设备enp0s25**10:enp0s25:<广播、多播、向上、向下\u向上>mtu 1500 qdisc noqueue状态向上组默认qlen 1000

链接/以太00:16:3e:e2:52:42 brd ff:ff:ff:ff:ff:ff:ff链接网络ID 0 inet 10.102.66.200/24 brd 10.102.66.255作用域全局动态eth0有效\u lft 2857秒首选\u lft 2857秒inet6 fe80:：216:3eff:fee2:5242/64作用域链接有效\u lft永久首选\u lft forever 6

要配置默认网关，可以按以下方式使用ip命令。修改默认网关地址以符合您的网络要求。**sudo ip路由通过10.102.66.1添加默认值**

要验证默认网关配置，可以按以下方式使用ip命令。

**ip路由显示**

默认通过10.102.66.1 dev eth0 proto dhcp src 10.102.66.200 metric 100 10.102.66.0/24 dev eth0 proto内核作用域链接src 10.102.66.200

10.102.66.1 dev eth0协议dhcp作用域链接src 10.102.66.200公制100

如果临时网络配置需要DNS，可以在文件/etc/resolv.conf中添加DNS服务器IP地址。一般来说，不建议直接编辑/etc/resolv.conf，但这是一种临时和非持久配置。下面的示例显示如何将两个DNS服务器输入到/etc/resolv.conf，应将其更改为适合您网络的服务器。下面一节将详细介绍进行DNS客户端配置的正确持久化方法。

名称服务器8.8.8.8名称服务器8.8.4.4

如果您不再需要此配置，并且希望从接口中清除所有IP配置，则可以使用带有flush选项的IP命令，如下所示。**ip地址刷新eth0**

使用IP命令刷新IP配置不会清除/etc/resolv.conf的内容。您必须手动删除或修改这些条目，或者重新引导，这也会导致/etc/resolv.conf（指向/run/systemd/resolve/stub-resolv.conf的符号链接）被重新写入。

##### 1.2.2. 动态IP地址分配（DHCP客户端）

要将服务器配置为使用DHCP进行动态地址分配，请在文件/etc/netplan/99\_config.yaml中创建网络计划配置。下面的示例假设您正在配置标识为enp3s0的第一个以太网接口。

网络：

版本：2渲染器：networkd以太网：enp3s0:dhcp4:true

然后可以使用netplan命令应用配置。**sudo网络计划应用**

##### 1.2.3. 静态IP地址分配

要将系统配置为使用静态地址分配，请在文件/etc/netplan/99\_config.yaml中创建一个netplan配置。下面的示例假设您正在配置标识为eth0的第一个以太网接口。更改地址、网关4和名称服务器值以满足网络的要求。

网络：

版本：2渲染器：networkd以太网：eth0:地址：-10.10.10.2/24网关4:10.10.10.1名称服务器：

搜索：[mydomain，otherdomain]地址：[10.10.10.1,1.1.1]

然后可以使用netplan命令应用配置。**sudo网络计划应用**

##### 1.2.4. 环回接口

系统将环回接口标识为lo，其默认IP地址为127.0.0.1。可以使用ip命令查看它。

**ip地址显示lo**1:lo:<LOOPBACK，UP，LOWER\u UP>mtu 65536 qdisc noqueue state未知组默认qlen 1000链接/LOOPBACK 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8作用域主机lo有效\u lft forever首选\u lft forever inet6:：1/128作用域主机

永远有效\u lft首选\u lft永远有效

#### 1.3. 名称解析

与IP网络相关的名称解析是将IP地址映射到主机名的过程，从而更容易识别网络上的资源。以下部分将解释如何正确配置系统，以便使用DNS和静态主机名记录进行名称解析。

##### 1.3.1. DNS客户端配置

传统上，文件/etc/resolv.conf是一个静态配置文件，很少需要通过DCHP客户机挂钩进行更改或自动更改。Systemd resolved处理名称服务器配置，应该通过Systemd resolve命令与之交互。Netplan将systemd resolved配置为生成要放入/etc/resolv.conf中的名称服务器和域的列表，这是一个符号链接：

/etc/resolv.conf->../run/systemd/resolve/stub-resolv.conf

要配置冲突解决程序，请将适合您网络的名称服务器的IP地址添加到netplan配置文件中。您还可以添加可选的DNS后缀搜索列表，以匹配您的网络域名。生成的文件可能如下所示：

网络：

版本：2

渲染器：networkd以太网：enp0s25:地址：-192.168.0.100/24网关4:192.168.0.1名称服务器：

搜索：[mydomain，otherdomain]地址：[1.1.1,8.8.8,4.4.4]

搜索选项也可用于多个域名，以便DNS查询将按输入顺序追加。例如，您的网络可能有多个子域要搜索；example.com的父域，以及sales.example.com和dev.example.com两个子域。

如果要搜索多个域，则配置可能如下所示：

网络：

版本：2渲染器：networkd以太网：enp0s25:地址：-192.168.0.100/24网关4:192.168.0.1名称服务器：

搜索：[example.com，sales.example.com，dev.example.com]地址：[1.1.1,8.8.8,4.4.4]

如果尝试ping名称为server1的主机，系统将按以下顺序自动查询DNS以获取其完全限定域名（FQDN）：

1.    server1.example.com

2.    server1.sales.example.com

##### 3.server1.dev.example.com

如果未找到匹配项，DNS服务器将提供notfound结果，DNS查询将失败。

###### 1.3.2. 静态主机名

静态主机名是位于文件/etc/hosts中的本地定义的主机名到IP的映射。默认情况下，主机文件中的条目优先于DNS。这意味着，如果您的系统尝试解析主机名，并且它与/etc/hosts中的条目匹配，则不会尝试在DNS中查找记录。在某些配置中，特别是当不需要Internet访问时，可以方便地将与有限数量的资源通信的服务器设置为使用静态主机名而不是DNS。

以下是一个主机文件示例，其中许多本地服务器通过简单的主机名、别名及其等效的完全限定域名（FQDN）进行标识。

127.0.0.1本地主机

127.0.1.1 ubuntu服务器

10.0.0.11服务器1服务器1.example.com vpn

10.0.0.12服务器2服务器2.example.com邮件

10.0.0.13服务器3服务器3.example.com www

10.0.0.14 server4 server4.example.com文件

在上面的示例中，请注意，除了它们的专有名称和FQDN之外，还为每个服务器提供了别名。Server1已映射到名称vpn，server2称为邮件，server3称为www，server4称为文件。

###### 1.3.3. 名称服务交换机配置

系统选择将主机名解析为IP地址的方法的顺序由

名称服务交换机（NSS）配置文件/etc/nsswitch.conf。如前一节所述，通常在systems/etc/hosts文件中定义的静态主机名优先于从DNS解析的名称。下面是负责文件/etc/nsswitch.conf中主机名查找顺序的行的示例。主机：文件mdns4\u最小[NOTFOUND=return]dns mdns4

•首先尝试解析位于/etc/hosts中的静态主机名。**文件夹**

•尝试使用多播DNS解析名称。**mdns4\_最小值**

•意味着之前的mdns4\_最小流程未发现的任何响应应被视为权威性响应，系统不应试图继续寻找答案。**[未找到=返回]**

•表示传统的单播DNS查询。**域名系统**

•表示多播DNS查询。**mdns4**

要修改上述名称解析方法的顺序，只需将hosts:string更改为您选择的值。例如，如果您更喜欢使用传统的单播DNS而不是多播DNS，则可以更改/etc/nsswitch.conf中的字符串，如下所示。主机：文件dns[NOTFOUND=return]mdns4\u最小mdns4

#### 1.4. 架桥

桥接多个接口是一种更高级的配置，但在多个场景中非常有用。一种方案是建立一个具有多个网络接口的网桥，然后使用防火墙过滤两个网段之间的流量。另一种方案是在具有一个接口的系统上使用网桥，以允许虚拟机直接访问外部网络。下面的示例介绍了后一种情况。

通过编辑/etc/netplan/中的网络计划配置来配置网桥：

网络：

版本：2

渲染器：网络以太网络：enp3s0:

dhcp4:无桥：br0:

dhcp4：是接口：-enp3s0

为物理接口和网络输入适当的值。

现在应用配置以启用网桥：**sudo网络计划应用**

新的网桥接口现在应该已启动并运行。brctl提供有关网桥状态的有用信息，控制哪些接口是网桥的一部分等。有关更多信息，请参阅man brctl。

#### 1.5. 资源

•UbuntuWiki网络页面[37]链接到涵盖更高级网络配置的文章。

•netplan网站[38]有其他示例和文档。

•netplan手册页[39]提供了有关netplan的更多信息。

•systemd resolve手册页[40]详细介绍了systemd resolve命令。

•systemd resolved手册页[41]提供了有关systemd resolved服务的更多信息。

•有关桥接的更多信息，请参阅netplan.io示例页面[42]和Linux基金会的网络桥接[43]页面。

## 2.TCP/IP

传输控制协议和互联网协议（TCP/IP）是美国国防高级研究计划局（DARPA）在20世纪70年代末开发的一套标准协议，作为不同类型计算机和计算机网络之间的通信手段。TCP/IP是Internet的驱动力，因此它是地球上最流行的一组网络协议。

#### 2.1. TCP/IP简介

TCP/IP的两个协议组件处理计算机网络的不同方面。Internet协议，TCP/IP中的“IP”是一种无连接协议，它只处理使用IP数据报作为网络信息基本单位的网络数据包路由。IP数据报由一个标头和一条消息组成。传输控制协议是TCP/IP的“TCP”，使网络主机能够建立可用于交换数据流的连接。TCP还保证连接之间的数据被传递，并且数据到达一个网络主机的顺序与从另一个网络主机发送的顺序相同。

#### 2.2. TCP/IP配置

TCP/IP协议配置由多个元素组成，必须通过编辑适当的配置文件或部署解决方案（如动态主机配置协议（DHCP）服务器）来设置这些元素，而动态主机配置协议（DHCP）服务器又可以配置为自动向网络客户端提供适当的TCP/IP配置设置。必须正确设置这些配置值，以便于Ubuntu系统的正确网络操作。

TCP/IP的常见配置元素及其用途如下：

•IP地址是一个唯一的标识字符串，表示为四个十进制数字，范围从零（0）到二百五十五（255），用句点分隔，四个数字中的每一个代表地址的八（8）位，整个地址的总长度为三十二（32）位。这种格式称为点四元表示法。**IP地址**

•子网掩码（或简单地说，网络掩码）是一个本地位掩码，或一组标志，用于将对网络重要的IP地址部分与对子网重要的位分开。例如，在C类网络中，标准网络掩码为255.255.255.0，它屏蔽IP地址的前三个字节，并允许IP地址的最后一个字节保持可用，以指定子网络上的主机。**子网掩码**

•网络地址表示组成IP地址网络部分的字节。例如，a类网络中的主机12.128.1.2将使用12.0.0.0作为网络地址，其中十二（12）表示IP地址的第一个字节（网络部分），其余三个字节中的零（0）表示潜在主机值。使用专用IP地址192.168.1.100的网络主机将依次使用192.168.1.0的网络地址，该地址指定C类192.168.1网络的前三个字节，并为网络上所有可能的主机指定零（0）。**网络地址**

•广播地址是一个IP地址，允许将网络数据同时发送到给定子网上的所有主机，而不是指定特定主机。IP网络的标准通用广播地址为255.255.255.255，但此广播地址不能用于向Internet上的每台主机发送广播消息，因为路由器会阻止它。设置更合适的广播地址以匹配特定子网。例如，在专用C类IP网络192.168.1.0上，广播地址为192.168.1.255。广播消息通常由网络协议产生，如地址解析协议（ARP）和路由信息协议（RIP）。**广播地址**

•网关地址是IP地址，通过它可以访问特定网络或网络上的主机。如果一个网络主机希望与另一个网络主机通信，而该主机不在同一网络上，则必须使用网关。在许多情况下，网关地址将是同一网络上路由器的地址，而路由器又将流量传递到其他网络或主机，如Internet主机。网关地址设置的值必须正确，否则系统将无法访问同一网络上的主机以外的任何主机。**网关地址**

•名称服务器地址表示域名服务（DNS）系统的IP地址，该系统将网络主机名解析为IP地址。名称服务器地址有三个级别，可以按优先级顺序指定：主名称服务器、次名称服务器和第三名称服务器。为了使您的系统能够将网络主机名解析为其相应的IP地址，您必须指定您有权在系统的TCP/IP配置中使用的有效名称服务器地址。在许多情况下，这些地址可以并将由您的网络服务提供商提供，但许多免费和可公开访问的名称服务器可供使用，例如IP地址从4.2.2.1到4.2.2.6的Level3（Verizon）服务器。**名称服务器地址**

IP地址、网络掩码、网络地址、广播地址、网关地址和名称服务器地址通常通过文件/etc/Network/interfaces中的相应指令指定。有关详细信息，请查看界面的系统手册页面，在终端提示下键入以下命令：

使用以下命令访问系统手册页面以获取接口：**人机界面**

#### 2.3. IP路由

IP路由是一种指定和发现TCP/IP网络中的路径的方法，网络数据可以沿着该路径发送。路由使用一组路由表将网络数据包从其源转发到目的地，通常通过许多称为路由器的中间网络节点。IP路由有两种主要形式：静态路由和动态路由。

静态路由包括手动将IP路由添加到系统的路由表中，这通常是通过使用route命令操纵路由表来完成的。与动态路由相比，静态路由具有许多优点，例如在较小的网络上实现的简单性、可预测性（路由表总是预先计算的，因此每次使用的路由都是完全相同的），以及由于缺少动态路由协议，其他路由器和网络链路的开销较低。然而，静态路由也存在一些缺点。例如，静态路由仅限于小型网络，无法很好地扩展。

由于路由的固定性质，静态路由也无法完全适应路由沿线的网络中断和故障。

动态路由依赖于具有从源到目标的多条可能IP路由的大型网络，并利用特殊的路由协议，如路由器信息协议（RIP），该协议处理路由表中的自动调整，使动态路由成为可能。与静态路由相比，动态路由具有一些优势，例如优越的可扩展性和适应网络路由故障和中断的能力。此外，路由表的手动配置更少，因为路由器相互学习它们的存在和可用路由。这种特性还消除了通过人为错误在路由表中引入错误的可能性。然而，动态路由并不是完美的，并且存在一些缺点，例如路由器通信带来的复杂性增加和额外的网络开销，这不会立即为最终用户带来好处，但仍然会消耗网络带宽。

#### 2.4. TCP和UDP

TCP是一种基于连接的协议，通过所谓的流控制提供错误纠正和有保证的数据传输。流控制确定何时需要停止数据流的流，并且由于诸如冲突之类的问题而应该重新发送先前发送的数据包，从而确保数据的完整和准确传递。TCP通常用于交换重要信息，如数据库事务。

另一方面，用户数据报协议（UDP）是一种无连接协议，很少处理重要数据的传输，因为它缺乏流量控制或任何其他方法来确保数据的可靠传输。UDP通常用于音频和视频流等应用中，由于缺少纠错和流量控制，UDP的速度比TCP快得多，并且一些数据包的丢失通常不是灾难性的。

#### 2.5. ICMP

Internet控制消息传递协议（ICMP）是在征求意见（RFC）792中定义的Internet协议（IP）的扩展，支持包含控制、错误和信息消息的网络数据包。ICMP由ping实用程序等网络应用程序使用，它可以确定网络主机或设备的可用性。ICMP返回的对网络主机和路由器等设备都有用的一些错误消息的示例包括目标不可到达和超出时间。

#### 2.6. 后台程序

守护进程是特殊的系统应用程序，通常在后台连续执行，并等待其他应用程序对其提供的功能的请求。许多守护进程是以网络为中心的；也就是说，在Ubuntu系统上后台执行的大量守护进程可能提供与网络相关的功能。此类网络守护程序的一些示例包括超文本传输协议守护程序（httpd），它提供web服务器功能；安全SHell守护程序（sshd），提供安全的远程登录SHell和文件传输功能；以及提供电子邮件服务的Internet消息访问协议守护程序（imapd）。

#### 2.7. 资源

•TCP[44]和IP[45]的手册页包含更多有用信息。

•另外，请参阅TCP/IP教程和技术概述[46]IBM红皮书。

•另一个资源是O&apos;Reilly的TCP/IP网络管理[47]。

## 3.动态主机配置协议（DHCP）

动态主机配置协议（DHCP）是一种网络服务，它使主机计算机能够从服务器自动分配设置，而不是手动配置每个网络主机。配置为DHCP客户端的计算机无法控制从DHCP服务器接收的设置，并且配置对计算机的用户是透明的。

DHCP服务器向DHCP客户端提供的最常见设置包括：

•IP地址和网络掩码

•要使用的默认网关的IP地址

•要使用的DNS服务器的IP地址

但是，DHCP服务器也可以提供配置属性，例如：

•主机名

•域名

•时间服务器

•打印服务器

使用DHCP的优点是，对网络的更改（例如DNS服务器地址的更改）只需在DHCP服务器上更改，并且所有网络主机将在其DHCP客户端下次轮询DHCP服务器时重新配置。作为一个额外的优势，将新计算机集成到网络中也更容易，因为不需要检查IP地址的可用性。IP地址分配中的冲突也减少了。

DHCP服务器可以使用以下方法提供配置设置：

手动分配（MAC地址）

此方法需要使用DHCP来识别连接到网络的每个网卡的唯一硬件地址，然后在每次DHCP客户端使用该网络设备向DHCP服务器发出请求时持续提供恒定的配置。这样可以确保根据网卡的MAC地址自动将特定地址分配给该网卡。

动态分配（地址池）

在这种方法中，DHCP服务器将从一个地址池（有时也称为范围或作用域）分配一个IP地址，时间或租约在服务器上配置，或直到客户端通知服务器不再需要该地址。通过这种方式，客户端将在“先到先得”的基础上动态地接收其配置属性。当DHCP客户端在指定时间段内不再在网络上时，配置将过期并释放回地址池供其他DHCP客户端使用。这样，一个地址可以在一段时间内租用或使用。在此期间之后，客户端必须与服务器重新协商租约，以保持地址的使用。

自动分配

使用此方法，DHCP会自动将IP地址永久分配给设备，并从可用地址池中进行选择。通常使用DHCP为客户端分配临时地址，但DHCP服务器可以允许无限的租用时间。

最后两种方法可以被认为是“自动”的，因为在每种情况下，DHCP服务器都会分配一个地址，而不需要额外的干预。它们之间的唯一区别在于IP地址被租用的时间，换句话说，客户的地址是否随时间而变化。Ubuntu提供的DHCP服务器是dhcpd（动态主机配置协议守护进程），它易于安装和配置，并将在系统启动时自动启动。

#### 3.1. 安装

在终端提示下，输入以下命令以安装dhcpd：**sudo apt安装isc dhcp服务器**

您可能需要通过编辑/etc/dhcp/dhcpd.conf来更改默认配置，以满足您的需要和特定的配置。

您可能还需要编辑/etc/default/isc dhcp server来指定dhcpd应该侦听的接口。

注意：dhcpd的消息正在发送到syslog。查看那里的诊断信息。

#### 3.2. 配置

安装结束时出现的错误消息可能有点混乱，但以下步骤将帮助您配置服务：

通常，您要做的是随机分配一个IP地址。这可以通过以下设置完成：

#最小示例/etc/dhcp/dhcpd.conf默认租用时间600；最大租赁时间7200；

子网192.168.1.0网络掩码255.255.255.0{range 192.168.1.150 192.168.1.200；可选路由器192.168.1.254；

选项域名服务器192.168.1.1192.168.1.2；选项域名“mydomain.example”；}

这将导致DHCP服务器为客户端提供范围为192.168.1.150-192.168.1.200的IP地址。

如果客户端不要求特定的时间范围，它将租用一个IP地址600秒。否则，最大（允许）租用时间为7200秒。服务器还将“建议”客户端使用192.168.1.254作为默认网关，使用192.168.1.1和192.168.1.2作为其DNS服务器。

更改配置文件后，必须重新启动dhcpd：**sudo systemctl重新启动isc-dhcp-server.service**

#### 3.3. 工具书类

•dhcp3服务器Ubuntu Wiki[48]页面有更多信息。

•有关更多/etc/dhcp/dhcpd.conf选项，请参阅dhcpd.conf手册页[49]。•ISC dhcp服务器[50]

## 4.时间同步

NTP是一种TCP/IP协议，用于通过网络同步时间。基本上，客户机从服务器请求当前时间，并使用它设置自己的时钟。

在这个简单的描述背后，有很多复杂性——有多层NTP服务器，第一层NTP服务器连接到原子钟，第二层和第三层服务器将实际处理请求的负载分散到Internet上。此外，客户端软件比您想象的要复杂得多——它必须考虑到通信延迟，并以一种不会打乱服务器上运行的所有其他进程的方式调整时间。但幸运的是，所有这些复杂性都对你隐瞒了！

Ubuntu默认使用timedatectl/timesyncd来同步时间，用户可以选择使用chrony来实现第4.2节“为网络时间协议服务”[p.56]。

#### 4.1. 同步系统时间

由于Ubuntu 16.04 timedatectl/timesyncd（systemd的一部分）取代了大部分ntpdate/ntp。

timesyncd在默认情况下可用，它不仅替换ntpdate，还替换chrony（或以前的ntpd）的客户端部分。因此，除了ntpdate在启动和网络激活时提供的一次性操作之外，默认情况下，现在的timesyncd定期检查并保持本地时间同步。它还将时间更新存储在本地，以便在重新启动后单调地前进（如果适用）。

如果安装了chrony，则timedatectl会后退一步，让chrony计时。这将确保没有两次同步服务发生冲突。虽然不再推荐使用，但这仍然适用于安装ntpd以保留通过升级获得的任何类型的旧行为/配置。但这也意味着在从以前版本升级时，ntp/ntpdate可能仍会安装，因此会禁用新的基于systemd的服务。

ntpdate被认为是不推荐使用的，支持timedatectl（或chrony），因此默认情况下不再安装。

timesyncd通常会做正确的事情保持时间同步，而chrony将有助于处理更复杂的情况。但是如果你有一些已知的特殊NTPUTE用例，请考虑以下内容：

•如果您需要一次性同步，请使用：chronyd-q

•如果您需要一次性时间检查，而不设置时间，请使用：chronyd-Q

##### 4.1.1. 配置timedatectl和timesyncd

通过timedatectl和timesyncd可以使用timedatectl status检查时间和时间配置的当前状态。

$timedatectl状态

当地时间：Fr 2018-02-23 08:47:13 UTC

世界时间：Fr 2018-02-23 08:47:13 UTC

RTC时间：Fr 2018-02-23 08:47:13时区：Etc/UTC（UTC，+0000）

系统时钟已同步：是

systemd-timesyncd.service活动：是本地RTC TZ:否

如果chrony正在运行，它将自动切换到：[……]

systemd-timesyncd.service活动：否

管理员可以通过timedatectl控制时区、系统时钟与hwclock的关系以及是否应启用永久同步。有关更多详细信息，请参阅man timedatectl。timesyncd本身仍然是一项正常的服务，因此您也可以通过查看更详细的状态。

$systemctl状态systemd timesyncd

systemd-timesyncd.service-加载的网络时间同步：加载（/lib/systemd/system/systemd-timesyncd.service；已启用；供应商预设：已启用）活动：自2018-02-23 08:55:46 UTC星期五起活动（正在运行）；十年前

文档：man:systemd timesyncd.service（8）

主PID:3744（systemd timesyn）状态：“已同步到时间服务器91.189.89.198:123（ntp.ubuntu.com）。”

任务：2项（限额：4915）

CGroup:/system.slice/systemd-timesyncd.service

|-3744/lib/systemd/systemd timesyncd

Feb 23 08:55:46仿生测试系统D[1]：开始网络时间同步。。。

Feb 23 08:55:46仿生测试系统D[1]：开始网络时间同步。2月23日08:55:46仿生测试系统d timesyncd[3744]：同步到时间服务器91.189.89.198:123（ntp.ubuntu.com）。

可以在/etc/systemd/timesyncd.conf中指定从中获取timedatectl和timesyncd时间的名称服务器，并且可以在/etc/systemd/timesyncd.conf.d/中存储其他配置文件。NTP=和FallbackNTP=的条目是以空格分隔的列表。有关更多信息，请参阅man timesyncd.conf。

#### 4.2. 服务于网络时间协议

如果除了同步系统外，您还希望提供NTP信息，则需要一台NTP服务器。

chrony、ntpd和open ntp有多个选项。推荐的解决方案是chrony。

##### 4.2.1. 慢性病（d）

NTP守护进程chronyd计算系统时钟的漂移和偏移量，并不断调整它，因此没有可能导致不一致日志的大型更正。成本是一点处理能力和内存，但对于现代服务器来说，这通常可以忽略不计。

##### 4.2.2. 安装

要安装chrony，请在终端提示符下输入：

**sudo-apt-install-chrony**

这将提供两个二进制文件：

•chronyd-通过NTP协议同步和服务的实际守护进程

•chronyc-chrony守护程序的命令行界面

##### 4.2.3. Chronyd配置

编辑/etc/chrony/chrony.conf以添加/删除服务器行。默认情况下，这些服务器配置为：

#使用NTP池项目中的服务器。Ubuntu技术委员会于2011-02-08批准（LP:#104525）。看见http://www.pool.ntp.org/join.html 更多信息。

池0.ubuntu.pool.ntp.org iburst池1.ubuntu.pool.ntp.org iburst池2.ubuntu.pool.ntp.org iburst池3.ubuntu.pool.ntp.org iburst

有关配置选项的更多详细信息，请参阅man chrony.conf。更改任何配置文件后，必须重新启动chrony：**sudo systemctl重新启动chrony.service**

如果需要的话，pool 2.ubuntu.pool.ntp.org以及ntp.ubuntu.com也支持ipv6。如果需要强制ipv6，还有一个ipv6.ntp.ubuntu.com，默认情况下没有配置。

##### 4.2.4. 查看状态

使用chronyc查看查询chrony守护程序的状态。例如，获取当前可用和选定时间源的概述。

**计时源**

MS名称/IP地址到达最后一个样本

===============================================================================

^+伽马射线在28377135-1048us[-1048us]+/-29ms处

^-2b.ncomputers.org 2 8 377 204-1141us[-1124us]+/-50ms

^+www.kashra.com 28377139+3483us[+3483us]+/-18ms

^+地层2-4.NTP.TechFak.U>28377143-2090us[-2073us]+/-19ms

^-zepto.mcl.gg 27 377 9-774us[-774us]+/-29ms

^-mirrorhost.pw 2737778-660us[-660us]+/-53ms

^-atto.mcl.gg 27377 8-823us[-823us]+/-50ms

^-静态.140.107.46.78.cli>283779-1503us[-1503us]+/-45ms

^-4.53.160.75 28377137-11ms[-11ms]+/-117ms

^-37.44.185.42 37 377 10-3274us[-3274us]+/-70ms

^-bagnikita.com 2737774+3131us[+3131us]+/-71ms

^-europa.eliple.net 28377204-790us[-773us]+/-97ms

^-tethys.hot-chilli.net 28377141-797us[-797us]+/-59ms

^-66-232-97-8.静态hvvc>27377206+1669us[+1686us]+/-133ms

^+85.199.214.102 18377 205+175us[+192us]+/-12ms

^\*46-243-26-34.tangos.nl 188377141-123us[-106us]+/-10ms

^-pugot.canonical.com 2837721-95us[-95us]+/-57ms

^-alphyn.canonical.com 2 6 377 23-1569us[-1569us]+/-79ms

^-golem.canonical.com 2737792-1018us[-1018us]+/-31ms^-chilipepper.canonical.com 2837721-1106us[-1106us]+/-27ms

**chronyc sourcestats**

210来源数量=20

名称/IP地址NP NR范围频率频率偏移标准偏差偏差=25 15 32m-0.007 0.142-878us 106us 2b.ncomputers.org 26 16 35m-0.132 0.283-1169us 256us www.kashrack.com32m-0.0920.259+3426US195USStratum2-4.NTP.TechFak.U>251432M-0.0180.130-2056US96USZEPTO.mcl.GG131121M+0.1480.196-683US66USMirrorHost.PW65645+0.117 0.445-591US19USATTO.mcl.GG21325M-0.0690199-904us 103us静态.140.107.46.78.cli>251834M-0.005 0.094-1526us 78us 4.53.160.75 251032M+0.4120.110-11ms 84us

37.44.185.42 24 12 30m-0.983 0.173-3718us 122us bagnikita.com 17 7 31m-0.132 0.217+3527us 139us europa.ellipse.net 26 15 35m+0.038 0.553-473us 424us tethys.hot-chilli.net 25 11 32m-0.094 0.110-864us 88us 66-232-97-8.static.hvvc.>20 1135m-0.116 0.165+1561us 109us

85.199.214.102 26 11 35m-0.054 0.390+129us 343us

46-243-26-34.tangos.nl 25 16 32m+0.129 0.297-307us 198us pugot.canonical.com 25 14 34m-0.271 0.176-143us 135us alphyn.canonical.com 17 11 1100-0.087 0.360-1749us 114us golem.canonical.com 23 12 30m+0.057 0.370-988us 229us Chillipepper.canonical.com 25 1834m-0.0840.224-1116us 169us

某些chronyc命令具有特权，如果不明确允许，则无法通过网络运行。有关更多详细信息，请参阅man chrony.conf中的“命令和监视访问”一节。本地管理员可以像往常一样使用sudo，因为这将授予他访问本地管理员套接字/var/run/chrony/chronyd.sock的权限。

##### 4.2.5. PPS支持

Chrony本机支持各种PPS类型。它可以使用内核PPS API以及PTP硬件时钟。大多数通用GPS接收机可通过GPSD使用。后者（可能更多）可通过SHM或插座（推荐）访问。以上所有这些都可以用于通过额外的高质量时间源来增加计时，以获得更好的精度、抖动、漂移、长期或短期精度（通常每种时钟类型在其中一种方面都很好，但在其他方面并不完美）。有关配置的更多详细信息，请参阅下面列出的一些外部PPS/GPSD资源。

#### 4.3. 工具书类

•Chrony常见问题解答[51]

•ntp.org，网络时间协议项目之家16

•pool.ntp.org项目，是一个大型虚拟时间服务器集群。[52]

•关于timedatectl的Freedesktop.org信息[53]

•关于systemd TimeSync服务的Freedesktop.org信息[54]

•来自GPSD的喂食时间[55][56]

•有关更多信息，请参阅Ubuntu Time21 wiki页面。

## 5.数据平面开发工具包

DPDK是一组用于快速数据包处理的库和驱动程序，主要在Linux用户环境中运行。它是一组提供所谓的“环境抽象层”（EAL）的库。EAL隐藏了环境的细节，并提供了一个标准的编程接口。常见的用例是围绕特殊的解决方案，例如网络功能虚拟化和高级高通量网络交换。DPDK使用从运行到完成的模式来实现快速数据平面性能，并通过轮询访问设备，以消除中断处理的延迟，同时权衡更高的cpu消耗。它被设计为在任何处理器上运行。第一个受支持的CPU是Intel x86，它现在扩展到IBM Power 8、EZchip TILE Gx和ARM。

Ubuntu目前支持DPDK 2.2版，并提供了一些基础设施来简化其可用性。

#### 5.1. 先决条件

这个包目前是为尽可能低的CPU需求而编译的。这仍然要求CPU至少支持SSE3。

支持DPDK的上游网卡列表可在支持的NIC上找到[57]。但在上游项目中，由于它们还未处于稳定状态，因此默认情况下会禁用很多。DPDK在Ubuntu 16.04中提供的包中启用的网卡子集是：

英特尔

•e1000[58]（82540、82545、82546）

•e1000e[59]（82571..82574、82583、ICH8..ICH10、PCH..PCH2）

•igb[60]（82575..82576、82580、I210、I211、I350、I354、DH89xx）

•ixgbe[61]（82598..82599、X540、X550）

•i40e[62]（X710、XL710、X722）

•fm10k[63]（FM10420）

切西奥

•cxgbe[64]（终端器5）

思科

•enic[65]（UCS虚拟接口卡）

半虚拟化

•虚拟网络[66]（QEMU）

•vmxnet3[67]

其他

•af\_数据包[68]（Linux af\_数据包套接字）

•环[69]（存储器）

最重要的是，它通过实验启用了以下两个PMD驱动程序，因为它们代表终端用户非常容易访问的（虚拟）设备。

半虚拟化

•xenvirt[70]（Xen）

其他

•pcap[71]（文件或内核驱动程序）

卡必须从其内核驱动程序中取消分配，而是分配给vfio pci的uio\_pci\_generic。uio\_pci\_generic较旧，通常更容易工作。

较新的vfio pci需要激活以下内核参数才能启用iommu。

iommu=pt英特尔\_iommu=on

在vfio pci的顶部，您必须相应地配置和分配iommu组。

注意：在基于virtio的环境中，从内核驱动程序“取消分配”设备就足够了。否则DPDK将拒绝使用设备，以避免内核和DPDK同时在设备上工作时出现问题。由于DPDK可以直接在virtio设备上工作，因此无需为这些设备分配例如uio\_pci\_generic。

手动配置和状态检查可以通过sysfs或使用工具dpdk\_nic\_bind完成

dpdk\_nic\_绑定--帮助

用法：------

dpdk\_nic\_绑定[选项]设备1设备2。。。。

其中，DEVICE1、DEVICE2等通过PCI“域：总线：插槽.func”语法或“总线：插槽.func”语法指定。对于绑定到Linux内核驱动程序的设备，它们也可以通过Linux接口名称来引用，例如eth0、eth1、em0、em1等。

选项：

--帮助，--用法：显示用法信息并退出

-s、 --地位：

打印所有已知网络接口的当前状态。对于每个设备，它显示PCI域、总线、插槽和功能，以及设备的文本说明。根据设备是否由内核驱动程序、igb\_uio驱动程序或无驱动程序使用，将显示其他相关信息：\*Linux接口名称，例如if=eth0

\*正在使用的驱动程序，例如drv=igb\_uio\*当前未使用该设备的任何合适驱动程序

e、 g.unused=igb\_uio注意：如果此标志与绑定/取消绑定选项一起传递，则状态显示将始终在其他操作发生后出现。

-b driver，--bind=driver：选择要使用的驱动程序，或选择“无”解除设备绑定

-u、 --解除绑定：解除设备绑定（相当于“-b无”）

--强制：默认情况下，无法修改Linux使用的设备（如路由表中有路由所示）。使用--force标志将覆盖此行为，允许强制解除活动链接的绑定。警告：这可能会导致网络连接中断，应小心使用。

示例：

     ---------

显示当前设备状态：dpdk\_nic\_bind--status

要从当前驱动程序绑定eth1并使用igb\_uio dpdk\_nic\_bind--bind=igb\_uio eth1

解除0000:01:00.0与任何驱动程序dpdk\_nic\_bind的绑定-u 0000:01:00.0

将0000:02:00.0和0000:02:00.1绑定到ixgbe内核驱动程序dpdk\_nic\_bind-b ixgbe 02:00.0 02:00。

#### 5.2. DPDK设备配置

包dpdk提供了init脚本，可以简化设备分配和巨大页面的配置。它还使它们能够持久地重新启动。

以下是配置网卡两个端口的文件/etc/dpdk/接口示例。一个带有uio\_pci\_generic，另一个带有vfio pci

#<bus>目前只支持“pci”

#指定总线上的设备id要绑定的驱动程序（vfio pci或uio#U pci#通用）

##请注意，两个与DPDK兼容的驱动程序uio\_pci\_generic和vfio pci#是linux image extra-<VERSION>包的一部分。

#默认情况下并不总是安装此软件包-例如在云图像中因此，请安装它，以防您遇到丢失的模块问题。

##<bus><id><driver>pci 0000:04:00.0 uio#U pci#U通用pci 0000:04:00.1 vfio pci

卡由其PCI-ID标识。如果您不确定，可以使用工具dpdk\_nic\_bind显示当前可用的设备以及分配给它们的驱动程序。

**dpdk\_nic\_绑定--状态**

使用DPDK兼容驱动程序的网络设备

=================================================0000:04:00.0&apos;以太网控制器万兆X540-AT2&apos;drv=uio\U pci\U通用未使用=ixgbe

使用内核驱动程序的网络设备

========================0000:02:00.0“NetXtreme BCM5719千兆以太网PCIe”if=eth0 drv=tg3 unused=uio\_pci\_generic\*Active\*0000:02:00.1“NetXtreme BCM5719千兆以太网PCIe”if=eth1 drv=tg3 unused=uio\_pci\_generic 0000:02:00.2“NetXtreme BC719千兆以太网PCIe”if=eth2 drv=tg3=unused=uio\_pci\_generic:00:00“NetXtreme BCM5719千兆以太网PCIe”if=eth3 drv=tg3 unused=uio\_pci\_generic 0000:04:00.1“以太网控制器10千兆X540-AT2”if=eth5 drv=ixgbe unused=uio\_pci\_generic

其他网络设备=====================

<none>

#### 5.3. DPDK HugePage配置

DPDK大量使用巨大的页面来消除TLB上的压力。因此，必须在系统中配置hugepages。

dpdk包有一个配置文件和脚本，它们试图以/etc/dpdk/dpdk.conf的形式简化dpdk的hugepage配置。如果系统中hugepages的使用者多于DPDK，或者对hugepages的设置有非常特殊的要求，那么您可能希望自己分配/控制它们。如果没有，这将大大简化DPDK的配置，以满足您的需求。

这里是一个配置1024个Hugepages（每个页面2M）和4个1G页面的示例。

页数=1024页

NR\_1G\_页面=4

如图所示，它支持配置2M和更大的1G hugepages（或两者的混合）。它将确保有合适的hugetlbfs装入点供DPDK查找这两种大小，而不管默认的巨大页面大小是多少。如果您想通过内核参数手动分配hugepages，配置文件本身包含有关某些特殊情况的更多详细信息和一些提示。

这取决于您需要的大小-1G页面在TLB压力方面肯定更有效。但有报道称它们在DPDK内存中碎裂。此外，在系统生命周期的后期，要获得足够的可用空间来设置一定数量的1G页面可能会更加困难。

#### 5.4. 编译DPDK应用程序

目前DPDK库的稳定和发布的消费者并不多。OpenVswitch DPDK是一个例外（见下文），但一般来说，您可能希望/必须针对库编译应用程序。

您经常会找到一些指南，告诉您获取DPDK源，根据需要构建它们，并通过为构建系统设置值RTE\_\*最终基于DPDK构建应用程序。由于Ubunutu为您提供了一个已经编译好的DPDK，您可以跳过所有这些。为了简化正确变量的设置，您可以在构建应用程序之前获取文件/usr/share/dpdk/dpdk-sdk-env.sh的源代码。这里是构建随dpdk文档包提供的l2fwd示例应用程序的摘录。

sudo apt get安装dpdk dev libdpdk dev/usr/share/dpdk/dpdk-sdk-env.sh make-C/usr/share/dpdk/examples/l2fwd

根据您构建的内容，在make之前安装所有DPDK构建依赖项可能是一个很好的补充。

sudo-apt-get-install-build-dep-dpdk

#### 5.5. OpenV开关DPDK

作为一个图书馆，它自己做的事情并不多，所以它依赖于利用它的新兴项目。Ubuntu 16.04版本中已经捆绑的库的一个消费者是OpenVswitch，在OpenVswitch switch DPDK包中支持DPDK。

下面是一个如何使用DPDK安装和配置基本OpenVswitch的示例，供以后通过libvirt/qemu-kvm使用。

sudo apt get安装openvswitch开关dpdk

sudo更新替代方案--设置ovs-vswitchd/usr/lib/openvswitch-switch-dpdk/ovs-vswitchddpdk

echo“DPDK\_OPTS=”--DPDK-c 0x1-n 4-m 2048--vhost所有者libvirt qemu:kvm--vhost perm 0664’”| sudo tee-a/etc/default/openvswitch switch sudo service openvswitch switch restart

请记住，在重新启动之前，必须将设备分配给与DPDK兼容的驱动程序（见上文）。

--vhost-owner-libvirt-qemu:kvm--vhost-perm 0664部分将设置具有所有者/权限的vhost\_用户端口，以与Ubuntus兼容，从而以降低权限的方式运行qemu-kvm/libvirt，从而提高安全性。

请注意，-m 2048节是单插座系统最基本的numa设置。如果您有多个套接字，您可能需要定义如何在它们之间分割内存，例如-m 1024、1024。请注意，DPDK将尝试仅使用其使用的网卡的本地内存（出于性能原因）。也就是说，如果你有多个节点，但是所有的网卡上都有一个，你应该考虑推广你的卡。如果没有，则至少将内存分配给卡所在的节点，例如，在双节点all-to节点#2:-m 0，2048中。您可以使用hwloc nox软件包中的工具lstopo查看卡位于哪个插座上。

您现在启动的OpenVswitch支持OpenVswitch通常支持的所有端口类型，以及DPDK端口类型。这里是一个如何创建网桥的示例，并向其添加一个外部DPDK端口，而不是一个普通的外部端口。

ovs vsctl add br ovsdpdkbr0--设置网桥OVSDKBR0数据路径类型=netdev ovs vsctl add端口ovsdpdkbr0 dpdk0--设置接口dpdk0类型=dpdk

在OpenVSwitch中启用DPDK在版本2.6中已更改。因此，对于版本>=16.10的用户，以及Ubuntu云存档[72]>=neutron的用户来说，与Ubuntu 16.04的用户相比，启用功能已经改变。以前通过DPDK\_OPTS传递的选项现在通过ovs vsctl配置到开放的vSwitch配置数据库中。

与上述相同的示例以新的方式如下所示：

#启用DPDK

ovs vsctl设置打开开关。“其他配置：dpdk init=true”#在核心0上运行

ovs vsctl设置打开开关。“其他配置：dpdk lcore mask=0x1”#分配2G大页面（不支持Numa节点）

ovs vsctl设置打开开关。“other\_config:dpdk alloc mem=2048”#vhost用户套接字的组/权限（需要与libvirt/qemu一起使用）ovs vsctl set Open\_vSwitch.#“其他配置：dpdk extra=--vhost所有者libvirt qemu:kvm--vhost perm 0666”

有关更多详细信息，请参阅软件包提供的相关上游文档和vswitch配置手册页：

•/usr/share/doc/openvswitch common/INSTALL.DPDK.md.gz

•/usr/share/doc/openvswitch common/INSTALL.DPDK-ADVANCED.md.gz

• **man ovs-vswitchd.conf.db**

#### 5.6. OpenVswitch DPDK到KVM来宾

如果您没有在DPDK上构建某种SDN交换机或NFV，则很可能希望将流量转发给KVM客户。好消息是，在Ubuntu 16.04的新qemu/libvirt/dpdk/openvswitch版本中，不再需要手动添加命令行字符串。本章介绍如何将KVM客户机连接到OpenVswitch DPDK实例的基本配置。

DPDK/vhost\_用户必须有共享的hugepages支持来宾工作。一般来说，为了确保libvirt/qemu-kvm找到合适的hugepage挂载点，您可以在/etc/default/qemu-kvm中启用kvm\_-hugepage。然后重新启动服务以获取更改的配置。

sed-ri-e的，（KVM\_HUGEPAGES=）.\*，\11，/etc/default/qemu-KVM服务qemu-KVM-restart

为了让guest得到hugepages的支持，最近的libvirt现在也支持hugepages，只需将以下代码片段添加到您的VirshXML（或您使用的等效libvirt接口）中即可。这些XML还可以用作模板，以便使用“uvt kvm create”轻松生成来宾。

<numa><cell id=&apos;0&apos;cpu=&apos;0&apos;内存=&apos;6291456&apos;单元=&apos;KiB&apos;内存访问=&apos;shared&apos;/>

</numa>

[...]

<memoryBacking>

<hugepages><page size=“2”unit=“M”nodeset=“0”/

</hugepages></memoryBacking>

访问KVM客户机的新方法和推荐方法是使用vhost\_用户。这将导致DPDK创建qemu将来宾连接到的套接字。下面是一个如何将这样的端口添加到您创建的网桥的示例（请参见上文）。

ovs vsctl添加端口ovsdpdkbr0 vhost-user-1——设置接口vhost-user-1类型=dpdkvhostuser

这将在/var/run/openvswitch/vhost-user-1处创建vhost\_用户套接字

要让libvirt/kvm使用此套接字并为其创建来宾virtio网络设备，请在来宾定义中添加一个类似这样的片段作为网络定义。

<interface type=&apos;vhostuser&apos;><source type=&apos;unix&apos;

path=&apos;/var/run/openvswitch/vhost-user-1&apos;mode=&apos;client&apos;/><model type=&apos;virtio&apos;/>

</interface>

#### 5.7. KVM来宾中的DPDK

如果您无法访问支持DPDK的网卡，您仍然可以使用支持virtio的DPDK。为此，您必须创建由hugepages支持的来宾（见上文）。

除此之外，还要求至少有SSE3。qemu/libvirt使用的默认CPU型号仅限于SSE2。因此，您必须定义一个通过适当特性标志的模型——当然还有一个支持它的主机系统。可以在以下virshxml（或您使用的等效virsh接口）的代码片段中找到一个示例。

<cpu模式=&apos;host-passthrough&apos;>

此示例非常具有攻击性，通过了所有主机功能。这反过来又使得客户机不太容易迁移，因为目标机也需要所有的功能。“更软”的方法是只将sse3添加到默认模型中，如以下示例所示。

<cpu模式=&apos;custom&apos;匹配=&apos;exact&apos;>

<model fallback=&apos;allow&apos;>qemu64</model><feature policy=&apos;require&apos;name=&apos;ssse3&apos;/>

</cpu>

此外，virtio现在支持多队列，DPDK反过来可以利用多队列提高速度。要修改普通virtio定义以拥有多个队列，请将以下内容添加到接口定义中。这是关于增强一个正常的virtio nic，使其具有多个队列，以便稍后由来宾中的DPDK使用。

<driver name=“vhost”队列=“4”/

#### 5.8. 调谐OpenV开关DPDK

DPDK有很多选项-与Openvswitch DPDK结合使用时，最常用的两个选项是：

ovs vsctl设置打开开关。其他配置：n-dpdk-rxqs=2 ovs vsctl设置打开开关。其他配置：pmd cpu掩码=0x6

第一个选择每个DPDK接口要使用多少rx队列，而第二个控制运行PMD线程的数量和位置。上面的示例将利用两个rx队列并在CPU 1和2上运行PMD线程。有关更多信息，请参阅本文档末尾“EAL命令行选项”和“OpenVswitch DPDK安装”的参考链接。

与往常一样，对于调优，您必须非常了解您的系统和工作负载-因此，请验证工作负载与实际用例匹配的任何调优。

#### 5.9. 支持和故障排除

DPDK是一个快速发展的项目。在搜索支持和进一步指南的任何情况下，强烈建议首先检查它们是否适用于当前版本。

•DPDK邮件列表[73][74]

•针对OpenVswitch DPDK OpenStack邮件列表39

•DPDK发射台区域的已知问题[75]

•加入freenode上的IRC频道#DPDK或#openvswitch。

问题通常是由于常规设置中缺少小细节造成的。后来，这些缺失的细节会导致问题，很难找到其根本原因。常见的情况似乎是“无法打开网络设备dpdk0（无此类设备）”问题。在使用DPDK在Open vSwitch中设置端口时，这种情况发生得相当晚。但根本原因大部分时间是在设置和初始化的早期。这里是一个正确初始化设备的示例—在启用DPDK的情况下启动Open vSwitch时，可以在syslog/journal中找到这一点。

ovs ctl[3560]：EAL:NUMA套接字上的PCI设备0000:04:00.1 0 ovs ctl[3560]：EAL:probe驱动程序：8086:1528 rte\_ixgbe\_pmd ovs ctl[3560]：EAL:PCI内存映射在0x7F214000000 ovs ctl[3560]：EAL:PCI内存映射在0x7f2140200000

如果由于被忽略的卡、初始化失败或其他原因而丢失，则以后将没有DPDK设备可供参考。不幸的是，日志分布在syslog/journal和openvswitch日志中。为了允许在这里进行交叉检查，可以在这些日志中找到与输入的命令相关的示例。

#注意：此日志带有dpdk 2.2和openvswitch 2.5标题：

CMD：您输入的

系统日志：（包括EAL和OVS消息）OVS-LOG：（Openvswitch消息）

#准备将接口绑定到DPDK UIO驱动程序，使Hugepages可用，在OVS CMD:sudo服务openvswitch开关重新启动时启用DPDK

SYSLOG:2016-01-22T08:58:31.372Z | 00003 | daemon | u unix（monitor）| INFO | pid 3329死亡、死亡（终止），退出2016-01-22T08:58:33.377Z | 00002 | vlog INFO |打开的日志文件/var/log/openvswitch/ovsvswitchd.log 2016-01-22T08:58:33.381Z | u numa 1240CPU节点上发现的12个内核

2016-01-22T08:58:33.381Z | 00004 | ovs | U numa | INFO |发现1个numa节点和12个CPU内核2016-01-22T08:58:33.381Z | 00005 |重新连接| INFO | unix:/var/run/openvswitch/db.sock:正在连接。。。2016-01-22T08:58:33.383Z | 00006 |重新连接|信息| unix:/var/run/openvswitch/db.sock:connected 2016-01-22T08:58:33.386Z | 00007 | bridge | INFO | ovs vSwitch 2.5.0

OVS-LOG：

systemd[1]：正在停止打开V开关。。。systemd[1]：停止打开V开关。systemd[1]：停止打开V开关内部单元。。。

ovs ctl[3541]：\*终止ovs vswitchd（3329）ovs ctl[3541]：\*终止ovsdb服务器（3318）系统D[1]：停止打开vSwitch内部单元。systemd[1]：启动打开的V开关内部单元。。。

ovs ctl[3560]：\*启动ovsdb服务器ovs vsctl:ovs | 00001 | vsctl | INFO |称为ovs vsctl--无等待--初始化--设置打开|。

db版本=7.12.1

ovs vsctl:ovs | 00001 | vsctl | INFO |称为ovs vsctl--无等待设置打开| vSwitch。ovsversion=2.5.0“外部id:系统id=\”e7c5ba80-bb14-45c1-b8eb-628f3ad03903\“系统类型=\”Ubuntu\“系统版本=\”16.04-xenial\“ovs ctl[3560]：\*配置开放式虚拟交换机系统id

ovs ctl[3560]：2016-01-22T08:58:31Z | 00001 | dpdk | INFO | No-提供的vhost\_sock\_dir-默认为/var/run/openvswitch

ovs VSwitch:ovs | 00001 | dpdk | INFO | No-提供了vhost|u sock|u dir-默认为/var/run/openvswitch

ovs ctl[3560]：EAL:在插槽0 ovs ctl[3560]上将lcore 0检测为core 0:EAL:在插槽0 ovs ctl[3560]上将lcore 1检测为core 1:EAL:在插槽0 ovs ctl[3560]上将lcore 2检测为core 2:EAL:在插槽0 ovs ctl[3560]上将lcore 3检测为core 4:：EAL:在插槽0 ovs ctl[3560]上检测到lcore 5作为核心5:EAL:在插槽0 ovs ctl[3560]上检测到lcore 6作为核心0:EAL:在插槽0 ovs ctl[3560]上检测到lcore 7作为核心1:EAL:在插槽0 ovs ctl[3560]上检测到lcore 9作为核心3:EAL:在插槽0 ovs ctl上检测到lcore 10作为核心4[3560]：EAL:在套接字0 ovs ctl[3560]上检测到lcore 11作为核心5:EAL:按配置最多支持128个逻辑核心。

ovs ctl[3560]：EAL:检测到12个lcore ovs ctl[3560]：EAL:未全部加载VFIO模块，跳过VFIO支持…ovs ctl[3560]：EAL:设置物理连续内存…ovs ctl[3560]：EAL:请求0x100000000字节的虚拟区域

ovs ctl[3560]：EAL:在0x7F204000000（大小=0x100000000）处找到虚拟区域ovs ctl[3560]：EAL:从套接字0请求大小为1024MB的4页ovs ctl[3560]：EAL:TSC频率为~2397202 KHz ovs VSwitch[3592]：EAL:TSC频率为~2397202 KHz

ovs-vswitchd[3592]：EAL:Master lcore 0已就绪（tid=fc6cbb00；cpuset=[0]）ovs-vswitchd[3592]：EAL:PCI设备0000:04:00.0在NUMA套接字上0 ovs-vswitchd[3592]：EAL:probe-driver:8086:1528 rte\_ixgbe\_pmd-ovs-vswitchd[3592]：EAL:不受支持的内核驱动程序管理，跳过了ovs-vswitchd[3592]：EAL:PCI设备0000:04:00.1在NUMA套接字上0 ovs vswitchd[3592]：EAL:probe驱动程序：8086:1528 rte\_ixgbe\_pmd ovs vswitchd[3592]：EAL:PCI内存映射在0x7F214000000 ovs vswitchd[3592]：EAL:PCI内存映射在0x7f2140200000 ovs ctl[3560]：主lcore 0已就绪（tid=fc6cbb00；cpuset=[0]）ovs ctl[3560]：EAL:NUMA套接字0 ovs ctl上的PCI设备0000:04:00.0[3560]：EAL:probe驱动程序：8086:1528 rte\_ixgbe\_pmd ovs ctl[3560]：EAL:不受支持的内核驱动程序管理，跳过了ovs ctl[3560]：EAL:NUMA套接字0 ovs ctl上的PCI设备0000:04:00.1[3560]：EAL:probe驱动程序：8086:1528 rte\_ixgbe\_pmd ovs ctl[3560]：EAL:PCI内存映射到0x7F214000000 ovs ctl[3560]：EAL:PCI内存映射到0x7f2140200000 ovs vswitchd[3592]：PMD:eth\_ixgbe\_dev\_init（）：MAC:4，PHY:3

ovs vswitchd[3592]：PMD:eth\_ixgbe\_dev\_init（）：端口0 vendorID=0x8086 deviceID=0x1528 ovs ctl[3560]：PMD:eth\_ixgbe\_dev\_init（）：MAC:4，PHY:3

ovs ctl[3560]：PMD:eth\_ixgbe\_dev\_init（）：端口0 vendorID=0x8086 deviceID=0x1528 ovs ctl[3560]：区域0：名称：<RG\_MP\_log\_history>，物理：0x83fffdec0，len:0x2080，virt:0x7f213fffdec0，套接字id:0，标志：0

ovs ctl[3560]：区域1:名称：<MP\_log\_history>，物理：0x83fd73d40，len:0x28a0c0，virt:0x7f213fd73d40，套接字id:0，标志：0

ovs ctl[3560]：区域2:名称：<rte\_eth\_dev\_data>，物理：0x83fd43380，len:0x2f700，virt:0x7f213fd43380，套接字id:0，标志：0 ovs ctl[3560]：\*启动ovs vswitchd ovs ctl[3560]：\*启用远程OVSDB管理器systemd[1]：启动打开vSwitch内部单元。systemd[1]：启动打开vSwitch…systemd[1]：启动打开vSwitch。

CMD:sudo ovs vsctl add br ovsdpdkbr0--设置网桥ovsdpdkbr0数据路径\u type=netdev SYSLOG:

2016-01-22T08:58:56.344Z | 00008 |内存|信息| 37256 kB峰值驻留设置24.5秒后的大小2016-01-22T08:58:56.346Z | 00009 |原始dpif |信息|netdev@ovs-netdev:Datapath支持再循环2016-01-22T08:58:56.346Z | 00010 | of proto|u dpif | INFO|netdev@ovs-netdev:MPLS标签堆栈长度探测为3 2016-01-22T08:58:56.346Z | 00011 | of proto|u dpif | INFO|netdev@ovs-netdev:Datapath支持唯一的流ID 2016-01-22T08:58:56.346Z | 00012 | of proto|u dpif | INFO|netdev@ovs-netdev:Datapath不支持ct\_state 2016-01-22T08:58:56.346Z|00013|of proto\_dpif|INFO|netdev@ovs-netdev:Datapath不支持ct\_zone 2016-01-22T08:58:56.346Z | 00014 | of proto\_dpif | INFO|netdev@ovs-netdev:数据路径不存在支持项目dpif信息的ct|U标记2016-01-22T08:58:56.346Z | 00015 ||netdev@ovs-netdev:Datapath不支持ct\_标签2016-01-22T08:58:56.360Z | 00016 | bridge | INFO | bridge ovsdpdkbr0:在端口65534 2016-01-22T08:58:56.361Z | 00017 | INFO | bridge ovsdpdkbr0:使用数据路径ID

00005a4a1ed0a14d 2016-01-22T08:58:56.361Z | 00018 | connmgr | INFO | ovsdpdkbr0：添加服务控制器“punix:/var/run/openvswitch/ovsdpdkbr0.mgmt”

OVS-LOG:OVS vsctl:OVS | 00001 | vsctl | INFO |称为OVS vsctl add br ovsdpdkbr0--设置网桥ovsdpdkbr0数据路径\_type=netdev

systemd udevd[3607]：无法为ovs netdev生成持久MAC地址：没有这样的文件或目录

内核：[50165.886554]设备ovs netdev进入混杂模式内核：[50165.901261]设备ovsdpdkbr0进入混杂模式

CMD:sudo ovs vsctl add port ovsdpdkbr0 dpdk0--设置接口dpdk0 type=dpdk

SYSLOG:2016-01-22T08:59:06.369Z | 00019 |内存|信息|峰值驻留集大小在过去10.0秒内增长了155%，从37256KB增长到95008KB 2016-01-22T08:59:06.369Z | 00020 |内存|信息|处理程序：4个端口：1个重新验证程序：2个规则：5

2016-01-22T08:59:30.989Z | 00021 | dpdk | INFO |端口0:8c:dc:d4:b3:6d:e9

2016-01-22T08:59:31.520Z | 00022 | dpdk | INFO |端口0:8c:dc:d4:b3:6d:e9

2016-01-22T08:59:31.521Z | 00023 | dpif | u netdev | INFO |在numa节点0上创建了1个pmd线程

2016-01-22T08:59:31.522Z | 00001 | dpif | u netdev（pmd16）| INFO | Core 0处理端口&apos;dpdk0&apos;2016-01-22T08:59:31.522Z | 00024 | bridge | INFO | bridge ovsdpdkbr0:在端口上添加了接口dpdk0

1 2016-01-22T08:59:31.522Z | 00025 |桥|信息|桥ovsdpdkbr0:使用数据路径ID

00008cdcd4b36de9 2016-01-22T08:59:31.523Z | 00002 | dpif | u netdev（pmd16）| INFO |核心0处理端口“dpdk0”

OVS-LOG:OVS vsctl:OVS | 00001 | vsctl | INFO |称为OVS vsctl添加端口ovsdpdkbr0 dpdk0--设置

接口dpdk0类型=dpdk

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a79ebc0 hw\_ring=0x7f211a7a6c00 dma\_addr=0x81a7a6c00

ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：使用简单的发送代码路径ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：向量发送已启用。ovs-vswitchd[3595]：PMD:ixgbe\u-dev\u-rx\u队列设置（）：sw\u-ring=0x7f211a78a6c0 sw\u-sc\u-ring=0x7f211a786580 hw\u-ring=0x7f211a78e800

ovs vswitchd[3595]：PMD:ixgbe\_set\_rx\_function（）：向量rx已启用，请确保rx突发大小不小于4（端口=0）。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a79ebc0 hw\_ring=0x7f211a7a6c00 dma\_addr=0x81a7a6c00

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a76e4c0 hw\_ring=0x7f211a776500 dma\_addr=0x81a776500

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a756440 hw\_ring=0x7f211a75e480 dma\_addr=0x81a75e480

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a73e3c0 hw\_ring=0x7f211a746400 dma\_addr=0x81a746400

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a726340 hw\_ring=0x7f211a72e380 dma\_addr=0x81a72e380

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a70e2c0 hw\_ring=0x7f211a716300 dma\_addr=0x81a716300

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a6f6240 hw\_ring=0x7f211a6fe280 dma\_addr=0x81a6fe280

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a6de1c0 hw\_ring=0x7f211a6e6200 dma\_addr=0x81a6e6200

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a6c6140 hw\_ring=0x7f211a6ce180 dma\_addr=0x81a6ce180

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a6ae0c0 hw\_ring=0x7f211a6b6100 dma\_addr=0x81a6b6100

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a696040 hw\_ring=0x7f211a69e080 dma\_addr=0x81a69e080

ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：使用简单的发送代码路径ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：向量发送已启用。ovs-vswitchd[3595]：PMD:ixgbe\u-dev\u-tx\u队列设置（）：sw\u-ring=0x7f211a67dfc0-hw\u-ring=0x7f211a68600dma\u-addr=0x81a600

ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：使用简单的tx代码路径ovs vswitchd[3595]：PMD:ixgbe\_集\_tx\_函数（）：启用向量tx。

ovs vswitchd[3595]：PMD:ixgbe\_dev\_tx\_queue\_setup（）：sw\_ring=0x7f211a665e40 hw\_ring=0x7f211a66de80 dma\_addr=0x81a66de80

ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：使用简单的发送代码路径ovs-vswitchd[3595]：PMD:ixgbe\u-set\u-tx\u函数（）：向量发送已启用。ovs-vswitchd[3595]：PMD:ixgbe\u-dev\u-rx\u队列设置（）：sw\u-ring=0x7f211a78a6c0 sw\u-sc\u-ring=0x7f211a786580 hw\u-ring=0x7f211a78e800

ovs vswitchd[3595]：PMD:ixgbe\_set\_rx\_function（）：向量rx已启用，请确保rx突发大小不小于4（端口=0）。

CMD:sudo ovs vsctl add port ovsdpdkbr0 vhost-user-1--设置接口vhost-user-1 type=dpdkvhostuser

OVS-LOG:2016-01-22T09:00:35.145Z | 00026 | dpdk | INFO | Socket/var/run/openvswitch/vhost-user-1为vhost用户端口vhost-user-1 2016-01-22T09:00:35.145Z | 00003 | dpif | u netdev（pmd16）| INFO |核心0处理端口“dpdk0”

2016-01-22T09:00:35.145Z | 00004 | dpif | u netdev（pmd16）| INFO | Core 0处理端口“vhost-user-1”2016-01-22T09:00:35.145Z | 00027 | bridge | INFO | bridge ovsdpdkbr0:在端口2上添加了接口vhost-user-1

SYSLOG:ovs vsctl:ovs | 00001 | vsctl | INFO |称为ovs vsctl add port ovsdpdkbr0 vhost-user-1--设置接口vhost-user-1 type=dpdkvhostuser ovs vswitchd[3595]：vhost|CONFIG:socket created，fd:46

ovs vswitchd[3595]：VHOST\_配置：绑定到/var/run/openvswitch/VHOST-user-1

最终我们可以在顶部看到轮询线程

PID用户PR NI VIRT RES SHR S%CPU%MEM TIME+命令3595根10-10 4975344 103936 9916 S 100.0 0.3 33:13.56 ovs VSwitched

#### 5.10.资源

•DPDK文件[76]

•与Ubuntu 16.04[77]中的版本包相匹配的发行说明

•Linux DPDK用户入门[78]

•EAL命令行选项[79]

•DPDK Api文件[80]

•OpenVswitch DPDK安装[81]

•维基百科对DPDK的定义[82]

# 第5章DM多路传输

## 1.设备映射器多路径

设备映射器多路径（DM多路径）允许您将服务器节点和存储阵列之间的多个I/O路径配置到单个设备中。这些I/O路径是物理SAN连接，可以包括单独的电缆、交换机和控制器。Multipathing聚合I/O路径，创建由聚合路径组成的新设备。本章概述了e在Ubuntu Server 12.04的初始版本中新增的DM Multipath功能。接下来，本章提供DM Multipath及其组件的高级概述，以及DM Multipath设置的概述。

#### 1.1.Ubuntu服务器12.04的新增和更改功能

从多路径-0.4.8迁移到多路径-0.4.9

##### 1.1.1.从0.4.8迁移

优先级检查器不再作为独立二进制文件运行，而是作为共享库运行。此功能的键值名称也略有更改。将名为prio\_callout的属性复制到prio，同时修改参数优先级检查器的名称，不再需要系统路径。转换示例：

设备{供应商“NEC”产品“磁盘阵列”

prio\_标注mpath\_prio\_alua/dev/%n prio alua}

有关完整列表，请参见表优先级检查器转换[p.76]

##### **表5.1.优先级检查器转换**

|  |  |  |
| --- | --- | --- |
| **v0.4.8** |  | **v0.4.9** |
| **优先级调出mpath\u优先级\u emc/dev/%n** | **prio emc** |  |
| **优先级标注mpath\u prio\u alua/dev/%n** | **普里奥阿鲁阿** |  |
| **优先调用mpath\u优先调用netapp/dev/%n** | **prio netapp** |  |
| **优先级标注mpath\u prio\u rdac/dev/%n** | **prio rdac** |  |
| **优先级调出mpath\u优先级hp\u sw/dev/%n** | **普里奥hp\_sw** |  |
| **优先级调出mpath\u优先级hds\u模块%b** | **prio hds** |  |

由于多路径配置文件解析器基本上解析它找到的所有键/值对，然后使用它们，因此prio\_callout和prio共存是安全的，建议在开始迁移之前插入prio属性。之后，您可以安全地删除旧的prio\_callout属性，而不会中断服务。

#### 1.2.概述

DM多路径可用于提供：

•DM Multipath可以在主/被动配置中提供故障切换。在主/被动配置中，任何时候只有一半的路径用于I/O。如果I/O路径的任何元素（电缆、交换机或控制器）出现故障，DM Multipath将切换到备用路径。*冗余*

•可在主动/主动模式下配置Performance DM Multipath，其中I/O以循环方式分布在路径上。在某些配置中，DM Multipath可检测I/O路径上的负载并动态重新平衡负载。*改进的性能*

#### 1.3.存储阵列概述

默认情况下，DM Multipath包括对支持DM Multipath的最常见存储阵列的支持。

支持的设备可以在multipath.conf.defaults文件中找到。如果您的存储阵列支持DMMultipath，并且默认情况下未在此文件中配置，则可能需要将其添加到DM multipath配置文件multipath.conf中。有关DM multipath配置文件的信息，请参阅DM multipath配置文件一节。有些存储阵列需要特殊处理I/O错误和路径切换。这些需要单独的硬件处理器内核模块。

#### 1.4.DM多路径组件

表DM Multipath Components描述了DM Multipath包的组件。

##### **表5.2.DM多路径组件**

|  |  |
| --- | --- |
| **组成部分** | **描述** |
| **dm\_多路径内核模块** | 重新路由I/O并支持路径和路径组的故障切换。 |
| **多路径命令** | 列出并配置多路径设备。通常使用/etc/rc.sysinit启动，也可以在添加块设备时由udev程序启动，或者可以由initramfs文件系统运行。 |
| **多路径守护进程** | 监视路径；当路径发生故障并返回时，它可能会启动路径组开关。提供对多路径设备的交互式更改。必须重新启动此守护程序才能使对/etc/multipath.conf文件的任何更改生效。 |
| **kpartx命令** | 为设备上的分区创建设备映射器设备对于具有DM Multipath的基于DOS的分区，必须使用此命令。kpartx在其自己的包中提供，但Multipath tools包依赖于它。 |

#### 1.5.DM多路径设置概述

DM Multipath包括适用于常见多路径配置的默认编译设置。设置DM Multipath通常是一个简单的过程。使用DM Multipath配置系统的基本过程如下：

##### 1.安装多路径工具和多路径工具启动包

2.    创建一个空的配置文件/etc/multipath.conf，它重新定义以下内容

3.    如有必要，编辑multipath.conf配置文件以修改默认值并保存更新的文件。

4.    启动多路径守护进程

5.    更新初始ramdisk

有关多路径配置的详细设置说明，请参阅“设置DM多路径”一节。

## 2.多路径设备

如果没有DM Multipath，系统会将从服务器节点到存储控制器的每条路径视为单独的设备，即使I/O路径将同一服务器节点连接到同一存储控制器。DMMultipath提供了一种逻辑组织I/O路径的方法，方法是在底层设备之上创建一个多路径设备。

#### 2.1. 多路径设备标识符

每个多路径设备都有一个全球通用标识符（WWID），该标识符保证全局唯一且不变。默认情况下，多路径设备的名称设置为其WWID。或者，您可以在多路径配置文件中设置用户友好的名称选项，这会导致DM multipath使用形式为mpathn的nodeunique别名作为名称。例如，具有两个HBA的节点通过单个未分区FC交换机连接到具有两个端口的存储控制器，可以看到四个设备：/dev/sda、/dev/sdb、/dev/sdc和/dev/sdd。DM Multipath创建具有唯一WWID的单个设备，该设备根据多路径配置将I/O重新路由到这四个基础设备。当“用户友好名称”配置选项设置为“是”时，多路径设备的名称设置为mpathn。当新设备处于DM Multipath的控制之下时，可以在/dev目录：/dev/mapper/mpathn和/dev/DM-n下的两个不同位置看到新设备。

•在引导过程的早期创建/dev/mapper中的设备。使用这些设备访问多路径设备，例如在创建逻辑卷时。

•任何形式为/dev/dm-n的设备仅供内部使用，不得使用。

有关多路径配置默认值（包括用户友好的名称配置选项）的信息，请参阅“配置文件默认值”部分。您还可以使用多路径配置文件的多路径部分中的别名选项，将多路径设备的名称设置为您选择的名称。有关多路径配置文件的多路径部分的信息，请参阅多路径设备配置属性部分。

#### 2.2. 群集中一致的多路径设备名称

当user\u friendly\u names configuration（用户友好名称配置）选项设置为yes（是）时，多路径设备的名称对于节点是唯一的，但不能保证在使用多路径设备的所有节点上都相同。类似地，如果在multipath.conf配置文件的multipath部分中为设备设置别名选项，则名称不会自动在集群中的所有节点上保持一致。如果您使用LVM从多路径设备创建逻辑设备，这不会造成任何困难，但如果您要求多路径设备名称在每个节点中保持一致，建议您将“用户友好名称”选项设置为“否”，并且不要为设备配置别名。默认情况下，如果未将“用户友好名称”设置为“是”，或未为设备配置别名，则设备名称将是设备的WWID，并且始终相同。但是，如果希望系统定义的用户友好名称在群集中的所有节点上保持一致，则可以执行以下步骤：

1.    在一台机器上设置所有多路径设备。

2.    通过运行以下命令禁用其他计算机上的所有多路径设备：

#systemctl停止多路径工具服务

#多路径F

3.    将/etc/multipath/bindings文件从第一台计算机复制到群集中的所有其他计算机。

4.    通过运行以下命令，在群集中的所有其他计算机上重新启用multipathd守护程序：

#systemctl启动多路径工具.service

如果添加新设备，则需要重复此过程。

类似地，如果要为要在群集中的节点之间保持一致的设备配置别名，则应按照相同的过程确保群集中每个节点的/etc/multipath.conf文件相同：

1.    在一台计算机上的multipath.conf文件中为中的多路径设备配置别名。

2.    通过运行以下命令禁用其他计算机上的所有多路径设备：

#systemctl停止多路径工具服务

#多路径F

3.    将multipath.conf文件从第一台计算机复制到群集中的所有其他计算机。

4.    通过运行以下命令，在群集中的所有其他计算机上重新启用multipathd守护程序：

#systemctl启动多路径工具.service

添加新设备时，需要重复此过程。

#### 2.3. 多路径设备属性

除了用户友好的名称和别名选项外，多路径设备还具有许多属性。通过在多路径配置文件的多路径部分中为特定多路径设备创建条目，可以修改该设备的这些属性。有关多路径配置文件的多路径部分的信息，请参阅“配置文件多路径属性”部分。

#### 2.4. 逻辑卷中的多路径设备

创建多路径设备后，可以使用多路径设备名称，就像创建LVM物理卷时使用物理设备名称一样。例如，如果/dev/mapper/mpatha是多路径设备的名称，则以下命令将/dev/mapper/mpatha标记为物理卷。

#pvcreate/dev/mapper/mpatha

您可以在创建LVM卷组时使用生成的LVM物理设备，就像使用任何其他LVM物理设备一样。

如果尝试在已配置分区的整个设备上创建LVM物理卷，pvcreate命令将失败。

创建使用主动/被动多路径阵列作为底层物理设备的LVM逻辑卷时，应在LVM.conf中包含筛选器，以排除多路径设备底层的磁盘。这是因为，如果阵列在接收I/O时自动将主动路径更改为被动路径，则当LVM扫描被动路径时，如果这些设备未被过滤，多路径将进行故障切换和回切。对于需要命令使被动路径处于活动状态的主动/被动阵列，发生这种情况时，LVM将打印一条警告消息。要筛选LVM配置文件（LVM.conf）中的所有SCSI设备，请在该文件的设备部分包括以下筛选器。

过滤器=[“r/block/”、“r/disk/”、“r/sd.\*/”、“a/\*/”]

在更新/etc/lvm.conf之后，有必要更新initrd，以便在引导期间将此文件复制到过滤器最重要的位置。执行：更新initramfs-u-kall

每次更新/etc/lvm.conf或/etc/multipath.conf时，都应该重建initrd以反映这些更改。当需要黑名单和过滤器来保持稳定的存储配置时，这是必需的。

## 3.设置DM多路径概述

本节提供配置DM多路径的分步示例过程。它包括以下程序：

•基本DM多路径设置

•忽略本地磁盘

•向配置文件中添加更多设备

#### 3.1. 设置DM多路径

在系统上设置DM Multipath之前，请确保系统已更新并包含Multipath tools包。如果需要从SAN引导，则还需要多路径工具引导包。

基本的/etc/multipath.conf甚至不需要存在，当运行multpath时没有附带的/etc/multipath.conf，它会从其内部数据库中提取以找到合适的配置，也会从其内部黑名单中提取。如果在没有配置文件的情况下运行multipath-ll，则不会发现多路径。必须继续增加详细程度，以发现为什么没有创建多路径。考虑引用SAN厂商的文档、在/Ur/St/Doc／多路径工具/示例中找到的多路径示例配置文件和Live Multuple数据库：

#echo&apos;show config&apos;| multipath-k>multipath.conf-live

要解决multipathd中的一个怪癖，当/etc/multipath.conf不存在时，前面的命令将不返回任何内容，因为它是/etc/multipath.conf和内存中的数据库合并的结果。要解决此问题，请使用touch定义一个空的/etc/multipath.conf，或创建一个重新定义默认值的文件，如：

默认值{

用户友好的名称否}

然后重新启动multipathd：

#systemctl重新启动multipath-tools.service

现在，“showconfig”命令将返回实时数据库。

#### 3.2. 使用多路径支持安装

要在安装期间启用多路径支持[83]，请使用

在安装程序提示下安装磁盘检测/multipath/enable=true。如果找到多路径设备，则在安装期间这些设备将显示为/dev/mapper/mpath<X>。

#### 3.3. 生成多路径设备时忽略本地磁盘

有些机器的内部磁盘有本地SCSI卡。这些设备不建议使用DM多路径。以下过程显示了如何在配置多路径时修改多路径配置文件以忽略本地磁盘。

1.确定哪些磁盘是内部磁盘，并将其标记为要列入黑名单的磁盘。在本例中，是内部磁盘。注意，正如在默认多路径配置文件中最初配置的那样，执行multipath-v2会在多路径映射中显示本地磁盘/dev/sda。有关多路径命令输出的更多信息，请参阅多路径命令输出一节。**/发展/社会发展局**

#多路径-v2

创建：SIBM-ESXSST336732LC\_uuuuuuuf3et0ep0q00007248bx1 undef WINSYS，SF2372 size=33 GB features=“0”hwhandler=“0”wp=undef`-+-policy=&apos;round-robin 0&apos;prio=1 status=undef |-0:0:0:0 sda 8:0[-----------

设备映射器ioctl cmd 9失败：无效参数设备映射器ioctl cmd 14失败：没有此类设备或地址创建：3600A0B80001327D8000006D43621677未定义WINSYS，SF2372 size=12G features=&apos;0&apos;hwhandler=&apos;0&apos;wp=unde`-+-policy=&apos;round-robin 0&apos;prio=1 status=undef

|-2:0:0:0 sdb 8:16未定义就绪运行“-3:0:0:0 sdf 8:80未定义就绪运行

创建：3600A0B80001327501000009A436215EC undef WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;优先级=1状态=undef

|-2:0:0:1 sdc 8:32未定义就绪运行“-3:0:0:1 sdg 8:96未定义就绪运行

创建：3600A0B80001327D80000070436216B3未定义WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;prio=1状态=未定义

|-2:0:0:2 sdd 8:48未定义就绪运行“-3:0:0:2 sdg 8:112未定义就绪运行

创建：3600A0B80001327501000009B4362163E undef WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;优先级=1状态=undef

|-2:0:0:3 sdd 8:64未定义就绪运行

`-3:0:0:3 sdg 8:128未定义就绪运行

2.    为了防止设备映射程序在其多路径映射中映射/dev/sda，请编辑/etc/multipath.conf文件的黑名单部分以包含此设备。虽然可以使用devnode类型将sda设备列入黑名单，但这不是安全的过程，因为/dev/sda在重新启动时不保证相同。要将单个的d列入黑名单，请执行以下操作：设备，您可以使用该设备的WWID将其列入黑名单。

请注意，在multipath-v2命令的输出中，/dev/sda设备的WWID为SIBMESXSST336732LC\_uuuuuuuuuuf3et0ep0q000072428bx1。要将此设备列入黑名单，请在

/etc/multipath.conf文件。

黑名单{

wwid SIBM-ESXSST336732LC\_uuuuuuuuuuf3et0ep0q000072428bx1}

3.    更新/etc/multipath.conf文件后，必须手动通知multipath守护程序重新加载该文件。

#systemctl重新加载多路径工具.service

4.    运行以下命令以删除多路径设备：

#多路径-f SIBM-ESXSST336732LC\_uuuuuuuuuF3ET0EP0Q000072428Bx1

5.    要检查设备删除是否有效，您可以运行multipath-ll命令以显示当前的多路径配置。有关multipath-ll命令的信息，请参阅multipath querys with multipath command一节。要检查黑名单上的设备是否没有被重新添加，您可以运行multipath命令，如以下示例所示。如果未指定-v选项，则多路径命令的详细级别默认为v2。

#多路径

创建：3600A0B80001327D8000006D43621677未定义WINSYS，SF2372 size=12G features=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;prio=1 status=undef

|-2:0:0:0 sdb 8:16未定义就绪运行“-3:0:0:0 sdf 8:80未定义就绪运行

创建：3600A0B80001327501000009A436215EC undef WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;优先级=1状态=undef

|-2:0:0:1 sdc 8:32未定义就绪运行“-3:0:0:1 sdg 8:96未定义就绪运行

创建：3600A0B80001327D80000070436216B3未定义WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;prio=1状态=未定义

|-2:0:0:2 sdd 8:48未定义就绪运行“-3:0:0:2 sdg 8:112未定义就绪运行

创建：3600A0B80001327501000009B4362163E undef WINSYS，SF2372大小=12G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=undef`-+-policy=&apos;round-robin 0&apos;优先级=1状态=undef

|-2:0:0:3 sdd 8:64未定义就绪运行

`-3:0:0:3 sdg 8:128未定义就绪运行

#### 3.4.配置存储设备

默认情况下，DM Multipath包括对支持DM Multipath的最常见存储阵列的支持。

默认配置值（包括支持的设备）可以在multipath.conf.defaults文件中找到。

如果需要将默认情况下不支持的存储设备添加为已知多路径设备，请编辑/etc/multipath.conf文件并插入适当的设备信息。

例如，要添加有关HP Open-V系列的信息，条目如下所示，其中%n是设备名称：

设备{设备{供应商“HP”产品“OPEN-V.”

getuid\u callout“/lib/udev/scsi\u id--whitelisted--device=/dev/%n”}

}

有关配置文件的设备部分的更多信息，请参阅配置文件设备部分[p.94]。

## 4.DM多路径配置文件

默认情况下，DM Multipath为Multipath的最常见用途提供配置值。此外，DM Multipath还包括对支持DM Multipath的最常见存储阵列的支持。

默认配置值和支持的设备可以在multipath.conf.defaults文件中找到。

您可以通过编辑/etc/Multipath.conf配置文件来覆盖DM Multipath的默认配置值。如有必要，您还可以将默认情况下不支持的存储阵列添加到配置文件中。本章提供了有关分析和修改Multipath.conf文件的信息。本章包含以下部分g主题：•配置文件概述[p.86]

• *配置文件黑名单[第87页]*

• *配置文件默认值[第89页]*

• *配置文件多路径属性[p.93]*

• *配置文件设备[p.94]*

在多路径配置文件中，您只需要指定配置所需的部分，或者您希望从multipath.conf.defaults文件中指定的默认值更改的部分。如果文件中有与您的环境无关的部分或者您不需要覆盖默认值的部分，则y您可以将它们注释掉，因为它们在初始文件中。

配置文件允许使用正则表达式描述语法。

配置文件的注释版本可以在/usr/share/doc/multipath tools/examples/multipath.conf.annotated.gz中找到。

#### 4.1.配置文件概述

多路径配置文件分为以下部分：

**黑名单**

不考虑多路径的特定设备列表。

##### **黑名单及例外情况**

根据黑名单部分的参数列出否则将被列入黑名单的多路径候选。

**默认值**

DM多路径的常规默认设置。

##### **多路径**

单个多路径设备特性的设置。这些值覆盖配置文件的“默认值”和“设备”部分中指定的内容。

##### **装置**

各个存储控制器的设置。这些值覆盖配置文件的“默认值”部分中指定的内容。如果您使用的存储阵列默认不受支持，则可能需要为阵列创建“设备”子部分。

当系统确定多路径设备的属性时，首先检查多路径设置，然后检查每设备设置，然后检查多路径系统默认设置。

#### 4.2.配置文件黑名单

多路径配置文件的“黑名单”部分指定系统配置多路径设备时将不使用的设备。列入黑名单的设备将不会分组到多路径设备中。

•如果您确实需要将设备列入黑名单，您可以根据以下标准执行此操作：

•根据WWID，如WWID黑名单所述[p.87]

•按设备名称，如按设备名称列入黑名单[p.87]

•按设备类型划分，如按设备类型划分的黑名单所述[p.88]

默认情况下，各种设备类型都会被列入黑名单，即使在您注释掉配置文件的初始黑名单部分之后也是如此。有关信息，请参阅按设备名称列入黑名单[p.87]

##### 4.2.1.按WWID列入黑名单

您可以通过配置文件的黑名单部分中的wwid条目，通过其全球标识将各个设备指定为黑名单。

以下示例显示配置文件中的行，这些行将WWID为26353900f02796769的设备列入黑名单。

黑名单{

wwid 26353900f02796769}

##### 4.2.2.按设备名称列入黑名单

您可以按设备名称将设备类型列入黑名单，以便通过在配置文件的黑名单部分指定devnode条目，不会将它们分组到多路径设备中。

以下示例显示了配置文件中的行，这些行将黑名单所有SCSI设备，因为它将黑名单所有sd\*设备。

黑名单{

devnode“^sd[a-z]”

您可以使用配置文件的黑名单部分中的devnode条目将单个设备指定为黑名单，而不是指定特定类型的所有设备。但是，不建议这样做，因为除非它由udev规则静态映射，否则无法保证特定设备在重新启动时具有相同的名称。例如，de重新启动时，设备名称可能从/dev/sda更改为/dev/sdb。

默认情况下，以下devnode条目在默认黑名单中编译；这些条目黑名单中的设备通常不支持DM Multipath。要在这些设备上启用Multipath，您需要在配置文件的blacklist\_exceptions部分中指定它们，如blacklist exceptions[p.88]中所述

黑名单{

devnode“^（ram | raw | loop | fd | md | dm | sr | scd | st）[0-9]\*“devnode”^hd[a-z]”

##### 4.2.3.按设备类型列出的黑名单

您可以在配置文件的黑名单部分使用设备部分指定特定的设备类型。

以下示例列出了所有IBM DS4200和HP设备的黑名单。

黑名单{设备{供应商“IBM”

产品“3S42”#DS4200产品10}设备{供应商“HP”产品“\*”}

}

##### 4.2.4.黑名单例外情况

您可以使用配置文件的blacklist\_exceptions部分在默认情况下已被列入黑名单的设备上启用多路径。

例如，如果您有大量设备，并且只想对其中一个设备进行多路径传输（WWID为3600d0230000000000e13955cc3757803），则可以将所有设备都列入黑名单，而不是单独将所需设备以外的每个设备列入黑名单，然后通过向/etc/multipath.conf文件中添加以下行，只允许您想要的一个。

黑名单{wwid“\*”}

黑名单及例外情况{

wwid“3600d0230000000000e13955cc3757803”}

在配置文件的“黑名单\u异常”部分中指定设备时，必须以与黑名单中指定的相同方式指定异常。例如，WWID异常将不适用于devnode黑名单条目指定的设备，即使黑名单设备与该WWID关联。类似地，devnode异常仅适用于devnode条目，而设备异常仅适用于设备条目。

#### 4.3. 配置文件默认值

/etc/multipath.conf配置文件包含一个defaults部分，该部分将user\u-friendly\u-names参数设置为yes，如下所示。

默认值{

用户友好的名称是}

这将覆盖用户友好名称参数的默认值。

配置文件包括配置默认值的模板。本节注释如下。

#默认值{

#udev\_主任/开发

#轮询间隔5

#选择器“循环0”

#路径\分组\策略故障转移\ getuid \ callout”/lib/dev/scsi\ id--whitelisted--device=/dev/%n

#普里奥常数

#路径检测器方向

#rr\_min\_io 1000

#重量均匀

#故障回复手册

#无路径重试失败用户友好名称否

#}

要覆盖任何配置参数的默认值，可以将此模板中的相关行复制到“默认值”部分并取消注释。例如，要覆盖path\_grouping\_policy参数，使其成为多总线而不是故障转移的默认值，请将相应的行从模板复制到配置文件的initial defaults部分，并取消注释，如下所示。

默认值{

用户友好\u名称是路径\u分组\u策略多总线}

表Multipath Configuration Defaults[p.90]描述了Multipath.conf配置文件的Defaults部分中设置的属性。DM Multipath使用这些值，除非它们被Multipath.conf文件的devices和Multipath部分中指定的属性覆盖。

##### **表5.3。多路径配置默认值**

|  |  |
| --- | --- |
| **属性** | **描述** |
| **轮询间隔** | 以秒为单位指定两次路径检查之间的间隔。对于正常运行的路径，检查之间的间隔将逐渐增加到（4\*轮询间隔）。默认值为5。 |
| **乌代夫迪尔** | 创建udev设备节点的目录。默认值是/dev。 |
| **多路径目录** | 存储动态共享对象的目录。默认值取决于系统，通常为/lib/multipath。 |
| **冗长** | 默认的冗长。值越高，详细程度越高。有效级别介于0和6之间。默认值为2。 |
| **路径选择器** | 指定用于确定下一个I/O操作使用的路径的默认算法。可能的值包括：  •：循环路径组中的每个路径，向每个路径发送相同数量的I/O。**循环赛0**  •：以最少的未完成I/O请求数沿路径发送下一组I/O。**队列长度0**  •：以最短的估计服务时间沿路径发送下一组I/O，这是通过将每个路径的未完成I/O的总大小除以其相对吞吐量来确定的。**服务时间0**  默认值为循环0。 |
| **路径分组策略** | 指定要应用于未指定的多路径的默认路径分组策略。可能的值包括：  •=每个优先级组1条路径**故障转移**  •=1个优先级组中的所有有效路径**多总线**  •=每个检测到的序列号1个优先级组**按顺序分组**  •=每个路径优先级值1个优先级组•按节点分组\u名称=每个目标节点名称1个优先级组。**按优先顺序分组**  默认值为故障转移。 |
| **getuid\u标注** | 指定要调用以获取唯一路径标识符的默认程序和参数。需要绝对路径。  默认值为/lib/udev/scsi\_id--whitelisted--device=/dev/%n。 |

|  |  |
| --- | --- |
| **属性** | **描述** |
| **普里奥** | 指定要调用以获取路径优先级值的默认函数。例如，SPC-3中的ALUA位提供可利用的prio值。  可能的值包括：  •：将所有路径的优先级设置为1。**常数**  •：为EMC阵列生成路径优先级。**电磁兼容**  •：根据SCSI-3 ALUA设置生成路径优先级。**阿鲁阿**  •：为NetApp阵列生成路径优先级。**网络存储**  •：为LSI/Engenio RDAC控制器生成路径优先级。**rdac**  •：在主/备用模式下为Compaq/HP控制器生成路径优先级。**hp\_sw**  •：为日立HDS模块化存储阵列生成路径优先级。**hds**  默认值为const。 |
| **prio\_args** | 传递给prio函数的参数字符串大多数prio函数不需要参数。datacore优先顺序器需要一个。例如，“timeout=1000 preferredsds=foo”。默认值为（null）”。 |
| **特征** | 多路径设备的额外功能。唯一现有的功能是队列（如果没有路径），这与将无路径设置为队列（重试）相同。有关使用此功能时可能出现的问题的信息，请参阅“如果没有路径功能，则队列问题”一节。 |
| **路径检测器** | 指定用于确定路径状态的默认方法。  可能的值包括：  •：读取设备的第一个扇区。**readsector0**  •：向设备发送一个准备好的测试单元。**图尔**  •：查询EMC Clariion特定EVPD页面0xC0以确定路径。**emc\u clariion**  •：检查带有主/备用固件的HP存储阵列的路径状态。**hp\_sw**  •：检查LSI/Engenio RDAC存储控制器的路径状态。**rdac**  •：读取具有直接I/O的第一个扇区。**导演**  默认值为directio。 |
| **故障回复** | 管理路径组回切。  •立即值指定立即回切到包含活动路径的最高优先级路径组。 |

|  |  |
| --- | --- |
| **属性** | **描述** |
|  | •手动值规定不应立即进行故障回复，但只有在操作员干预下才能进行故障回复。  •大于零的数值指定延迟回切，以秒为单位。  默认值为手动。 |
| **瑞敏欧** | 指定在切换到当前路径组中的下一个路径之前路由到某个路径的I/O请求数。  默认值为1000。 |
| **剩余重量** | 如果设置为priorities，则在调用path\_selector选择下一条路径之前，不向路径发送rr\_min\_io请求，而是通过rr\_min\_io乘以路径优先级来确定要发送的请求数，这由prio函数确定。如果设置为“均匀”，则所有路径权重都相等。  默认值是统一的。 |
| **没有路径，请重试** | 此属性的数值指定系统在禁用排队之前尝试使用失败路径的次数。值fail表示立即失败，不排队。queue的值表示在路径固定之前不应停止排队。  默认值为0。 |
| **用户友好的名称** | 如果设置为“是”，则指定系统应使用/etc/multipath/bindings文件以mpathn的形式为多路径分配持久且唯一的别名。如果设置为“否”，则指定系统应使用WWID作为多路径的别名。在任何一种情况下，此处指定的内容都将被您在配置文件的“多路径”部分中指定的任何特定于设备的别名覆盖。  默认值为否。 |
| **不带\u守护进程的队列\u** | 如果设置为否，多路径守护进程将在关闭时禁用对所有设备的排队。  默认值为“是”。 |
| **最后冲水** | 如果设置为“是”，则当设备的最后一条路径被删除时，多路径将禁用排队。  默认值为否。 |
| **最大值** | 设置多路径和多路径守护程序可以打开的最大打开文件描述符数。这相当于 |
| **属性** | **描述** |
|  | ulimit-n命令。最大值将从设置为系统限制  /proc/sys/fs/nr\u打开。如果未设置，则从调用进程获取打开的文件描述符的最大数量；通常是1024。为了安全起见，如果路径数大于1024，则应将其设置为最大路径数加32。 |
| **检查计时器** | 路径检查器发出带有显式超时的SCSI命令时使用的超时，以秒为单位。  默认值取自/sys/block/sdx/device/timeout，从12.04开始为30秒 |
| **快速io失败tmo** | 在FC远程端口上检测到问题后，SCSI层在该远程端口上的设备I/O失败之前等待的秒数。此值应小于dev\_loss\_tmo的值。将此设置为off将禁用超时。  默认值由操作系统确定。 |
| **开发损失** | 在FC远程端口上检测到问题后，SCSI层将等待的秒数，然后再将其从系统中删除。  将此设置为无穷大将设置为2147483647秒，即68年。  默认值由操作系统确定。 |

#### 4.4. 配置文件多路径属性

表Multipath Attributes[p.93]显示了可以在Multipath.conf配置文件的Multipath部分中为每个特定多路径设备设置的属性。这些属性仅适用于指定的多路径。DM Multipath使用这些默认值，并覆盖Multipath.conf文件的defaults和devices部分中设置的属性。

##### **表5.4。多路径属性**

|  |  |
| --- | --- |
| **属性** | **描述** |
| **wwid** | 指定应用多路径属性的多路径设备的WWID。此参数对于multipath.conf文件的此部分是必需的。 |
| **别名** | 指定应用多路径属性的多路径设备的符号名称。如果您使用的是用户友好的名称，请不要将此值设置为mpathn；这可能与自动分配的用户友好名称冲突，并给您错误的设备节点名称。 |

此外，在本节中可能会覆盖以下参数

• *路径分组策略*

• *路径选择器*

• *故障回复*

• *普里奥*

• *prio\_args*

• *没有路径，请重试*

• *瑞敏欧*

• *剩余重量*

• *最后冲水*

以下示例显示了在配置文件中为两个特定多路径设备指定的多路径属性。第一个设备的WWID为3600508b4000156d70001200000b0000，符号名称为黄色。

示例中的第二个多路径设备的WWID为1DEC\_u\_\_\_\_321; 816758474，符号名为red。在本例中，rr\_权重属性设置为优先级。

多径{多径{

wwid 3600508b4000156d70001200000b0000别名黄色路径\u分组\u策略多总线路径\u选择器“循环0”回切手动rr权重优先级无路径\u重试5}多路径{

wwid 1DEC uuuuuuuuuuuu321816758474别名红色rr uu权重优先级}

}

#### 4.5.配置文件设备

表设备属性[p.95]显示可以在multipath.conf配置文件的devices部分中为每个存储设备设置的属性。DM multipath使用这些属性，除非它们被multipath.conf文件multipath部分中为包含设备的路径指定的属性覆盖。这些属性覆盖e在multipath.conf文件的defaults部分中设置的属性。

默认情况下，多路径配置中包括许多支持多路径的设备。默认情况下支持的设备的值列在multipath.conf.defaults文件中。您可能不需要修改这些设备的值，但如果这样做，您可以通过在conf文件中包含条目来覆盖默认值覆盖这些值的设备的配置文件。您可以从multipath.conf.annotated.gz复制设备配置默认值，或者如果您希望有一个简短的配置文件multipath.conf.synthetic文件，用于设备并覆盖要更改的值。

要将默认情况下未自动配置的设备添加到配置文件的此部分，您必须设置供应商和产品参数。您可以通过查看/sys/block/device\u name/device/vendor和/sys/block/device\u name/device/model来查找这些值，其中device\u name是要进行多路径处理的设备，如下图所示乐：

#cat/sys/block/sda/设备/供应商

WINSYS#cat/sys/block/sda/device/model

SF2372

要指定的其他参数取决于您的特定设备。如果该设备处于活动/活动状态，通常不需要设置其他参数。您可能需要将path\_grouping\_策略设置为multibus。您可能需要设置的其他参数包括no\_path\_retry和rr\_min\_io，如表“多路径属性”[p.93]中所述。

如果设备是主动/被动的，但它会自动将带有I/O的路径切换到被动路径，则您需要将checker函数更改为不向路径发送I/O的函数，以测试其是否工作（否则，您的设备将继续故障切换）。这几乎总是意味着您将path\_checker设置为tur；这适用于支持测试单元就绪命令的所有SCSI设备，大多数SCSI设备都支持该命令。

如果设备需要特殊命令来切换路径，则为多路径配置此设备需要一个硬件处理程序内核模块。当前可用的硬件处理程序是emc。如果这对于您的设备来说还不够，则您可能无法为多路径配置设备。

##### **表5.5.设备属性**

|  |  |
| --- | --- |
| **属性** | **描述** |
| **小贩** | 指定应用设备属性的存储设备的供应商名称，例如COMPAQ。 |
| **产品** | 指定应用设备属性的存储设备的产品名称，例如HSV110（C）COMPAQ。 |
| **修订** | 指定存储设备的产品版本标识符。 |
| **产品黑名单** | 指定用于按产品将设备列入黑名单的正则表达式。 |
| **硬件处理器** | 指定在切换路径组或处理I/O错误时用于执行硬件特定操作的模块。可能的值包括：  •：EMC存储阵列的硬件处理程序**1 emc**  •：SCSI-3 ALUA阵列的硬件处理程序。**1阿鲁阿**  •：Compaq/HP控制器的硬件处理器。**1 hp\_sw**  •：LSI/Engenio RDAC控制器的硬件处理器。**1 rdac** |

此外，以下参数可能会在该设备部分被覆盖

• *路径分组策略*

• *getuid\u标注*

• *路径选择器*

• *路径检测器*

• *特征*

• *故障回复*

• *普里奥*

• *prio\_args*

• *没有路径，请重试*

• *瑞敏欧*

• *剩余重量*

• *快速io失败tmo*

• *开发损失*

• *最后冲水*

无论何时指定硬件\_处理程序，您都有责任确保加载适当的内核模块以支持指定的接口。可以在中找到这些模块。必要的模块应集成到initrd中，以确保在引导期间具有必要的发现和故障切换回切能力。检查嗯，**/lib/modules/`uname-r`/kernel/drivers/scsi/device\u handler/**

#echo scsi\_dh\_alua>>/etc/initramfs tools/modules##将模块附加到文件

#更新initramfs-u-kall

以下示例显示多路径配置文件中的设备条目。

#装置{

#装置{

#供应商“康柏”

#产品“MSA1000”#路径\_分组\_策略多总线

#路径检查器tur#rr(权重优先级)

# }

#}

供应商、产品和修订字段中保留的间距非常重要，因为多路径正在对这些属性执行直接匹配，这些属性的格式由SCSI规范定义，特别是标准查询[84]命令。使用引号时，供应商、产品和修订字段将严格按照规范进行解释。正则表达式可以集成到引号中的字符串中。如果定义的字段没有必要的间距，则多路径将字符串复制到适当大小的缓冲区中，并用适当数量的spa填充规范要求整个字段由可打印字符或空格填充，如上面的示例所示

•供应商：8个字符

•产品：16个字符•版本：4个字符

要创建更健壮的配置文件，还可以使用正则表达式。运算符包括^$[]。

**\* ? +**。通过检查live multipath数据库和/usr/share/doc/multipath tools/Examples中的multipath.conf示例文件，可以找到函数正则表达式的示例：

#echo“显示配置”|多路径-k

## 5.DM多路径管理和故障排除

#### 5.1.调整在线多路径设备的大小

如果需要调整联机多路径设备的大小，请使用以下步骤

1.         调整物理设备的大小。这是特定于存储平台的。

2.         使用以下命令查找LUN的路径：

#多路径-l

3.         调整路径大小。对于SCSI设备，将1写入设备的重新扫描文件会导致SCSI驱动程序重新扫描，如下命令所示：

#echo 1>/sys/block/device\u name/device/rescan

4.         通过运行multipathd Resize命令调整多路径设备的大小：

#multipathd-k“调整贴图大小”

5.         调整文件系统大小（假定未使用LVM或DOS分区）：

#调整大小2FS/dev/mapper/mpatha

#### 5.2.将根文件系统从单路径设备移动到多路径设备

通过使用UUID将设备标识为固有标签，这大大简化了操作。只需安装多路径工具引导并重新启动即可。这将重建初始RAM磁盘，并在UUID装载根文件系统之前为多路径提供构建路径的机会。

无论何时更新multipath.conf，initrd都应该通过执行update initramfs-u-k all来更新。原因是multipath.conf被复制到ramdisk，并且是通过其黑名单和设备部分确定分组可用设备的一部分。

#### 5.3.将交换文件系统从单路径设备移动到多路径设备

该过程与上一节“将根文件系统从单一路径移动到多路径设备”中所述的过程完全相同。

#### 5.4.多路径守护进程

如果发现在实现多路径配置时遇到问题，则应确保多路径守护程序按照“设置DM多路径”中的说明运行。必须运行multipathd守护进程才能使用multipathd设备。另请参阅multipathd交互控制台故障排除一节，了解如何将multipathd作为调试辅助工具与multipathd交互。

#### 5.5.如果队列没有路径，则队列出现问题

如果在/etc/multipath.conf文件中指定了功能“1 queue\u If\u no\u path”，则任何使用I/O的进程都将挂起，直到恢复一个或多个路径。为避免此情况，请在/etc/multipath.conf中设置no\u path\u retry N参数。

设置no\_path\_retry参数时，请从/etc/multipath.conf文件中删除功能“1 queue\_if\_no\_path”选项。但是，如果您使用的多路径设备的功能“1 queue\u If\u no\u path”选项在默认情况下设置为已编译，就像许多SAN设备一样，则必须添加功能“0”以覆盖此默认值。您可以通过将现有设备部分以及该部分（而不是整个文件）从/usr/share/doc/multipath tools/examples/multipath.conf.annotated.gz复制到/etc/multipath.conf并根据需要进行编辑来实现这一点。

如果需要使用功能“1 queue\u If\u no\u path”选项，并且遇到此处指出的问题，请使用dmsetup命令在运行时编辑特定LUN（即所有路径均不可用）的策略。例如，如果要将多路径设备mpathc上的策略从“queue\u if\u no\u path”更改为“fail\u if\u no\u path”，请执行以下命令。

#dmsetup消息mpathc 0“如果没有路径，则失败”

必须指定mpathN别名，而不是路径

#### 5.6. 多路径命令输出

创建、修改或列出多路径设备时，将获得当前设备设置的打印输出。格式如下。对于每个多路径设备：

操作\u如果\u有：别名（wwid\u如果\u与\u别名不同\u）dm\u设备\u名称\u如果\u已知供应商、产品

size=size features=&apos;features&apos;hwhandler=&apos;hardware\u handler&apos;wp=write\u permission\u如果每个路径组已知：

-+-policy=&apos;scheduling\u policy&apos;prio=prio\u if\u known status=path\u group\u status\u if\u known For each path:

`-主机：通道：id:lun devnode主：次dm\_状态\u如果\u已知路径\u状态联机\u状态

例如，多路径命令的输出可能如下所示：

3600d0230000000000e13955cc3757800 dm-1 WINSYS，SF2372 size=269G features=&apos;0&apos;hwhandler=&apos;0&apos;wp=rw |-+-policy=&apos;round-robin 0&apos;prio=1 status=active

|`-6:0:0:0 sdb 8:16活动就绪运行

`-+-policy=&apos;round-robin 0&apos;优先级=1状态=已启用

`-7:0:0:0 sdf 8:80活动就绪运行

如果路径已启动并准备好进行I/O，则路径的状态为就绪或重影。如果路径向下，则状态为故障或不稳定。路径状态由multipathd守护进程根据/etc/multipath.conf文件中定义的轮询间隔定期更新。

dm状态与path状态相似，但从内核的角度来看。dm状态有两种状态：失败（类似于故障）和活动（覆盖所有其他路径状态）。有时，设备的路径状态和dm状态会暂时不一致。

联机状态的可能值为“正在运行”和“脱机”。脱机状态表示SCSI设备已被禁用。

创建或修改多路径设备时，路径组状态、dm设备名称、写入权限和dm状态未知。此外，这些功能并不总是正确的

#### 5.7. 使用Multipath命令进行多路径查询

您可以使用multipath命令的-l和-ll选项来显示当前的多路径配置。l选项显示从sysfs和设备映射器中的信息收集的多路径拓扑。-ll选项除了显示系统的所有其他可用组件外，还显示-l显示的信息。

显示多路径配置时，可以使用multipath命令的-v选项指定三个详细级别。指定-v0不会产生任何输出。指定-v1仅输出创建或更新的多路径名称，然后可以将其馈送到其他工具，如kpartx。指定-v2将打印所有检测到的路径、多路径和设备映射。

多路径的默认详细级别为2，可以通过在multipath.conf的defaults部分中定义详细属性进行全局修改。

下面的示例显示了multipath-l命令的输出。

#多路径-l 3600d0230000000000e13955cc3757800 dm-1 WINSYS，SF2372 size=269G features=&apos;0&apos;hwhandler=&apos;0&apos;wp=rw |-+-policy=&apos;round-robin 0&apos;prio=1 status=active

|`-6:0:0:0 sdb 8:16活动就绪运行

`-+-policy=&apos;round-robin 0&apos;优先级=1状态=已启用

`-7:0:0:0 sdf 8:80活动就绪运行

下面的示例显示multipath-ll命令的输出。

#多路径-ll 3600d0230000000000e13955cc3757801 dm-10 WINSYS，SF2372 size=269G features=&apos;0&apos;hwhandler=&apos;0&apos;wp=rw |-+-policy=&apos;round-robin 0&apos;prio=1 status=enabled

|`-19:0:0:1 sdc 8:32活动就绪运行

`-+-policy=&apos;round-robin 0&apos;优先级=1状态=已启用

`-18:0:0:1 sdh 8:112活动就绪运行3600d0230000000000e13955cc3757803 dm-2 WINSYS，SF2372大小=125G功能=&apos;0&apos;hwhandler=&apos;0&apos;wp=rw`-+-策略=&apos;循环0&apos;优先级=1状态=活动

|-19:0:0:3 sde 8:64活动就绪运行

`-18:0:0:3 sdj 8:144活动就绪运行

#### 5.8. 多路径命令选项

表有用的多路径命令选项[p.101]描述了多路径命令的一些选项，您可能会发现这些选项很有用。

##### **表5.6。有用的多路径命令选项**

|  |  |
| --- | --- |
| **选项** | **描述** |
| **-l** | 显示从sysfs和设备映射器收集的当前多路径配置。 |
| **-ll** | 显示从sysfs、设备映射器和系统上所有其他可用组件收集的当前多路径配置。 |
| **-f装置** | 删除命名的多路径设备。 |
| **-F** | 删除所有未使用的多路径设备。 |

#### 5.9. 使用dmsetup命令确定设备映射器条目

您可以使用dmsetup命令找出哪些设备映射器条目与多路径设备匹配。

以下命令显示所有设备映射器设备及其主要和次要编号。次要编号确定dm设备的名称。例如，小数目3对应于多路径设备。**/dev/dm-3**

#dmsetup-ls-mpathd（253,4）MPAThP1（253,12）mpathfp1（253,11）mpathb（253,3）mpathgp1（253,14）mpathhp1（253,13）mpathh（253,2）mpathh（253,9）mpathg（253,8）VolGroup00-LogVol01（253,1）mpathf（253,7）VolGroup00-LogVol00（253,0）MPAThP（253,6）mpathbp1（253,10）mpathd（253,5）

#### 5.10. 多路径交互式控制台的故障排除

multipathd-k命令是multipathd守护进程的交互式接口。输入此命令将打开交互式多路径控制台。输入此命令后，可以输入帮助以获取可用命令的列表，也可以输入交互式命令，或者输入CTRL-D以退出。

multipathd交互式控制台可用于解决系统可能存在的问题。例如，以下命令序列在退出控制台之前显示多路径配置，包括默认值。有关更多示例，请参阅IBM文章“使用Multipathd的技巧”[85]。

#多路径k

>>显示配置

>>CTRL-D

以下命令序列确保multipath已获取对multipath.conf的任何更改，

#多路径k

>>重新配置

>>CTRL-D

使用以下命令序列确保路径检查器工作正常。

#多路径k

>>显示路径

>>CTRL-D

命令也可以使用stdin流式传输到multipathd，如下所示：

#echo“显示配置”|多路径-k

# 第六章。远程管理

有许多方法可以远程管理Linux服务器。本章将介绍三种最流行的应用程序OpenSSH、Puppet和Zentyal。

## 1.OpenSSH服务器

#### 1.1. 介绍

《Ubuntu服务器指南》的这一部分介绍了一个强大的工具集合，用于远程控制网络计算机，以及在网络计算机之间传输数据，称为OpenSSH。您还将了解OpenSSH服务器应用程序可能的一些配置设置，以及如何在Ubuntu系统上更改这些设置。

OpenSSH是Secure Shell（SSH）协议系列工具的免费版本，用于在计算机之间远程控制或传输文件。用于完成这些功能的传统工具，如telnet或rcp，是不安全的，在使用时以明文形式传输用户密码。OpenSSH提供了一个服务器守护程序和客户端工具，以促进安全、加密的远程控制和文件传输操作，有效地取代了传统工具。

OpenSSH服务器组件sshd持续侦听来自任何客户端工具的客户端连接。发生连接请求时，sshd会根据客户端工具连接的类型设置正确的连接。例如，如果远程计算机正在与ssh客户端应用程序连接，则OpenSSH服务器将在身份验证后设置远程控制会话。如果远程用户使用scp连接到OpenSSH服务器，则OpenSSH服务器守护程序会在身份验证后在服务器和客户端之间启动文件的安全副本。OpenSSH可以使用许多身份验证方法，包括普通密码、公钥和Kerberos票证。

#### 1.2. 安装

OpenSSH客户端和服务器应用程序的安装非常简单。要在Ubuntu系统上安装OpenSSH客户端应用程序，请在终端提示符下使用以下命令：**sudoapt安装openssh客户端**

要安装OpenSSH服务器应用程序和相关支持文件，请在终端提示符下使用以下命令：**sudoapt安装openssh服务器**

在server Edition安装过程中，还可以选择安装openssh服务器包。

#### 1.3. 配置

您可以通过编辑文件/etc/ssh/sshd\u config来配置OpenSSH服务器应用程序sshd的默认行为。有关此文件中使用的配置指令的信息，您可以使用在终端提示符下发出的以下命令查看相应的手册页面：

**mansshd\_配置**

sshd配置文件中有许多指令控制通信设置和身份验证模式等内容。以下是可由更改的配置指令示例

编辑/etc/ssh/sshd\_配置文件。

在编辑配置文件之前，应复制原始文件并防止其写入，以便将原始设置作为参考，并在必要时重新使用。

复制/etc/ssh/sshd\_config文件，并使用在终端提示符下发出的以下命令防止其写入：

**sudo cp/etc/ssh/sshd\u config/etc/ssh/sshd\u config.original sudo chmod a-w/etc/ssh/sshd\u config.original**

以下是您可以更改的配置指令示例：

•要将OpenSSH设置为在TCP端口2222而不是默认的TCP端口22上侦听，请更改端口指令如下：

2222端口

•要使sshd允许基于公钥的登录凭据，只需添加或修改以下行：

PubkeyAuthentication是

如果该行已经存在，则确保它未被注释掉。

•要使OpenSSH服务器将/etc/issue.net文件的内容显示为预登录横幅，只需添加或修改以下行：

Banner/etc/issue.net

在/etc/ssh/sshd\_配置文件中。

在对/etc/ssh/sshd\_config文件进行更改后，保存该文件，并在终端提示符下使用以下命令重新启动sshd服务器应用程序以实现更改：**sudo systemctl重新启动sshd.service**

sshd的许多其他配置指令可用于更改服务器应用程序的行为以满足您的需要。但是，请注意，如果您访问服务器的唯一方法是ssh，并且您在通过/etc/ssh/sshd\_config文件配置sshd时出错，则重新启动服务器时可能会发现您被锁定在服务器之外。此外，如果提供了错误的配置指令，sshd服务器可能会拒绝启动，因此在远程服务器上编辑此文件时要格外小心。

#### 1.4. SSH密钥

SSH密钥允许在两台主机之间进行身份验证，而无需密码。SSH密钥身份验证使用两个密钥，一个私钥和一个公钥。

要生成键，请在终端提示下输入：**ssh-keygen-t rsa**

这将使用RSA算法生成密钥。在此过程中，系统将提示您输入密码。

当提示创建密钥时，只需按Enter键。

默认情况下，公钥保存在~/.ssh/id\_rsa.pub文件中，而~/.ssh/id\_rsa是私钥。

现在，将id\_rsa.pub文件复制到远程主机，并通过输入以下内容将其附加到~/.ssh/authorized\_密钥：**ssh副本idusername@remotehost**

最后，再次检查授权密钥文件的权限，只有经过身份验证的用户才应该具有读写权限。如果权限不正确，请通过以下方式更改权限：**chmod 600.ssh/authorized\_密钥**

您现在应该能够通过SSH连接到主机，而无需提示输入密码。

#### 1.5. 工具书类

•Ubuntu Wiki SSH[86]页面。

•OpenSSH网站[87]

•高级OpenSSH Wiki页面[88]

## 2.木偶

Puppet是一个跨平台的框架，允许系统管理员使用代码执行常见任务。该代码可以执行各种任务，从安装新软件到检查文件权限或更新用户帐户。Puppet不仅在系统的初始安装期间，而且在系统的整个生命周期中都非常出色。在大多数情况下，将在客户机/服务器配置中使用puppet。

本节将介绍在客户机/服务器配置中安装和配置Puppet。这个简单的示例将演示如何使用Puppet安装Apache。

#### 2.1. 预配置

在配置puppet之前，您可能希望为puppet.example.com添加DNS CNAME记录，其中example.com是您的域。默认情况下，Puppet客户端将Puppet.example.com的DNS作为Puppet服务器名称或Puppet主机进行检查。有关域名服务（DNS）的更多详细信息，请参见第8章域名服务（DNS）[166页]。

如果不希望使用DNS，可以向服务器和client/etc/hosts文件添加条目。例如，在Puppet服务器的/etc/hosts文件中添加：

127.0.0.1 localhost.localdomain localhost puppet

192.168.1.17 puppetclient.example.com puppetclient在每个Puppet客户端上，为服务器添加一个条目：

192.168.1.16 puppetmaster.example.com puppetmaster木偶

将上面的示例IP地址和域名替换为实际的服务器和客户端地址和域名。

#### 2.2. 安装

要安装Puppet，请在服务器上的终端中输入：**sudoapt安装puppetmaster**

在一台或多台客户端计算机上，输入：**sudo安装木偶**

#### 2.3. 配置

为apache2类创建文件夹路径：

sudo mkdir-p/etc/puppet/modules/apache2/manifests

现在为apache2设置一些资源。创建包含以下内容的文件/etc/puppet/modules/apache2/manifests/init.pp：

类apache2{package{&apos;apache2&apos;：确保=>installed，}

服务{&apos;apache2&apos;：确保=>true，启用=>true，

require=>Package[&apos;apache2&apos;]，}

}

接下来，使用以下内容创建节点文件/etc/puppet/code/environments/production/manifests/site.pp：

节点&apos;puppetclient.example.com&apos;{include apache2}

将puppetclient.example.com替换为实际Puppet客户端的主机名。

此简单Puppet服务器的最后一步是重新启动守护程序：**sudo systemctl重新启动puppetmaster.service**

现在一切都在Puppet服务器上配置好了，是时候配置客户端了。

首先，将Puppet代理守护进程配置为启动。编辑/etc/default/puppet，将开始更改为是：

开始=是

然后启动服务：查看客户端证书指纹**sudo systemctl start puppet.service sudo puppet代理--指纹**

回到Puppet服务器上，查看挂起的证书签名请求：

**sudo木偶证书列表**

在Puppet服务器上，验证客户端的指纹并签署puppetclient的证书：**sudo puppet证书签名puppetclient.example.com**

在Puppet客户端上，在前台手动运行Puppet代理。严格来说，这一步不是必需的，但它是测试和调试puppet服务的最佳方法。**sudo傀儡代理-测试**

检查两台主机上的/var/log/syslog是否存在配置错误。如果一切顺利，apache2包及其依赖项将安装在Puppet客户端上。

这个例子非常简单，没有突出Puppet的许多特性和优点。更多信息请参见第2.4节“资源”[p.109]。

#### 2.4. 资源

•参见官方文件[89]网站。

•参见Puppet forge[90]，Puppet模块在线存储库。

•另见亲木偶[91]。

## 3.二十世纪

Zentyal是一个Linux small business server，可以配置为网关、基础架构管理器、统一威胁管理器、办公服务器、统一通信服务器或它们的组合。Zentyal管理的所有网络服务都是紧密集成的，可以自动化大部分任务。这节省了时间，并有助于避免网络配置和管理中的错误。Zentyal是开源的，在GNU通用公共许可证（GPL）下发布，在Ubuntu GNU/Linux上运行。

Zentyal由一系列包（通常每个模块一个）组成，这些包提供一个web界面来配置不同的服务器或服务。配置存储在键值Redis数据库中，但与用户、组和域相关的配置存储在OpenLDAP上。通过web界面配置任何可用参数时，将使用模块提供的配置模板覆盖最终配置文件。使用Zentyal的主要优点是一个统一的图形用户界面，用于配置所有网络服务以及它们之间的高度现成集成。

Zentyal每年根据最新的Ubuntu LTS发布一次主要的稳定版本。

#### 3.1. 安装

如果要创建新用户以访问Zentyal web界面，请运行：**sudo adduser用户名sudo**

将Zentyal存储库添加到存储库列表：从Zentyal导入公钥：**sudo添加apt存储库“deb”http://archive.zentyal.org/zentyal 3.5主要额外费用“**

**sudo apt key adv--keyserver keyserver.ubuntu.com--recv key 10E239FF wget-qhttp://keys.zentyal.org/zentyal-4.2-archive.asc -O-| sudo apt按键添加**更新软件包并安装Zentyal:

**sudo apt更新sudo apt安装zentyal**

在安装过程中，将要求您设置根MySQL密码并确认端口443。

#### 3.2. 第一步

任何属于sudo组的系统帐户都可以登录Zentyal web界面。默认情况下，安装Ubuntu服务器时创建的用户将属于sudo组。

要访问Zentyal web界面，请将浏览器指向https://localhost/ 或远程服务器的IP地址。Zentyal创建自己的自签名SSL证书时，您必须在浏览器上接受安全异常。使用与登录服务器相同的用户名和密码登录。

登录后，您将看到服务器的概览。单个模块，如防病毒或防火墙，只需单击它们，然后单击安装即可安装。选择服务器角色（如网关或基础设施）可用于一次安装多个模块。

还可以通过命令行安装模块：**sudo apt安装<zentyal模块>**

请参阅下面的可用模块列表。

要启用模块，请转到仪表板，然后单击模块状态。单击模块的复选框，然后保存更改。

要配置已安装模块的任何功能，请单击左侧菜单上的不同部分。进行任何更改时，右上角会出现一个红色的“保存更改”按钮。

如果需要自定义任何配置文件或运行某些操作（脚本或命令）来配置Zentyal上不可用的功能，请将自定义配置文件模板放置在/etc/Zentyal/stubs/<module>/上，并将挂钩放置在/etc/Zentyal/hooks/<module><action>上。阅读更多关于存根和钩子的信息[92]。

#### 3.3. 模块

Zentyal2.3在Ubuntu18.04宇宙存储库中提供。可用的模块包括：

•zentyal core和zentyal common：zentyal接口的核心和框架的公共库。还包括日志和事件模块，这些模块为管理员提供了查看日志和从中生成事件的界面。

•zentyal网络：管理网络的配置。从接口（支持静态IP、DHCP、VLAN、网桥或PPPoE）到多个网关（当具有多个Internet连接、负载平衡和高级路由、静态路由或动态DNS时）。

•zentyal对象和zentyal服务：为网络地址（例如LAN而不是192.168.1.0/24）和命名为服务的端口（例如HTTP而不是80/TCP）提供抽象级别。

•zentyal firewall：配置iptables规则以阻止禁止连接、NAT和端口重定向。

•zentyal ntp：安装ntp守护进程以保持服务器准时运行，并允许网络客户端与服务器同步时钟。

•zentyal dhcp：配置ISC dhcp服务器，支持网络范围、静态租用和其他高级选项，如NTP、WINS、动态DNS更新和PXE网络引导。

•zentyal dns：将ISC Bind9 dns服务器带到您的服务器中，以缓存本地查询，作为已配置域的转发器或权威服务器。允许配置A、CNAME、MX、NS、TXT和SRV记录。

•zentyal ca：将证书颁发机构的管理集成到zentyal中，因此用户可以使用证书对服务进行身份验证，如OpenVPN。

•zentyal openvpn：允许使用openvpn配置多个VPN服务器和客户端，并使用Quagga进行动态路由配置。

•zentyal用户：提供一个界面，用于配置和管理OpenLDAP上的用户和组。Zentyal上的其他服务根据LDAP进行身份验证，LDAP具有集中的用户和组管理。还可以从Microsoft Active Directory域同步用户、密码和组。

•zentyal squid：配置squid和Dansguardian以加快浏览速度，这得益于缓存功能和内容过滤。

•zentyal samba：允许samba配置并与现有LDAP集成。从同一界面，您可以定义密码策略、创建共享资源和分配权限。

•zentyal打印机：将CUPS与Samba集成，不仅允许配置打印机，还允许根据LDAP用户和组授予打印机权限。

Ubuntu Universe存储库中没有，但Zentyal Team PPA[93]中有以下其他模块：

•zentyal antivirus：将ClamAV antivirus与代理、文件共享或邮件过滤器等其他模块集成。

•zentyal asterisk：将asterisk配置为提供基于LDAP的简单PBX身份验证。

•zentyal bwmonitor：允许监控局域网客户端的使用情况。

•zentyal captiveportal：将捕获门户与防火墙、LDAP用户和组集成在一起。

•zentyal ebackup：允许使用流行的duplicity备份工具对服务器进行定时备份。

•zentyal ftp：使用基于LDAP的身份验证配置ftp服务器。

•zentyal ids：集成网络入侵检测系统。

•zentyal ipsec：允许使用OpenSwan配置ipsec隧道。

•zentyal jabber：将ejabberd XMPP服务器与LDAP用户和组集成。

•zentyal thinclients：基于LTSP的瘦客户端解决方案。

•zentyal mail：一个完整的邮件堆栈，包括Postfix和带有LDAP后端的Dovecot。

•zentyal mailfilter：使用邮件堆栈配置amavisd，以过滤垃圾邮件和附加的病毒。

•zentyal monitor：集成collectd以监控服务器性能和运行服务。

•zentyal pptp：配置pptp VPN服务器。

•zentyal radius：将FreeRADIUS与LDAP用户和组集成。

•zentyal软件：用于管理已安装zentyal模块和系统更新的简单界面。

•zentyal TrafficShapping：配置流量限制规则以进行带宽限制并改善延迟。

•zentyal usercorner：允许用户使用web浏览器编辑自己的LDAP属性。

•zentyal virt：基于libvirt创建和管理虚拟机的简单界面。

•zentyal webmail：允许使用流行的Roundcube webmail访问您的邮件。

•zentyal webserver：将Apache webserver配置为在您的计算机上承载不同的站点。

•zentyal zarafa：将zarafa群件套件与zentyal邮件堆栈和LDAP集成。

#### 3.4. 工具书类

Zentyal官方文件[94]页。

Zentyal社区维基[95]。

访问Zentyal论坛[96]获取社区支持、反馈、功能请求等。

# 第七章。网络认证

本节将LDAP应用于网络身份验证和授权。

## 1.OpenLDAP服务器

轻量级目录访问协议（LDAP）是用于查询和修改在TCP/IP上运行的基于X.500的目录服务的协议。当前的LDAP版本是LDAPv3，如RFC4510[97]中所定义，Ubuntu中的实现是OpenLDAP。”

因此，LDAP协议访问LDAP目录。以下是一些关键概念和术语：

•LDAP目录是数据项的树，本质上是分层的，称为目录信息树（DIT）。

•条目由一组属性组成。

•属性具有类型（名称/描述）和一个或多个值。

•每个属性必须至少在一个objectClass中定义。

•属性和对象类在模式中定义（对象类实际上被视为一种特殊的属性）。

•每个条目都有一个唯一的标识符：其可分辨名称（DN或DN）。这依次由相对可分辨名称（RDN）和父条目的DN组成。

•条目的DN不是属性。它不被视为条目本身的一部分。

术语object、container和node有一定的含义，但它们本质上都与entry（技术上正确的术语）的含义相同。

例如，下面我们有一个由11个属性组成的条目，其中以下为真：

•DN为“cn=John Doe，dc=example，dc=com”

•RDN是“cn=John Doe”

•父DN为“dc=example，dc=com”

dn:cn=johndoe，dc=example，dc=com cn:johndoe-givenName:johnsn:Doe

电话号码：+1 888 555 6789电话号码：+1 888 555 1232邮件：john@example.com

经理：cn=Larry Smith，dc=example，dc=com对象类：inetOrgPerson对象类：organizationalPerson对象类：person对象类：top

上述条目采用LDIF格式（LDAP数据交换格式）。您输入到DIT中的任何信息也必须采用这种格式。RFC2849[98]中对此进行了定义。

尽管本指南将介绍如何使用LDAP进行中央身份验证，但LDAP适用于任何涉及到大量访问请求的情况，这些请求大多是读取的、基于属性（名称：值）的后端。示例包括通讯簿、电子邮件地址列表和邮件服务器的配置。

#### 1.1.安装

安装OpenLDAP服务器守护程序和传统的LDAP管理实用程序。它们分别位于slapd和LDAP UTIL包中。

slapd的安装将创建一个工作配置。特别是，它将创建一个可用于存储数据的数据库实例。但是，后缀（或基本DN）此实例的名称将根据主机的域名确定。如果您需要其他内容，可以在安装后立即更改，但此时您仍然没有任何有用的数据。

本指南将使用数据库后缀dc=example，dc=com。

继续安装：**sudo-apt安装slapd-ldap-utils**

如果要更改DIT后缀，现在是个好时机，因为更改它会丢弃现有的后缀。要更改后缀，请运行以下命令：**sudo dpkg重新配置slapd**

例如，要将DIT后缀切换为dc=example，dc=com，以便您可以更仔细地遵循本指南，请在询问有关DNS域名的问题时回答example.com。

由于Ubuntu8.10 slapd被设计为在slapd内部配置，为此专门提供了一个单独的DIT。这允许用户在不需要重新启动服务的情况下动态配置slapd。此配置数据库由位于/etc/ldap/slapd.d下的一组基于文本的LDIF文件组成。这种工作方式称为b有几种名称：slapd-config方法、RTC方法（实时配置）或cn=config方法。您仍然可以使用传统的平面文件方法（slapd.conf），但不推荐使用；该功能最终将被淘汰。

Ubuntu现在使用slapd配置方法进行slapd配置，本指南反映了这一点。

在安装过程中，系统会提示您定义管理凭据。这些是数据库实例根DN的基于LDAP的凭据。默认情况下，此用户的DN为cn=admin，dc=example，dc=com。此外，默认情况下，没有为slapd config数据库创建管理帐户，因此您需要验证externa为了访问LDAP，我们需要访问LDAP。稍后我们将看到如何执行此操作。

如今，一些经典模式（cosine、nis、inetorgperson）内置了slapd。还有一个包含的“核心”模式，这是任何模式工作的先决条件。

#### 1.2.安装后检查

安装过程设置了2个DIT。一个用于SLAPd配置，一个用于自己的数据（DC＝示例，Dc= COM）。让我们看一下。

•这就是slapd config数据库/DIT的外观。回想一下，该数据库是基于LDIF的，位于/etc/ldap/slapd.d下：

/etc/ldap/slapd.d/

/etc/ldap/slapd.d/cn=config.ldif

/etc/ldap/slapd.d/cn=config

/etc/ldap/slapd.d/cn=config/cn=schema

/etc/ldap/slapd.d/cn=config/cn=schema/cn={1}cosine.ldif

/etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif

/etc/ldap/slapd.d/cn=config/cn=schema/cn={2}nis.ldif/etc/ldap/slapd.d/cn=config/cn=schema/cn={3}inetorgperson.ldif

/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif

/etc/ldap/slapd.d/cn=config/olcDatabase={0}config.ldif

/etc/ldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif

/etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif

/etc/ldap/slapd.d/cn=config/olcBackend={0}mdb.ldif

/etc/ldap/slapd.d/cn=config/cn=schema.ldif

不要直接编辑slapd配置数据库。通过LDAP协议（实用程序）进行更改。

•通过LDAP协议，这就是slapd配置DIT的外观：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi://-b cn=config dn**

dn:cn=config

dn:cn=module{0}，cn=config

dn:cn=schema，cn=config

dn:cn={0}核心，cn=schema，cn=config

dn:cn={1}余弦，cn=schema，cn=config

dn:cn={2}nis，cn=schema，cn=config

dn:cn={3}inetorgperson，cn=schema，cn=config

dn:olcBackend={0}mdb，cn=config

dn:olcDatabase={-1}前端，cn=config

dn:olcDatabase={0}配置，cn=config

dn:olcDatabase={1}mdb，cn=config

条目说明：

•：全球环境*cn=config*

•：动态加载模块*cn=模块{0}，cn=config*

•：包含硬编码的系统级架构*cn=schema，cn=config*

•：硬编码核心模式*cn={0}核心，cn=schema，cn=config*

•：余弦模式*cn={1}余弦，cn=schema，cn=config*

•：nis模式*cn={2}nis，cn=schema，cn=config*

•：inetorgperson模式*cn={3}inetorgperson，cn=schema，cn=config*

•：“mdb”后端存储类型*olcBackend={0}mdb，cn=config*

•：前端数据库，其他数据库的默认设置*olcDatabase={-1}前端，cn=config*

•：slapd配置数据库（cn=config）•olcDatabase={1}mdb，cn=config：您的数据库实例（dc=example，dc=com）*olcDatabase={0}配置，cn=config*

•这就是dc=示例，dc=com DIT的样子：

**ldapsearch-x-LLL-hdap://-bdc=example，dc=com-dn**

dn:dc=example，dc=com

dn:cn=admin，dc=example，dc=com

条目说明：

•：DIT的基础*dc=示例，dc=com*

•：此DIT的管理员（rootDN）（在包安装期间设置）*cn=admin，dc=example，dc=com*

#### 1.3.修改/填充数据库

让我们向数据库中介绍一些内容。我们将添加以下内容：

•名为“人”的节点（用于存储用户）

•称为组的节点（用于存储组）

•一个名为矿工的团体

•一个叫john的用户

创建以下LDIF文件并将其命名为add\_content.LDIF：

dn:ou=People，dc=example，dc=com对象类：organizationalUnit ou:People

dn:ou=组，dc=示例，dc=com对象类：organizationalUnit ou:组

dn:cn=miners，ou=Groups，dc=example，dc=com对象类：posixGroup cn:miners编号：5000

dn:uid=john，ou=People，dc=example，dc=com对象类：inetOrgPerson对象类：posixAccount对象类：shadowAccount uid:john sn:Doe givenName:john cn:john Doe uidNumber:10000 gidNumber:5000用户密码：johnldap gecos:john Doe loginShell:/bin/bash homeditory:/home/john

目录中的uid和gid值不要与本地值冲突，这一点很重要。请使用较高的数字范围，例如从5000开始。通过在ldap high中设置uid和gid值，您还可以更轻松地控制本地用户与ldap用户的操作。稍后将详细介绍。

添加内容：

**ldapadd-x-dcn=admin，dc=example，dc=com-W-f add\_content.ldif**

输入LDAP密码：\*\*\*\*\*\*\*\*

添加新条目“ou=People，dc=example，dc=com”

添加新条目“ou=Groups，dc=example，dc=com”

添加新条目“cn=miners，ou=Groups，dc=example，dc=com”

添加新条目“uid=john，ou=People，dc=example，dc=com”

我们可以通过ldapsearch实用程序检查信息是否已正确添加：

**ldapsearch-x-LLL-bdc=example，dc=com&apos;uid=john&apos;cn编号**

dn:uid=john，ou=People，dc=example，dc=com cn:john-Doe-gid号码：5000

开关说明：

•“简单”绑定；不会使用默认的SASL方法*-x:*

•禁用打印无关信息*-LLL：*

•查找john用户的“过滤器”*uid=john:*

•请求显示某些属性（默认为显示所有属性）*cn编号：*

#### 1.4.修改slapd配置数据库

还可以查询和修改slapd配置DIT。

•使用ldapmodify将“Index”（DbIndex属性）添加到{1}mdb，cn=config数据库（dc=example，dc=com）中。创建一个文件，称之为uid\_Index.ldif，包含以下内容：

dn:olcDatabase={1}mdb，cn=config add:olcDbIndex olcDbIndex:mail eq，然后发出以下命令：

**sudo ldapmodify-Q-Y EXTERNAL-H ldapi://-f uid\u index.ldif**

修改条目“olcDatabase={1}mdb，cn=config”可以通过以下方式确认更改：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi:///-b\cn=config&apos;（olcDatabase={1}mdb）&apos;olcDbIndex**

dn:olcDatabase={1}mdb，cn=config olcDbIndex:objectClass eq olcDbIndex:cn，uid eq olcDbIndex:uidNumber，gidNumber eq olcDbIndex:member，memberUid eq olcDbIndex:mail eq，sub

•让我们添加一个模式。首先需要将其转换为LDIF格式。除了在/etc/ldap/schema目录中转换的模式外，还可以找到未转换的模式。

•从slapd配置数据库中删除模式并非易事。在测试系统上练习添加模式。

•在添加任何模式之前，应检查已安装的模式（显示的是默认的开箱即用输出）：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi:///-b\cn=schema，cn=config dn**

dn:cn=schema，cn=config

dn:cn={0}核心，cn=schema，cn=config

dn:cn={1}余弦，cn=schema，cn=config

dn:cn={2}nis，cn=schema，cn=config

dn:cn={3}inetorgperson，cn=schema，cn=config

在下面的示例中，我们将添加CORBA模式。

1.         创建包含以下行的转换配置文件schema\_convert.conf：

include/etc/ldap/schema/core.schema include/etc/ldap/schema/corba.schema include/etc/ldap/schema/cosine.schema include/etc/ldap/schema/duaconf.schema include/etc/ldap/schema/dyngroup.schema include/etc/ldap/schema/inetorgperson.schema include/etc/ldap/schema/misc、 schema include/etc/ldap/schema/nis.schema include/etc/ldap/schema/openldap.schema include/etc/ldap/schema/ppolicy.schema include/etc/ldap/schema/ldapns.schema include/etc/ldap/schema/pmi.schema

2.         创建输出目录ldif\_output。

3.         确定架构的索引：**slapcat-f schema\_convert.conf-f ldif\_output-n0 | grep corba，cn=schema**

cn={2}corba，cn=schema，cn=config

当slapd接收具有相同父DN的对象时，它将为该对象创建索引。

大括号中包含索引：{X}。

4.         使用slapcat执行转换：

**slapcat-f schema\u convert.conf-f ldif\u output-n0-H\ldap:///cn={2} corba，cn=schema，cn=config-lcn=corba.ldif**

转换后的模式现在位于cn=corba.ldif中

5.         编辑cn=corba.ldif以获得以下属性：

dn:cn=corba，cn=schema，cn=config…cn:corba

同时从底部拆下以下行：

StructureObjectClass:olcSchemaConfig entryUUID:52109a02-66ab-1030-8be2-bbf166230478创建者名称：cn=config createTimestamp:20110829165435Z

entryCSN:20110829165435.935248Z#000000#000#000000修饰符名称：cn=config modifyTimestamp:20110829165435Z

属性值将有所不同。

6.         最后，使用ldapadd将新架构添加到slapd config DIT：

**sudo ldapadd-Q-Y EXTERNAL-H ldapi://-f cn\=corba.ldif**

添加新条目“cn=corba，cn=schema，cn=config”

7.         确认当前加载的架构：**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi://-b cn=schema，cn=config dn**

dn:cn=schema，cn=config

dn:cn={0}核心，cn=schema，cn=config

dn:cn={1}余弦，cn=schema，cn=config

dn:cn={2}nis，cn=schema，cn=config

dn:cn={3}inetorgperson，cn=schema，cn=config

dn:cn={4}corba，cn=schema，cn=config

对于要使用LDAP进行身份验证的外部应用程序和客户端，它们都需要专门进行配置。有关详细信息，请参阅相应的客户端文档。

#### 1.5.记录

在实现基于OpenLDAP的解决方案时，slapd的活动日志记录是必不可少的，但必须在软件安装后手动启用。否则，日志中将只显示基本消息。

与任何其他slapd配置一样，日志记录是通过slapd配置数据库启用的。

OpenLDAP提供了多个日志子系统（级别），每个子系统都包含较低的一个（附加）。可以尝试的一个好级别是stats。slapd config[99]手册页对不同的子系统有更多的说明。

创建包含以下内容的logging.ldif文件：

dn:cn=config changetype:modify replace:olcLogLevel olcLogLevel:stats实现更改：**sudo ldapmodify-Q-Y EXTERNAL-H ldapi://-f logging.ldif**

这将产生大量日志记录，并且在系统投入生产后，您将希望将日志限制回较低的详细级别。在这种详细模式下，主机的syslog引擎（rsyslog）可能很难跟上，可能会删除消息：RSIGPRODS2177：IMuxSokes从PID 2547丢失了228条消息，因为速率限制，您可以考虑对RysLogo的配置进行更改。

#禁用速率限制#（默认值为5秒内200条消息；下面我们将5变为0）

$SystemLogRateLimitInterval 0，然后重新启动rsyslog守护程序：**sudo systemctl重新启动syslog.service**

#### 1.6.复制

随着越来越多的网络系统开始依赖LDAP服务，LDAP服务变得越来越重要。在这样的环境中，标准做法是在LDAP中构建冗余（高可用性），以防止LDAP服务器无响应时造成严重破坏。这是通过LDAP复制完成的。

复制是通过Syncrepl引擎实现的。这允许使用使用者同步更改

-提供者模型。我们将在本指南中实施的特定类型的复制是以下模式的组合：refreshAndPersist和delta syncrepl。这使提供者在更改条目后立即将其推送到使用者，但除此之外，只发送实际更改，而不发送整个条目。

##### 1.6.1. 提供程序配置

首先配置提供程序。

1.创建包含以下内容的LDIF文件，并将其命名为provider\_sync.LDIF：

#向前端数据库添加索引。dn:olcDatabase={1}mdb，cn=config changetype:modify add:olcDbIndex olcDbIndex:entryCSN eq-

添加：olcDbIndex olcDbIndex:entryUUID eq

#加载syncprov和accesslog模块。dn:cn=module{0}，cn=config changetype:modify add:olcModuleLoad olcModuleLoad:syncprov-

添加：olcModuleLoad olcModuleLoad:accesslog

#Accesslog数据库定义dn:olcDatabase={2}mdb，cn=config对象类：olcDatabaseConfig对象类：olcMdbConfig olcDatabase:{2}mdb

olcdb目录：/var/lib/ldap/accesslog olcSuffix:cn=accesslog

olcRootDN:cn=admin，dc=example，dc=com olcDbIndex:default eq

olcDbIndex:entryCSN，objectClass，reqEnd，reqResult，reqStart

#Accesslog数据库syncprov。dn:olcOverlay=syncprov，olcDatabase={2}mdb，cn=config changetype:add

objectClass:olcOverlayConfig objectClass:olcSyncProvConfig olcOverlay:syncprov olcSpNoPresent:TRUE olcSpReloadHint:TRUE

#主数据库的syncrepl提供程序

dn:olcOverlay=syncprov，olcDatabase={1}mdb，cn=config changetype:add

对象类：olcOverlayConfig

objectClass:olcSyncProvConfig olcOverlay:syncprov olcSpNoPresent:TRUE

#主要数据库dn的访问日志覆盖定义：olcOverlay=accesslog，olcDatabase={1}mdb，cn=config objectClass:olcOverlayConfig objectClass:olcAccessLogConfig olcOverlay:accesslog olcAccessLogDB:cn=accesslog olcaccesslogps:writes olcAccessLogSuccess:TRUE#每天扫描访问日志数据库，和早于7天的清除条目olcAccessLogPurge:07+00:00 01+00:00

更改LDIF文件中的rootDN，使其与目录中的rootDN相匹配。

2.         创建目录：

**sudo-u openldap mkdir/var/lib/ldap/accesslog**

3.         添加新内容：

**sudo ldapadd-Q-Y外部-H ldapi://-f provider\u sync.ldif**

现在已配置提供程序。

##### 1.6.2. 消费者配置

现在配置消费者。

1.         通过第1.1节“安装”安装软件[p.116]。确保slapd config数据库与提供程序的数据库相同。特别是，确保模式和数据库后缀相同。

2.         创建包含以下内容的LDIF文件，并将其命名为consumer\_sync.LDIF：

dn:cn=module{0}，cn=config changetype:modify add:olcModuleLoad olcModuleLoad:syncprov

dn:olcDatabase={1}mdb，cn=config changetype:modify add:olcDbIndex olcDbIndex:entryUUID eq-

地址：olcSyncRepl

olcSyncRepl:rid=0提供程序=ldap://ldap01.example.com bindmethod=simple binddn=“cn=admin，dc=example，dc=com”

credentials=secret searchbase=“dc=example，dc=com”logbase=“cn=accesslog”logfilter=“（&（objectClass=auditWriteObject）（reqResult=0））”schemacheck=on type=refresh和persist retry=“60+”syncdata=accesslog-

地址：olcUpdateRef

olcUpdateRef：ldap://ldap01.example.com

确保以下属性具有正确的值：

•（提供程序服务器的主机名——本例中为ldap01.example.com——或IP地址）*供应商*

•（您正在使用的管理员DN）*宾顿*

•（您正在使用的管理员DN密码）*资格证书*

•（您正在使用的数据库后缀）*搜索库*

•（提供商服务器的主机名或IP地址）*olcUpdateRef*

•（副本ID，标识副本的唯一3位数字。每个使用者应至少有一个rid）*摆脱*

3.添加新内容：

**sudo ldapadd-Q-Y外部-H ldapi://-f consumer\_sync.ldif**

你完了。这两个数据库（后缀：dc=example，dc=com）现在应该正在同步。

##### 1.6.3. 测试

复制启动后，您可以通过运行

**ldapsearch-z1-LLLQY EXTERNAL-H ldapi://-s base-b dc=example，dc=com contextCSN**

dn:dc=example，dc=com

上下文编号：20120201193408.178454Z#000000#000#000000

在提供者和使用者上。一旦两台机器的输出（上例中为20120201193408.178454Z#000000#000#000000）匹配，就可以进行复制。每次在提供程序中进行更改时，此值都会更改，使用者中的值也会更改。

如果您的连接速度慢和/或ldap数据库大，则可能需要一段时间才能使使用者的contextCSN与提供者的匹配。但是，您会知道它正在进步，因为消费者的上下文CSN将稳步增加。

如果消费者的contextCSN丢失或与提供程序不匹配，则应停止并解决问题，然后再继续。尝试检查提供程序中的slapd（syslog）和auth日志文件，以查看使用者的身份验证请求是否成功，或者其检索数据的请求（它们看起来像许多ldapsearch语句）是否没有返回错误。

要测试它是否工作，只需在使用者上查询数据库中的DNs：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi://-b dc=example，dc=com dn**

您应该看到用户“john”和组“miners”以及节点“People”和“Groups”。

#### 1.7. 访问控制

对用户应该被授予资源的访问类型（读、写等）的管理称为访问控制。涉及的配置指令称为访问控制列表或ACL。

当我们安装slapd包时，各种ACL都自动设置。我们将研究这些默认设置的一些重要后果，在这样做的过程中，我们将了解ACL是如何工作的以及它们是如何配置的。

为了获得LDAP查询的有效ACL，我们需要查看被查询数据库的ACL条目以及特殊前端数据库实例的ACL条目。如果前者的ACL不匹配，则属于后者的ACL将充当默认ACL。前端数据库是第二个要查询的数据库，要应用的ACL是这两个ACL源中第一个匹配的数据库（“第一个匹配获胜”）。以下命令将分别给出mdb数据库（“dc=example，dc=com”）和前端数据库的ACL：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi://-b\cn=config&apos;（olcDatabase={1}mdb）&apos;olcAccess**

dn:olcDatabase={1}mdb，cn=config

olcAccess:{0}到attrs=userPassword通过匿名身份验证自写\*无olcAccess:{1}到attrs=shadowLastChange通过自写\*读取olcAccess:{2}到\*读取

rootDN始终对其数据库具有完全权限，并且不需要包含在任何ACL中。

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi:///-b\cn=config&apos;（olcDatabase={-1}前端）&apos;olcAccess**

dn:olcDatabase={-1}前端，cn=config

olcAccess:{0}到\*按dn.exact=gidNumber=0+uidNumber=0，cn=peercred，cn=external，cn=auth manage by\*break olcAccess:{1}到dn.exact=”“by\*read olcAccess:{2}到dn.base=“cn=Subschema”by\*读取前两个ACL是至关重要的：

olcAccess:{0}到attrs=userPassword通过匿名身份验证自写\*无olcAccess:{1}到attrs=shadowLastChange通过自写\*读取可以用不同的方式表示，以便于理解：

to attrs=userPassword

通过匿名身份验证自行编写\*无

to attrs=shadowLastChange by self write by\*read

这些ACL强制执行以下内容：

•为userPassword属性提供匿名“身份验证”访问，以便用户可以进行身份验证或绑定。也许与直觉相反，即使不需要匿名访问DIT，也需要“通过匿名身份验证”，否则这将是一个鸡和蛋的问题：在身份验证之前，所有用户都是匿名的。

•by self write ACL将userPassword属性的写入权限授予作为属性所在dn进行身份验证的用户。换句话说，用户可以更新自己条目的userPassword属性。

•userPassword属性是所有其他用户都无法访问的，rootDN除外，它始终具有访问权限，不需要明确提及。

•为了让用户使用passwd或其他实用程序更改自己的密码，用户自己的shadowLastChange属性需要是可写的。所有其他目录用户都可以读取此属性的内容。

此DIT可以匿名搜索，因为此ACL中的“to\*by\*read”授予任何人（包括匿名用户）对其他所有内容的读取权限：

读

如果这是不需要的，那么您需要更改ACL。要在绑定请求期间强制身份验证，您也可以使用“olcRequire:authc”指令（或与修改的ACL结合使用）。

如前所述，没有为slapd config数据库创建管理帐户（“rootDN”）。但是，有一个SASL身份被授予对它的完全访问权限。它表示本地主机的超级用户（root/sudo）。这是：

dn.exact=gidNumber=0+uidNumber=0，cn=peercred，cn=external，cn=auth以下命令将显示slapd config数据库的ACL：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi:///-b\cn=config&apos;（olcDatabase={0}config）&apos;olcAccess**

dn:olcDatabase={0}配置，cn=config

olcAccess:{0}到\*按dn。精确=gidNumber=0+uidNumber=0，cn=peercred，cn=external，cn=auth按\*中断管理

由于这是一个SASL标识，因此在调用所讨论的LDAP实用程序时，我们需要使用SASL机制，我们在本指南中已经多次看到了它。这是外部机制。有关示例，请参见前面的命令。请注意：

1.         必须使用sudo成为根标识，ACL才能匹配。

2.         外部机制通过IPC（UNIX域套接字）工作。这意味着您必须使用ldapi URI格式。

获取所有ACL的简洁方法如下：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi:///-b\cn=config&apos;（olcAccess=\*）olcAccess olcSuffix**

关于访问控制的话题有很多话要说。请参阅手册页了解slapd.access[100]。

#### 1.8. TLS

对OpenLDAP服务器进行身份验证时，最好使用加密会话。这可以通过使用传输层安全性（TLS）来实现。

在这里，我们将成为自己的证书颁发机构，然后创建并签署LDAP服务器证书作为CA。由于slapd是使用gnutls库编译的，因此我们将使用certtool实用程序来完成这些任务。

1.         安装gnutls bin和ssl证书包：

**sudo-apt安装gnutls-bin-ssl证书**

2.         为证书颁发机构创建私钥：

**sudo sh-c“certtool——生成私钥>/etc/ssl/private/cakey.pem”**

3.         创建模板/file/etc/ssl/ca.info以定义ca：

cn=示例公司ca

证书签名密钥

4.         创建自签名CA证书：

**sudo certtool--生成自签名\--加载privkey/etc/ssl/private/cakey.pem**

**--模板/etc/ssl/ca.info\**

**--outfile/etc/ssl/certs/cacert.pem**

5.         为服务器创建私钥：

**sudo certtool--生成私钥\--位1024\**

**--outfile/etc/ssl/private/ldap01\_slapd\_key.pem**

将文件名中的ldap01替换为服务器的主机名。为将要使用它们的主机和服务命名证书和密钥将有助于保持清晰。

6.         创建/etc/ssl/ldap01.info文件，其中包含：

组织机构=示例公司cn=ldap01.Example.com tls\u www\u服务器加密\u密钥签名\u密钥过期\u天数=3650

上述证书有效期为10年。相应地调整。

7.         创建服务器的证书：

**sudo certtool--生成证书\--加载privkey/etc/ssl/private/ldap01\_slapd\_key.pem\**

**--加载ca证书/etc/ssl/certs/cacert.pem \--加载ca私钥/etc/ssl/private/cakey.pem\**

**--模板/etc/ssl/ldap01.info\**

**--outfile/etc/ssl/certs/ldap01\_slapd\_cert.pem**

8.         调整权限和所有权：

**sudo chgrp openldap/etc/ssl/private/ldap01\_slapd\_key.pem sudo chmod 0640/etc/ssl/private/ldap01\_slapd\_key.pem sudo gpasswd-openldap ssl证书**

9.         现在重新启动slapd，因为我们已将“openldap”用户添加到“ssl证书”组：

**sudo systemctl重新启动slapd.service**

您的服务器现在已准备好接受新的TLS配置。

使用以下内容创建文件certinfo.ldif（进行相应调整，我们的示例假设我们使用https://www.cacert.org):

dn:cn=config

添加：olctlscapertificatefile

olctlsca证书文件：/etc/ssl/certs/cacert.pem-

添加：olcTLSCertificateFile

olcTLSCertificateFile:/etc/ssl/certs/ldap01\u slapd\u cert.pem

-

添加：olcTLSCertificateKeyFile

olcTLSCertificateKeyFile:/etc/ssl/private/ldap01\_slapd\_key.pem

使用ldapmodify命令通过slapd config数据库告知slapd我们的TLS工作：**sudo ldapmodify-Y EXTERNAL-H ldapi://-f certinfo.ldif**

与流行的观点相反，使用加密不需要ldaps://in/etc/default/slapd。你应该：

SLAPD\_SERVICES=“ldap:///ldapi://”

TLS/SSL上的LDAP（ldaps://）已被弃用，取而代之的是StartTLS。后者指的是现有LDAP会话（在TCP端口389上侦听）受到TLS/SSL的保护，而LDAP（如HTTPS）是一种与通过TCP端口636运行的启动协议不同的加密协议。

#### 1.9. 复制和TLS

如果已设置服务器之间的复制，则通常会加密（StartTLS）复制流量以防止电子窃听。这不同于我们在上面使用加密和身份验证。在本节中，我们将以TLS身份验证工作为基础。

这里的假设是，您已经根据第1.6节“复制”[p.123]在提供者和使用者之间建立了复制，并根据第1.8节“TLS”[p.129]为提供者上的身份验证配置了TLS。

如前所述，复制的目标（对我们来说）是LDAP服务的高可用性。由于我们在提供者上有用于身份验证的TLS，因此我们将在使用者上要求相同的TLS。但是，除此之外，我们还希望加密复制流量。剩下要做的是为使用者创建密钥和证书，然后进行相应的配置。我们将在提供者上生成密钥/证书，以避免必须创建另一个CA证书，然后将必要的资料传递给使用者。

1.关于提供者，

创建保留目录（将用于最终传输），然后创建使用者的私钥：

**mkdir ldap02 ssl cd ldap02 ssl**

**sudo certtool--生成私钥\--位1024\**

**--输出文件ldap02\_slapd\_key.pem**

为消费者服务器创建信息文件ldap02.info，并相应调整其值：

组织机构=示例公司cn=ldap02.Example.com tls\u www\u服务器加密\u密钥签名\u密钥过期\u天数=3650

创建消费者证书：

**sudo certtool--生成证书\--加载私钥ldap02\u slapd\u key.pem\**

**--加载ca证书/etc/ssl/certs/cacert.pem \--加载ca私钥/etc/ssl/private/cakey.pem\**

**--模板ldap02.info\**

**--输出文件ldap02\_slapd\_cert.pem cp/etc/ssl/certs/cacert.pem。**获取CA证书的副本：

我们结束了。现在将ldap02 ssl目录传输到使用者。这里我们使用scp（相应调整）：

**光盘scp-r ldap02 ssluser@consumer:**

2.在消费者方面,，

配置TLS身份验证：

**sudo apt安装ssl证书sudo gpasswd-一个openldap ssl证书**

**sudo cp ldap02\_slapd\_cert.pem cacert.pem/etc/ssl/certs sudo cp ldap02\_slapd\_key.pem/etc/ssl/private sudo chgrp openldap/etc/ssl/private/ldap02\_slapd\_key.pem sudo chmod 0640/etc/ssl/private/ldap02\_slapd\_key.pem sudo系统ctl重启slapd.service**

创建具有以下内容的文件/etc/ssl/certinfo.ldif（相应调整）：

dn:cn=config

添加：olctlscapertificatefile

olctlsca证书文件：/etc/ssl/certs/cacert.pem-

添加：olcTLSCertificateFile

olcTLSCertificateFile:/etc/ssl/certs/ldap02\u slapd\u cert.pem-

添加：olcTLSCertificateKeyFile

olcTLSCertificateKeyFile:/etc/ssl/private/ldap02\_slapd\_key.pem

配置slapd配置数据库：

**sudo ldapmodify-Y EXTERNAL-H ldapi://-f certinfo.ldif**

在提供程序上配置/etc/default/slapd as（slapd\_服务）。

3.在消费者方面,，

为用户端复制配置TLS。通过添加一些TLS选项来修改现有的olcSyncrepl属性。这样，我们将第一次看到如何更改属性的值。

使用以下内容创建文件consumer\_sync\_tls.ldif：

dn:olcDatabase={1}mdb，cn=config replace:olcSyncRepl

olcSyncRepl:rid=0提供程序=ldap://ldap01.example.com bindmethod=简单

binddn=“cn=admin，dc=example，dc=com”credentials=secret searchbase=“dc=example，dc=com”logbase=“cn=accesslog”logfilter=“（&（objectClass=auditWriteObject）（reqResult=0））”schemacheck=on type=refreshandspersist retry=“60+”syncdata=accesslog starttls=critical tls\u reqcert=demand

额外选项分别指定使用者必须使用StartTLS和CA证书来验证提供者的身份。还要注意用于更改属性（“替换”）值的LDIF语法。

实施以下更改：并重新启动slapd：**sudo ldapmodify-Y EXTERNAL-H ldapi://-f consumer\u sync\u tls.ldif sudo systemctl restart slapd.service**

4.关于提供者，

检查TLS会话是否已建立。在/var/log/syslog中，如果设置了“conns”级别的日志记录，您应该会看到类似以下内容的消息：

slapd[3620]：conn=1047 fd=20从IP=10.153.107.229:57922（IP=0.0.0:389）接受slapd[3620]：conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037 slapd[3620]：conn=1047 op=0 STARTTLS

slapd[3620]：conn=1047 op=0 RESULT oid=err=0 text=slapd[3620]：conn=1047 fd=20 TLS已建立TLS\_ssf=128 ssf=128 slapd[3620]：conn=1047 op=1 BIND dn=“cn=admin，dc=example，dc=com”method=128 slapd[3620]：conn=1047 op=1 BIND dn=“cn=admin，dc=example，dc=com”mech=0 slapd[3620]：conn=1047 op=1 RESULT tag=97 err=0 text

#### 1.10. LDAP身份验证

一旦您有了一个工作的LDAP服务器，您就需要在客户机上安装库，以便知道如何和何时联系它。在Ubuntu上，这通常是通过安装libnss ldap包来实现的。

此软件包将引入其他工具，帮助您完成配置步骤。立即安装此软件包：**sudo-apt安装libnss-ldap**

系统将提示您输入LDAP服务器的详细信息。如果您犯了错误，可以使用以下方法重试：**sudo dpkg重新配置ldap身份验证配置**

对话框的结果可以在/etc/ldap.conf中看到。如果服务器需要菜单中未包含的选项，请相应地编辑此文件。

现在为NSS配置LDAP配置文件：将系统配置为使用LDAP进行身份验证：**sudo auth client config-t nss-p lac\_ldap sudo pam auth update**

从菜单中，选择LDAP和您需要的任何其他身份验证机制。

您现在应该能够使用基于LDAP的凭据登录。

如果正在使用复制，LDAP客户端将需要引用多个服务器。在/etc/ldap.conf中，您将看到如下内容：urildap://ldap01.example.com ldap://ldap02.example.com

如果提供者（ldap01）没有响应，请求将超时，消费者（ldap02）将尝试联系。

如果要使用LDAP存储Samba用户，则需要配置Samba服务器以使用LDAP进行身份验证。有关详细信息，请参见第2节“Samba和LDAP”[p.140]。

libnss ldap包的另一种替代方法是libnss ldapd包。然而，这将带来可能不需要的nscd包。之后只需将其移除即可。

#### 1.11. 用户和组管理

ldap utils包附带了足够多的实用程序来管理目录，但所需的长字符串选项可能会使它们成为使用的负担。ldapscripts包包含这些实用程序的包装脚本，有些人认为这些实用程序更易于使用。

安装软件包：**sudo apt安装ldapscripts**

然后编辑文件/etc/ldapscripts/ldapscripts.conf，以获得与以下类似的结果：

服务器=本地主机

BINDDN=&apos;cn=admin，dc=example，dc=com&apos;BINDPWDFILE=“/etc/ldapscripts/ldapscripts.passwd”

后缀=&apos;dc=example，dc=com&apos;

GSUFFIX=&apos;ou=Groups&apos;

USUFFIX=&apos;ou=人民的

MSUFFIX=&apos;ou=计算机&apos;

GIDSTART=10000

UIDSTART=10000

中间起动=10000

现在，创建ldapscripts.passwd文件以允许rootDN访问目录：

**sudo sh-c“echo-n&apos;secret&apos;>/etc/ldapscripts/ldapscripts.passwd”sudo chmod 400/etc/ldapscripts/ldapscripts.passwd**

用数据库的rootDN用户的实际密码替换“secret”。

这些脚本现在可以帮助管理目录了。以下是一些如何使用它们的示例：

•创建新用户：**sudo ldapadduser george示例**

这将创建一个uid为george的用户，并将用户的主要组（gid）设置为example

•更改用户密码：

**sudo ldapsetpasswd george**更改用户uid=george、ou=People、dc=example、dc=com的密码新密码：

**新密码（验证）：**

•删除用户：**SudoLDAPdeleteUser george**

•添加一个组：**sudo ldapaddgroup qa**

•删除组：

**sudo ldapdeletegroup qa**

•将用户添加到组：**sudo ldapaddusertogroup george qa**

您现在应该看到qa组的memberUid属性，其值为george。

•从组中删除用户：**sudo ldapdeleteuserfromgroup george qa**

现在应该从qa组中删除memberUid属性。

•ldapmodifyuser脚本允许您添加、删除或替换用户的属性。该脚本使用与ldapmodify实用程序相同的语法。例如：

**sudo ldapmodifyuser george**#即将修改以下条目：dn:uid=george，ou=People，dc=example，dc=com objectClass:account objectClass:posixAccount cn:george uid:george uidNumber:1001 gidNumber:1001 homeditory:/home/george loginShell:/bin/bash gecos:george description:User account

用户密码：：E1NTSEF9EXFSTFCYWLHWKF1EGUYBVDFWHZKRZJVMJFTSG9VCHK=

#在此处输入修改，以CTRL-D结束。

dn:uid=george，ou=People，dc=example，dc=com替换：gecos gecos:george Carlin

用户的GECO现在应该是“George Carlin”。

•ldapscripts的一个很好的特性是模板系统。模板允许您自定义用户、组和计算机对象的属性。例如，要启用用户模板编辑/etc/ldapscripts/ldapscripts.conf，请执行以下操作：

UTEMPLATE=“/etc/ldapscripts/ldapadduser.template”

在/usr/share/doc/ldapscripts/examples目录中有一些示例模板。将ldapadduser.template.sample文件复制或重命名为/etc/ldapscripts/ldapadduser.template：

**sudo cp/usr/share/doc/ldapscripts/examples/ldapadduser.template.sample\**

**/etc/ldapscripts/ldapadduser.template**

编辑新模板以添加所需的属性。以下内容将创建objectClass为inetOrgPerson的新用户：

dn:uid=<user>，<usuffix>，<suffix>对象类：inetOrgPerson对象类：posixAccount cn:<user>sn:<ask>uid:<user>uidNumber:<uid>gidNumber:<gid>homeditory:<home>loginShell:<shell>gecos:<user>说明：用户帐户名称：员工

请注意用于sn属性的<ask>选项。这将使ldapadduser提示您输入其值。

包中的一些实用程序未在此处介绍。以下是完整的列表：

ldaprenamechine[101]ldapadduser[102]ldapdeleteuserfromgroup[103]ldapfinger[104]ldapid[105]ldapgid[106]ldapmodifyuser[107]ldaprenameuser[108]lsldldldap[109]ldapaddusertogroup[110]ldapsetpasswd[111]ldapinit[112]ldapaddgroup[113]ldapdeletegroup[114]ldapmodifygroup[115]ldapdeletemechine[116]ldapenamegrain[118]ldapmodifymachine[119]ldapsetprimarygroup[120]ldapdeleteuser[121]

#### 1.12. 备份和恢复

现在，ldap正以我们想要的方式运行，是时候确保我们可以保存所有工作并根据需要进行恢复了。

我们需要的是一种备份ldap数据库的方法，特别是后端（cn=config）和前端（dc=example，dc=com）。如果我们要将这些数据库备份到，比如说，/export/backup，我们可以使用slapcat，如以下脚本所示，称为/usr/local/bin/ldapbackup：

#!/bin/bash

备份路径=/export/BACKUP SLAPCAT=/usr/sbin/SLAPCAT

nice${SLAPCAT}-n0>${BACKUP\_PATH}/config.ldif nice${SLAPCAT}-n1>${BACKUP\_PATH}/example.com.ldif nice${SLAPCAT}-n2>${BACKUP\_PATH}/access.ldif chmod 640${BACKUP\_PATH}/\*.ldif

这些文件是未压缩的文本文件，包含ldap数据库中的所有内容，包括树布局、用户名和每个密码。因此，您可能需要考虑制作/导出/备份加密分区，甚至当脚本创建这些分区时，还要对这些文件进行加密。

理想情况下，您应该同时执行这两项操作，但这取决于您的安全需求。

然后，我们只需要使用cron脚本，让它尽可能频繁地运行这个程序。对许多人来说，一天一次就足够了。对于其他人来说，需要更多的时间。下面是一个名为/etc/cron.d/ldapbackup的cron脚本示例，该脚本每晚22:45运行：

MAILTO=备份-emails@domain.com

45 22\*\*\*root/usr/local/bin/ldapbackup

现在文件已经创建，应该将它们复制到备份服务器。

假设我们重新安装了ldap，恢复过程可能如下所示：

**sudo systemctl stop slapd.service sudo mkdir/var/lib/ldap/accesslog**

**sudo slapadd-F/etc/ldap/slapd.d-n0-l/export/backup/config.ldif sudo slapadd-F/etc/ldap/slapd.d-n1-l/export/backup/domain.com.ldif sudo slapadd-F/etc/ldap/slapd.d-n2-l/export/backup/access.ldif sudo chown-R openldap:openldap/etc/ldap/slapd.d/sudo chown-R openldap:openldap/var/lib/ldap/sudo systemctl启动slapd.service**

#### 1.13. 资源

•主要资源是上游文档：www.openldap.org[122]

•slapd软件包附带许多手册页。以下是一些重要的建议，特别是考虑到本指南中介绍的材料：

slapd[123]slapd配置[124]slapd.access[125]slapo syncprov[126]

•其他手册页：

验证客户端配置[127]pam验证更新[128]

•Zytrax针对火箭科学家的LDAP[129]；对LDAP的不那么迂腐但全面的处理

•Ubuntu社区OpenLDAP wiki[130]页面包含一组注释

•O&apos;Reilly的LDAP系统管理[131]（教科书；2003年）

•Packt掌握OpenLDAP[132]（教科书；2007年）

## 2.Samba和LDAP

本节介绍Samba与LDAP的集成。Samba服务器的角色将是

“独立”服务器和LDAP目录将提供身份验证层，此外还包含Samba运行所需的用户、组和计算机帐户信息（在其3种可能的角色中的任何一种）。先决条件是一个OpenLDAP服务器，它配置了一个可以接受身份验证请求的目录。有关满足此要求的详细信息，请参见第1节“OpenLDAP服务器”[p.115]。本节完成后，您需要决定具体希望Samba为您做什么，然后相应地进行配置。

本指南假定LDAP和Samba服务在同一台服务器上运行，因此在cn=config下更改内容时使用SASL外部身份验证。如果情况并非如此，则必须在ldap服务器上运行这些ldap命令。

#### 2.1. 软件安装

将Samba与LDAP集成时需要两个包：Samba和smbldap工具。

严格来说，不需要smbldap tools包，但除非您有其他方法在LDAP上下文中管理各种Samba实体（用户、组、计算机），否则您应该安装它。

立即安装这些软件包：**sudoapt安装samba smbdap工具**

#### 2.2. LDAP配置

我们现在将配置LDAP服务器，以便它能够容纳Samba数据。在本节中，我们将执行三项任务：

1.         导入架构

2.         索引一些条目

3.         添加对象

##### 2.2.1. Samba模式

为了将OpenLDAP用作Samba的后端，逻辑上，DIT需要使用能够正确描述Samba数据的属性。这些属性可以通过引入Samba LDAP模式来获得。

我们现在就开始吧。

有关模式及其安装的更多信息，请参见第1.4节“修改slapd配置数据库”[p.120]。

1.         该模式可以在现在安装的samba包中找到，并且已经是ldif格式。我们可以通过一个简单的命令导入它：

**zcat/usr/share/doc/samba/examples/LDAP/samba.ldif.gz | sudo ldapadd-Q-Y EXTERNAL-H ldapi:///**

2.         要查询和查看此新架构，请执行以下操作：

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H ldapi://-b cn=schema，cn=config&apos;cn=\*samba\*&apos;**

##### 2.2.2. 桑巴指数

既然slapd已经了解了Samba属性，我们可以基于它们设置一些索引。当客户端在DIT上执行筛选搜索时，索引条目是一种提高性能的方法。

创建包含以下内容的文件samba\_index.ldif：

dn:olcDatabase={1}mdb，cn=config changetype:modify replace:olcDbIndex olcDbIndex:objectClass eq olcDbIndex:uidNumber，gidNumber eq olcDbIndex:loginShell eq olcDbIndex:uid，cn eq，sub olcDbIndex:memberUid eq，sub olcDbIndex:member，uniqueMember eq olcDbIndex:sambaSID eq olcDbIndex:sambaPrimaryGroupSID eq olcDbIndex:sambaGroupType eq olcDbIndex:sambaSIDList eq olcDbIndex:sambaDomainName eq olcDbIndex:default sub，eq

使用ldapmodify实用程序加载新索引：如果一切顺利，您应该使用ldapsearch查看新索引：**sudo ldapmodify-Q-Y EXTERNAL-H ldapi://-f samba\_index.ldif**

**sudo ldapsearch-Q-LLL-Y EXTERNAL-H\ldapi://-b cn=config olcDatabase={1}mdb olcDbIndex**

##### 2.2.3. 添加Samba LDAP对象

接下来，配置smbdap工具包以匹配您的环境。该包附带一个名为smbdap config的配置帮助程序脚本。不过，在运行它之前，您应该在/etc/samba/smb.conf中决定两个重要的配置设置：

•：如何了解该服务器。默认值来自服务器的主机名，但截断为15个字符。*电脑名称*

•：此服务器的工作组名称，或者，如果您以后决定将其设为域控制器，则此名称将为域。*工作组*

现在做出这些选择很重要，因为smbdap config将使用它们生成配置，该配置稍后将存储在LDAP目录中。如果您现在运行smbdap config，然后在/etc/samba/smb.conf中更改这些值，则会出现不一致。

当您对netbios名称和工作组满意后，通过运行配置脚本继续生成smbldap工具配置，该脚本将询问您一些问题：**sudosmbdap配置**

一些更重要的问题：

•：必须匹配稍后在/etc/samba/smb.conf中配置的内容。*工作组名称*

•：必须与配置ldap服务器时选择的ldap后缀匹配。*ldap后缀*

•其他ldap后缀：它们都与上面的ldap后缀相关。例如，对于ldap用户后缀，应该使用ou=People。

•和绑定密码：使用rootDN凭据。*ldap主绑定dn*

然后，smbdap填充脚本将添加Samba所需的LDAP对象。最好首先使用slapcat备份DIT：**sudo slapcat-l backup.ldif**

备份完成后，继续填充目录。它将要求您输入“域根”用户的密码，该用户也是LDAP中存储的“根”用户：**sudo-g 10000-u 10000-r 10000**

-g、-u和-r参数告诉smbldap工具在哪里开始LDAP用户的数字uid和gid分配。您应该选择一个不与本地/etc/passwd用户重叠的范围开始。

通过执行sudo smbdap populate-e Samba.LDIF，可以创建包含新Samba对象的LDIF文件。这允许您查看更改，确保一切都是正确的。如果是，请在不使用“-e”开关的情况下重新运行脚本。或者，您可以获取LDIF文件，并按照通常的方式导入其数据。

您的LDAP目录现在具有对Samba用户进行身份验证的必要信息。

#### 2.3. Samba配置

配置Samba有多种方法。有关一些常见配置的详细信息，请参见第18章，

*桑巴舞[p.305]*. 要将Samba配置为使用LDAP，请编辑其配置文件/etc/Samba/smb.conf，注释掉默认的passdb backend参数，并添加一些与LDAP相关的参数。确保使用与运行SMBLADP时相同的值：

#passdb backend=tdbsam工作组=示例

#LDAP设置

passdb backend=ldapsam：ldap://hostname ldap后缀=dc=示例，dc=com ldap用户后缀=ou=人员ldap组后缀=ou=组ldap机器后缀=ou=计算机ldap idmap后缀=ou=idmap

ldap admin dn=cn=admin，dc=example，dc=com#如果未配置TLS/SSL，则关闭ldap SSL=start TLS ldap passwd sync=yes

更改值以匹配您的环境。

该包提供的smb.conf相当长，并且有许多配置示例。无需任何注释就可以可视化它的一种简单方法是运行testparm-s。

现在将rootDN用户的密码（安装slapd包期间设置的密码）通知Samba：**sudo smbpasswd-W**

作为让LDAP用户能够连接到samba并进行身份验证的最后一步，我们需要这些用户也以“unix”用户的身份出现在系统中。一种方法是使用libnssldap。详细说明见第1.10节“LDAP身份验证”[p.134]一节，但我们只需要NSS部分。

1.         安装libnss ldap

sudo-apt安装libnss-ldap

不需要使用LDAP rootDN登录凭据，因此可以跳过该步骤。

2.         为NSS配置LDAP配置文件：

sudo auth客户端配置-t nss-p lac\_ldap

3.         重新启动Samba服务：

sudo systemctl重新启动smbd.service nmbd.service

4.         要快速测试设置，请查看getent是否可以列出Samba组：

**格滕集团**

...

帐户操作员：\*：548：

印刷操作员：\*：550：

备份操作员：\*：551：

复制者：\*：552：

如果您希望在新的基于LDAP的Samba中包含现有的LDAP用户，那么当然，还需要为他们提供一些额外的Samba特定属性。smbpasswd实用程序可以为您执行以下操作：**sudo smbpasswd-用户名**

系统将提示您输入密码。它将被视为该用户的新密码。与以前一样是合理的。请注意，此命令不能用于在LDAP中从头创建新用户（除非您使用的是ldapsam:trusted和ldapsam:editposix，本指南中未介绍）。

要管理用户、组和计算机帐户，请使用smbldap tools包提供的实用程序。以下是一些例子：

•要使用主目录添加新用户，请执行以下操作：**sudo smbdap useradd-a-P-m用户名**

-a选项添加Samba属性，-P选项在创建用户后调用smbdap passwd实用程序，允许您为用户输入密码。最后，-m创建一个本地主目录。使用getent命令进行测试：getentpasswdusername

如果没有得到响应，则说明libnss ldap配置不正确。

•要删除用户，请执行以下操作：**sudo smbdap userdel用户名**

在上面的命令中，使用-r选项删除用户的主目录。

•要添加组，请执行以下操作：**sudo smbdap groupadd-组名**

对于smbdap useradd，-a添加了Samba属性。

•使现有用户成为组成员：**sudo smbdap groupmod-m用户名groupname**

通过以逗号分隔的格式列出多个用户，-m选项可以一次添加多个用户。

•要从组中删除用户，请执行以下操作：**sudo smbdap groupmod-x用户名groupname**

•要添加Samba机器帐户：

**sudo smbdap useradd-t 0-w用户名**

将用户名替换为工作站的名称。-t0选项毫不延迟地创建机器帐户，而-w选项将用户指定为机器帐户。另外，请注意/etc/samba/smb.conf中的add machine脚本参数已更改为使用smbdap useradd。

smbldap tools包中有一些实用程序未在此处介绍。以下是完整的列表：

smbdap groupadd[133]smbdap groupdel[134]smbdap groupmod[135]smbdap groupshow[136]smbdap passwd[137]smbdap populate[138]smbdap useradd[139]smbdap userdel[140]smbdap userinfo[141]smbdap userlist[142]smbdap usermod[143]smbdap usershow[144]

#### 2.4. 资源

•有关安装和配置Samba的更多信息，请参阅本Ubuntu服务器指南第18章Samba[p.305]。

•上游Samba HOWTO集合[145]中记录了LDAP和Samba的多个地方。

•关于上述内容，具体参见passdb章节[146]。

•Linux Samba OpenLDAP HOWTO[147]虽然已过时（2007年），但其中包含有价值的注释。

•Samba Ubuntu社区文档[148]的主页上有大量链接，指向可能证明有用的文章。

## 3.Kerberos

Kerberos是一种基于可信第三方主体的网络身份验证系统。其他两方是用户和用户希望进行身份验证的服务。并非所有服务和应用程序都可以使用Kerberos，但对于那些可以使用Kerberos的服务和应用程序，它使网络环境更接近单点登录（SSO）。

本节介绍Kerberos服务器的安装和配置，以及一些示例客户端配置。

#### 3.1. 概述

如果您是Kerberos新手，那么在设置Kerberos服务器之前，有一些术语很容易理解。大多数术语都与您在其他环境中可能熟悉的内容有关：

•服务器提供的任何用户、计算机和服务都需要定义为Kerberos主体。*负责人：*

•用于服务负责人和特殊管理负责人。*实例：*

•Kerberos安装提供的独特控制领域。将其视为主机和用户所属的域或组。按照惯例，领域应该是大写的。默认情况下，ubuntu将使用转换为大写的DNS域（EXAMPLE.COM）作为域。*领域：*

•（KDC）由三部分组成：所有主体的数据库、身份验证服务器和票据授予服务器。对于每个领域，必须至少有一个KDC。*主要配送中心：*

•由认证服务器（AS）颁发，票据授予票据（TGT）在用户密码中加密，该密码仅为用户和KDC所知。*票务授予票务：*

•（TGS）应客户要求向其发出服务通知单。*票证授予服务器：*

•确认两位负责人的身份。一个主体是用户，另一个主体是用户请求的服务。票证建立一个加密密钥，用于在经过身份验证的会话期间进行安全通信。*门票：*

•是从KDC主体数据库提取的文件，包含服务或主机的加密密钥。*键表文件：*

为了将这些部分放在一起，一个领域至少有一个KDC，最好有更多的KDC用于冗余，其中包含一个主体数据库。当用户主体登录到配置为Kerberos身份验证的工作站时，KDC会发出票据授予票据（TGT）。如果用户提供的凭据匹配，则用户经过身份验证，然后可以从票证授予服务器（TGS）请求Kerberized服务的票证。服务票证允许用户对服务进行身份验证，而无需输入其他用户名和密码。

#### 3.2. Kerberos服务器

##### 3.2.1. 安装

在本次讨论中，我们将创建一个具有以下功能的MIT Kerberos域（编辑它们以满足您的需要）：

•EXAMPLE.COM*领域：*

•kdc01.example.com（192.168.0.1）*主要KDC：*

•kdc02.example.com（192.168.0.2）*辅助KDC：*

•史蒂夫*用户负责人：*

•史蒂夫/行政*行政负责人：*

强烈建议通过网络身份验证的用户的uid范围（例如，从5000开始）与本地用户的uid范围不同。

在安装Kerberos服务器之前，您的域需要一个正确配置的DNS服务器。由于Kerberos领域按约定与域名匹配，因此本节使用DNS文档第2.3节“主主机”[p.169]中配置的EXAMPLE.COM域。

此外，Kerberos是一种时间敏感的协议。因此，如果客户端计算机和服务器之间的本地系统时间相差超过五分钟（默认情况下），工作站将无法进行身份验证。要更正此问题，所有主机都应使用相同的网络时间协议（NTP）服务器进行时间同步。有关设置NTP的详细信息，请参见第4节“时间同步”[p.55]。

创建Kerberos领域的第一步是安装krb5 kdc和krb5管理服务器包。从终端输入：**sudo apt安装krb5 kdc krb5管理服务器**

在安装结束时，将要求您提供域的Kerberos和Admin服务器的主机名，这两个服务器可能是同一服务器，也可能不是同一服务器。

默认情况下，领域是从KDC的域名创建的。

接下来，使用kdb5\_newrealm实用程序创建新领域：**sudo krb5\_newrealm**

##### 3.2.2. 配置

安装过程中提出的问题用于配置/etc/krb5.conf文件。如果需要调整密钥分发中心（KDC）设置，只需编辑文件并重新启动krb5 KDC守护程序。如果您需要从头开始重新配置Kerberos，可能需要更改域名，那么可以通过键入

**sudo dpkg重新配置krb5 kdc**

1.一旦KDC正常运行，就需要一个管理员用户——管理员主体。建议使用与日常用户名不同的用户名。在终端提示中使用kadmin.local实用程序输入：

**sudo kadmin.local**作为主根进行身份验证/admin@EXAMPLE.COM使用密码。kadmin.local:addprinc steve/admin警告：没有为steve指定策略/admin@EXAMPLE.COM; 默认为无策略输入主体“steve”的密码/admin@EXAMPLE.COM":

重新输入负责人“steve”的密码/admin@EXAMPLE.COM“：校长”史蒂夫/admin@EXAMPLE.COM“创建。卡德明：退出

在上面的示例中，steve是主体，/admin是实例，@example.COM表示领域。“每天”原则，即用户原则steve@EXAMPLE.COM，并且应该只有正常的用户权限。

将EXAMPLE.COM和steve替换为您的领域和管理员用户名。

2.         接下来，新管理员用户需要具有适当的访问控制列表（ACL）权限。权限在/etc/krb5kdc/kadm5.acl文件中配置：steve/admin@EXAMPLE.COM \*

此项授予steve/admin对域中所有主体执行任何操作的能力。您可以配置具有更严格权限的主体，如果您需要初级人员可以在Kerberos客户端中使用的管理主体，这将非常方便。有关详细信息，请参阅kadm5.acl手册页。

3.         现在重新启动krb5管理服务器，使新ACL生效：

**sudo systemctl重新启动krb5-admin-server.service**

4.         可以使用kinit实用程序测试新用户主体：

**kinit steve/管理**史蒂夫/admin@EXAMPLE.COM的密码：

输入密码后，使用klist实用程序查看有关票证授予票证（TGT）的信息：

**克莱斯特**凭据缓存：文件：/tmp/krb5cc\_1000

校长：史蒂夫/admin@EXAMPLE.COM

发行到期本金

7月13日17:53:34 7月14日03:53:34 krbtgt/示例。COM@EXAMPLE.COM

其中，缓存文件名krb5cc\_1000由前缀krb5cc\_和用户id（uid）组成，在本例中为1000。您可能需要在KDC的/etc/hosts中添加一个条目，以便客户端可以找到KDC。例如：

192.168.0.1 kdc01.example.com kdc01

将192.168.0.1替换为KDC的IP地址。当您有一个包含由路由器分隔的不同网络的Kerberos域时，通常会发生这种情况。

5.允许客户端自动确定领域的KDC的最佳方法是使用DNS SRV记录。将以下内容添加到/etc/named/db.example.com：

\_kerberos.\_udp.EXAMPLE.COM。在SRV 1 0 88 kdc01.example.com中。

\_kerberos.\_tcp.EXAMPLE.COM。在SRV 1 0 88 kdc01.example.com中。

\_kerberos.\_udp.EXAMPLE.COM。在SRV 10 0 88 kdc02.example.com中。

\_kerberos.\_tcp.EXAMPLE.COM。在SRV 10 0 88 kdc02.example.com中。

\_kerberos-adm.\_tcp.EXAMPLE.COM。在SRV 1 0 749 kdc01.example.com中。

\_kpasswd.\_udp.EXAMPLE.COM。在SRV 1 0 464 kdc01.example.com中。

将EXAMPLE.COM、kdc01和kdc02替换为您的域名、主KDC和辅助KDC。

有关设置DNS的详细说明，请参阅第8章域名服务（DNS）[166页]。

您的新Kerberos领域现在已准备好对客户端进行身份验证。

#### 3.3. 次级KDC

一旦您的网络上有一个密钥分发中心（KDC），最好有一个辅助KDC，以防主KDC不可用。此外，如果您有位于不同网络中的Kerberos客户端（可能由使用NAT的路由器分隔），则明智的做法是在这些网络中的每个网络中放置一个辅助KDC。

1.         首先，安装软件包，当询问Kerberos和管理服务器名称时，输入主KDC的名称：**sudo apt安装krb5 kdc krb5管理服务器**

2.         安装包后，创建辅助KDC的主机主体。在终端提示中，输入：**kadmin-q“addprinc-randkey host/kdc02.example.com”**

发出任何kadmin命令后，系统将提示您输入用户名/admin@EXAMPLE.COM主体密码。

3.         提取keytab文件：

**kadmin-q“ktadd-norandkey-k keytab.kdc02 host/kdc02.example.com”**

4.         现在，当前目录中应该有一个keytab.kdc02，请将文件移动到/etc/krb5.keytab：

**sudo mv keytab.kdc02/etc/krb5.keytab**

如果keytab.kdc02文件的路径不同，请相应调整。

此外，您还可以使用klist实用程序在键表文件中列出主体，这在排除故障时非常有用：

**sudo klist-k/etc/krb5.keytab**

k选项表示该文件是一个keytab文件。

5.         接下来，每个KDC上都需要有一个kpropd.acl文件，其中列出了该领域的所有KDC。例如，在主KDC和辅助KDC上，创建/etc/krb5kdc/kpropd.acl：

host/kdc01.example。com@EXAMPLE.COMhost/kdc02.example。com@EXAMPLE.COM

6.         在辅助KDC上创建空数据库：

**sudo kdb5\_util-s create**

7.         现在启动kpropd守护进程，它侦听来自kprop实用程序的连接。kprop用于传输转储文件：**sudo kpropd-S**

8.         从主KDC上的终端，创建主体数据库的转储文件：

**sudo kdb5\_util dump/var/lib/krb5kdc/dump**

9.         提取主KDC的keytab文件并将其复制到/etc/krb5.keytab：

**kadmin-q“ktadd-k keytab.kdc01 host/kdc01.example.com”sudo mv keytab.kdc01/etc/krb5.keytab**

在提取Keytab之前，确保kdc01.example.com有一个主机。

10.      使用kprop实用程序将数据库推送到辅助KDC：

**sudo kprop-r EXAMPLE.COM-f/var/lib/krb5kdc/dump kdc02.EXAMPLE.COM**

如果传播有效，则应该有一条成功消息。如果有错误消息，请检查辅助KDC上的/var/log/syslog以了解更多信息。

您可能还希望创建一个cron作业来定期更新辅助KDC上的数据库。例如，以下内容将每小时推送一次数据库（请注意，为了适合此文档的格式，长行已被拆分）：

#m h dom mon dow命令

0\*\*\*\*/usr/sbin/kdb5\_util dump/var/lib/krb5kdc/dump&

/usr/sbin/kprop-r EXAMPLE.COM-f/var/lib/krb5kdc/dump kdc02.EXAMPLE.COM

11.      回到辅助KDC上，创建一个存储文件以保存Kerberos主密钥：

**sudo kdb5\_util储藏**

12.      最后，在辅助kdc上启动krb5 kdc守护程序：

**sudo systemctl启动krb5-kdc.service**

辅助KDC现在应该能够为该领域颁发票证。您可以通过停止主kdc上的krb5 kdc守护进程，然后使用kinit请求票证来测试这一点。如果一切顺利，您应该会收到来自二级KDC的罚单。否则，请检查辅助KDC中的/var/log/syslog和/var/log/auth.log。

#### 3.4. Kerberos Linux客户端

本节介绍如何将Linux系统配置为Kerberos客户端。一旦用户成功登录系统，这将允许访问任何kerberized服务。

##### 3.4.1. 安装

为了对Kerberos领域进行身份验证，需要krb5用户和libpam-krb5包，以及其他一些严格来说不需要的包，但这些包会使工作更轻松。要安装软件包，请在终端提示符中输入以下内容：**sudo apt安装krb5用户libpam-krb5 libpam身份验证客户端配置**

auth client config包允许对PAM进行简单配置，以便从多个源进行身份验证，libpam ccred将缓存身份验证凭据，以便在密钥分发中心（KDC）不可用时登录。该软件包也适用于在公司网络上使用Kerberos进行身份验证，但也需要在网络外访问的笔记本电脑。

##### 3.4.2. 配置

要在终端中配置客户端，请输入：

**sudo dpkg重新配置krb5配置**

然后将提示您输入Kerberos领域的名称。此外，如果您没有使用Kerberos SRV记录配置DNS，菜单将提示您输入密钥分发中心（KDC）和领域管理服务器的主机名。

dpkg重新配置会为您的领域向/etc/krb5.conf文件添加条目。您应该有类似于以下内容的条目：

[默认值]

默认\u realm=EXAMPLE.COM。。。

[realms]EXAMPLE.COM={kdc=192.168.0.1 admin\_server=192.168.0.1}

如果将每个经过网络身份验证的用户的uid设置为从5000开始，如中所建议

*第3.2.1节，“安装”[第147页]*，然后您可以告诉pam仅尝试使用uid>5000的Kerberos用户进行身份验证：

**#Kerberos应该只应用于ldap/Kerberos用户，而不是本地用户。用于公共身份验证公共会话公共帐户公共密码；做sudo sed-i-r \-e&apos;s/pam\_krb5.so minimum\_uid=1000/pam\_krb5.so minimum\_uid=5000/&apos;\/etc/pam.d/$i done**

这将避免在使用passwd更改本地身份验证用户的密码时要求其提供（不存在）Kerberos密码。

您可以通过使用kinit实用程序请求票证来测试配置。例如：

**基尼特steve@EXAMPLE.COM** 密码steve@EXAMPLE.COM:

授予票证后，可使用klist查看详细信息：

**克莱斯特**票证缓存：文件：/tmp/krb5cc\_1000

默认委托人：steve@EXAMPLE.COM

有效启动到期服务负责人07/24/08 05:18:56 07/24/08 15:18:56 krbtgt/示例。COM@EXAMPLE.COM续订至07/25/08 05:18:57

Kerberos 4票证缓存：/tmp/tkt1000 klist:您没有缓存的票证

接下来，使用auth client config配置libpam-krb5模块，以便在登录期间请求票证：**sudo auth客户端配置-a-p kerberos\u示例**

您现在将在成功登录验证后收到一张票据。

#### 3.5. 资源

•有关MIT Kerberos版本的更多信息，请参阅MIT Kerberos[149]网站。

•Ubuntu Wiki Kerberos[150]页面有更多详细信息。

•O&apos;Reilly的Kerberos：在设置Kerberos时，《权威指南》[151]是一个很好的参考。

•此外，如果您有kerberos问题，请随时访问Freenode上的#ubuntu服务器和#kerberos IRC频道[152]。

## 4.Kerberos和LDAP

大多数人不会单独使用Kerberos；一旦一个用户通过身份验证（Kerberos），我们需要弄清楚这个用户可以做什么（授权）。这将是LDAP等程序的工作。

在两台服务器之间复制Kerberos主体数据库可能会很复杂，并且会向网络中添加额外的用户数据库。幸运的是，可以将MIT Kerberos配置为使用LDAP目录作为主体数据库。本节介绍如何配置主kerberos服务器和辅助kerberos服务器，以便对主体数据库使用OpenLDAP。

这里给出的示例假设MIT Kerberos和OpenLDAP。

#### 4.1. 配置OpenLDAP

首先，需要在OpenLDAP服务器上加载必要的模式，该服务器具有到主KDC和辅助KDC的网络连接。本节的其余部分假设您还配置了至少两台服务器之间的LDAP复制。有关设置OpenLDAP的信息，请参阅第1节“OpenLDAP服务器”[p.115]。

还需要为TLS和SSL连接配置OpenLDAP，以便对KDC和LDAP服务器之间的通信进行加密。详见第1.8节“TLS”[p.129]。

cn=admin，cn=config是我们创建的具有编辑ldap数据库权限的用户。很多时候它是根DN。更改其值以反映您的设置。

•要将模式加载到LDAP中，请在LDAP服务器上安装krb5 kdc LDAP包。从终端输入：

**sudo apt安装krb5 kdc ldap**

•接下来，提取kerberos.schema.gz文件：

**sudo gzip-d/usr/share/doc/krb5 kdc ldap/kerberos.schema.gz sudo cp/usr/share/doc/krb5 kdc ldap/kerberos.schema/etc/ldap/schema/**

•需要将kerberos模式添加到cn=config树中。第1.4节“修改slapd配置数据库”[p.120]中还详细介绍了向slapd添加新模式的过程。

1.         首先，创建一个名为schema\_convert.conf或类似描述性名称的配置文件，其中包含以下行：

include/etc/ldap/schema/core.schema include/etc/ldap/schema/corba.schema include/etc/ldap/schema/cosine.schema include/etc/ldap/schema/duaconf.schema include/etc/ldap/schema/dyngroup.schema include/etc/ldap/schema/inetorgperson.schema include/etc/ldap/schema/java.schema include/etc/ldap/schema/misc.schema include/etc/ldap/schema/nis.schema include/etc/ldap/schema/openldap.schema include/etc/ldap/schema/ppolicy.schema include/etc/ldap/schema/kerberos.schema

2.         创建一个临时目录以保存LDIF文件：**mkdir/tmp/ldif\_输出**

3.         现在使用slapcat转换模式文件：

**slapcat-f schema\_convert.conf-f/tmp/ldif\_output-n0-s \“cn={12}kerberos，cn=schema，cn=config”>/tmp/cn=kerberos.ldif**

如果上述文件名和路径名不同，请更改它们以匹配您自己的文件名和路径名。

4.         编辑生成的/tmp/cn\=kerberos.ldif文件，更改以下属性：

dn:cn=kerberos，cn=schema，cn=config。。。cn:kerberos

并从文件末尾删除以下行：

StructureObjectClass:olcSchemaConfig entryUUID:18ccd010-746b-102d-9fbe-3760cca765dc创建者姓名：cn=config createTimestamp:20090111203515Z

entryCSN:20090111203515.326445Z#000000#000#000000修饰符名称：cn=config modifyTimestamp:20090111203515Z

属性值会有所不同，只需确保属性已删除即可。

5.         使用ldapadd加载新架构：**sudo ldapadd-Q-Y EXTERNAL-H ldapi://-f/tmp/cn\=kerberos.ldif**

6.         为krb5principalname属性添加索引：

**sudo ldapmodify-Q-Y外部-H ldapi:///**

**dn:olcDatabase={1}mdb，cn=config add:olcDbIndex**

**olcDbIndex:krbPrincipalName eq、pres、sub**

正在修改条目“olcDatabase={1}mdb，cn=config”

7.         最后，更新访问控制列表（ACL）：

**sudo ldapmodify-Q-Y外部-H ldapi:///**

**dn:olcDatabase={1}mdb，cn=config replace:olcAccess**

**olcAccess:to attrs=userPassword，shadowLastChange，krbPrincipalKey by dn=“cn=admin，dc=example，dc=com”由匿名身份验证自行编写\*无添加：olcAccess**

**olcAccess:to dn.base=”“by\*读取添加：olcAccess**

**olcacaccess:to\*by dn=“cn=admin，dc=example，dc=com”write by\*read**

正在修改条目“olcDatabase={1}mdb，cn=config”

就这样，您的LDAP目录现在可以用作Kerberos主体数据库了。

#### 4.2. 主KDC配置

配置了OpenLDAP之后，就可以配置KDC了首先，安装必要的软件包，从终端输入：**sudo apt安装krb5 kdc krb5管理服务器krb5 kdc ldap**

•现在编辑/etc/krb5.conf，在相应部分下添加以下选项：

[默认值]

默认\u realm=EXAMPLE.COM。。。

[realms]EXAMPLE.COM={

kdc=kdc01.example.com kdc=kdc02.example.com admin\_server=kdc01.example.com admin\_server=kdc02.example.com default\_domain=example.com database\_module=openldap\_ldapconf}。。。

[domain\u realm]

.example.com=example.com

...

[数据库默认值]

ldap\u kerberos\u container\u dn=cn=krbContainer，dc=example，dc=com

[dbmodules]

openldap\_ldapconf={db\_library=kldap

ldap\_kdc\_dn=“cn=admin，dc=example，dc=com”

#此对象需要对#领域容器、主体容器和领域子树ldap\_kadmind\_dn=“cn=admin，dc=example，dc=com”具有读取权限

#此对象需要在#领域容器、主体容器和领域子树ldap\_服务\_密码\_文件=/etc/krb5kdc/service.keyfile ldap\_服务器=ldaps://ldap01.example.com ldaps://ldap02.example.com ldap\_conns\_per\_server=5}

将example.com、dc=example、dc=com、cn=admin、dc=example、dc=com和ldap01.example.com更改为适合您网络的域、LDAP对象和LDAP服务器。

•接下来，使用kdb5\_ldap\_util实用程序创建领域：

**sudo kdb5\_ldap\_util-D cn=admin，dc=example，dc=com创建-子树\dc=example，dc=com-r example.com-s-Hldap://ldap01.example.com**

•创建用于绑定到LDAP服务器的密码的存储。此密码由/etc/krb5.conf中的ldap\_kdc\_dn和ldap\_kadmin\_dn选项使用：

**sudo kdb5\_ldap\_util-D cn=admin，dc=example，dc=com statshsrvpw-f\/etc/krb5kdc/service.keyfile cn=admin，dc=example，dc=com**

•从LDAP服务器复制CA证书：

**scp ldap01:/etc/ssl/certs/cacert.pem。sudo cp cacert.pem/etc/ssl/certs**

并编辑/etc/ldap/ldap.conf以使用证书：

TLS\_CACERT/etc/ssl/certs/CACERT.pem

还需要将证书复制到辅助KDC，以允许使用LDAP连接到LDAP服务器。

•启动Kerberos KDC和管理服务器：**sudo systemctl启动krb5-kdc.service**

**sudo systemctl启动krb5-admin-server.service**

现在，您可以将Kerberos主体添加到LDAP数据库中，它们将被复制到为复制配置的任何其他LDAP服务器。要使用kadmin.local实用程序添加主体，请输入：

**sudo kadmin.local**作为主根进行身份验证/admin@EXAMPLE.COM使用密码。

kadmin.local:addprinc-x dn=“uid=steve，ou=people，dc=example，dc=com”史蒂夫警告：没有为steve@EXAMPLE.COM; 默认为无策略为主体输入密码“steve@EXAMPLE.COM":

重新输入主体的密码“steve@EXAMPLE.COM":

“校长”steve@EXAMPLE.COM“创建。

现在应该有krbPrincipalName、krbPrincipalKey、krbLastPwdChange和krbExtraData属性添加到uid=steve、ou=people、dc=example、dc=com用户对象中。使用kinit和klist实用程序测试用户是否确实获得了票证。

如果已创建用户对象，则需要-x dn=“…”选项来添加Kerberos属性。

否则，将在领域子树中创建一个新的主体对象。

#### 4.3. 辅助KDC配置

使用LDAP后端配置辅助KDC类似于使用普通Kerberos数据库配置辅助KDC。

1.         首先，安装必要的软件包。在终端中输入：

**sudo apt安装krb5 kdc krb5管理服务器krb5 kdc ldap**

2.         接下来，编辑/etc/krb5.conf以使用LDAP后端：

[默认值]

默认\u realm=EXAMPLE.COM。。。

[realms]EXAMPLE.COM={

kdc=kdc01.example.com kdc=kdc02.example.com admin\_server=kdc01.example.com admin\_server=kdc02.example.com default\_domain=example.com database\_module=openldap\_ldapconf}。。。

[domain\u realm].example.com=example.com。。。

[数据库默认值]

ldap\u kerberos\u容器\u dn=dc=example，dc=com

[dbmodules]

openldap\_ldapconf={db\_library=kldap

ldap\_kdc\_dn=“cn=admin，dc=example，dc=com”

#此对象需要对#领域容器、主体容器和领域子树ldap\_kadmind\_dn=“cn=admin，dc=example，dc=com”具有读取权限

#此对象需要在#领域容器、主体容器和领域子树ldap\_服务\_密码\_文件=/etc/krb5kdc/service.keyfile ldap\_服务器=ldaps://ldap01.example.com ldaps://ldap02.example.com ldap\_conns\_per\_server=5}

3.         为LDAP绑定密码创建隐藏：

**sudo kdb5\_ldap\_util-D cn=admin，dc=example，dc=com statshsrvpw-f\/etc/krb5kdc/service.keyfile cn=admin，dc=example，dc=com**

4.         现在，在主KDC上，将/etc/krb5kdc/.k5.EXAMPLE.COM主密钥存储复制到辅助KDC。请确保通过加密连接（如scp）或物理介质复制文件。

**sudo scp/etc/krb5kdc/.k5.EXAMPLE.COMsteve@kdc02.example.com：~sudo mv.k5.EXAMPLE.COM/etc/krb5kdc/**

同样，将EXAMPLE.COM替换为您的实际领域。

5.         回到辅助KDC上，（重新）仅启动ldap服务器，

**sudo systemctl重新启动slapd.service**

6.         最后，启动krb5 kdc守护进程：

**sudo systemctl启动krb5-kdc.service**

7.         验证两个ldap服务器（扩展为kerberos）是否同步。

现在，您的网络上有了冗余的KDC，如果一台LDAP服务器、一台Kerberos服务器或一台LDAP和一台Kerberos服务器不可用，使用冗余的LDAP服务器，您应该能够继续对用户进行身份验证。

#### 4.4. 资源

•Kerberos管理指南[153]有一些额外的细节。

•有关kdb5\_ldap\_util的更多信息，请参见第5.6节[154]和kdb5\_ldap\_util手册[155]。

•另一个有用的链接是krb5.conf手册页[156]。

•另外，请参见Kerberos和LDAP[157]Ubuntu wiki页面。

## 5.SSSD和Active Directory

本节介绍如何使用sssd通过sssd的“ad”提供程序根据Active Directory验证用户登录。在以前版本的sssd中，可以使用“ldap”提供程序进行身份验证。但是，在针对Microsoft Windows AD域控制器进行身份验证时，通常需要在域控制器上安装POSIX AD扩展。“ad”提供程序简化了配置，不需要修改ad结构。

#### 5.1. 先决条件、假设和要求

•本指南不解释Active Directory、其工作原理、如何设置或如何维护。它可能不会为您的环境提供“最佳实践”。

•本指南假设已经配置了一个工作的Active Directory域。

•域控制器充当域的权威DNS服务器。

•域控制器是/etc/resolv.conf中指定的主DNS解析程序。

•适当的\_kerberos、\_ldap、\_kpasswd等条目在DNS区域中配置（有关外部链接，请参阅参考资料部分）。

•在域控制器上同步系统时间（Kerberos所必需）。

•本例中使用的域是myubuntu.example.com。

#### 5.2. 软件安装

需要以下包：krb5 user、samba、sssd和chrony。即使系统没有导出共享，也需要安装Samba。此步骤需要Kerberos领域和域控制器的FQDN或IP。

现在安装这些软件包。**sudo apt安装krb5用户samba sssd chrony**

有关krb5用户postinstall脚本提出的问题的答案，请参见下一节。

#### 5.3. Kerberos配置

krb5用户的安装将提示输入域名（大写）、kdc服务器（即域控制器）和管理服务器（本例中也是域控制器）。这将写入

/etc/krb5.conf中的[realm]和[domain\_realm]部分。如果域自动发现正在工作，则可能不需要这些部分。如果不是，那么两者都是必要的。

如果域是myubuntu.example.com，则输入域为myubuntu.example.com

（可选）使用一些附加设置编辑/etc/krb5.conf以指定Kerberos票证生存期（这些值可以安全地用作默认值）：

[默认值]

默认\u realm=MYUBUNTU.EXAMPLE.COM票证\u生命周期=24小时#续费\u生命周期=7d

如果未指定默认\u领域，则可能需要使用“登录”username@domain而不是“用户名”。

Active Directory成员上的系统时间需要与域控制器的系统时间一致，否则Kerberos身份验证可能会失败。理想情况下，域控制器服务器本身将提供NTP服务。

编辑/etc/chrony/chrony.conf:server dc.myubuntu.example.com

#### 5.4. Samba配置

Samba将用于执行与Active Directory身份验证相关的netbios/nmbd服务，即使没有导出文件共享。编辑文件/etc/samba/smb.conf并将以下内容添加到[global]部分：

[全球]

workgroup=MYUBUNTU client signing=yes client use spnego=yes kerberos method=secrets and keytab realm=MYUBUNTU.EXAMPLE.COM security=ads

一些指南指定应指定“密码服务器”并指向域控制器。仅当DNS未正确设置以查找DC时，才有必要执行此操作。默认情况下，如果使用“security=ads”指定“passwordserver”，Samba将显示警告。

#### 5.5. SSSD配置

sssd包中没有包含/etc/sssd/sssd.conf的默认/示例配置文件。有必要创建一个。这是一个最小的工作配置文件：

[sssd]services=nss，pam config\u file\u version=2 domains=MYUBUNTU.EXAMPLE.COM

[domain/MYUBUNTU.EXAMPLE.COM]id\u provider=ad access\u provider=ad

#如果用户登录到/.\此示例将/home/DOMAIN-FQDN/user指定为$home。与pam\_mkhomedir.so一起使用override\_homedir=/home/%d/%u

#如果客户端计算机主机名与DC上的计算机对象不匹配，请取消注释。

#ad\_hostname=mymachine.myubuntu.example.com

#如果DNS SRV解析不起作用，则取消注释

#ad\_server=dc.mydomain.example.com

#如果AD域的命名与Samba域不同，则取消注释

#ad\_domain=MYUBUNTU.EXAMPLE.COM

#出于性能原因，不鼓励枚举。

#枚举=真

保存此文件后，将所有权设置为root，文件权限设置为600：

**sudo chown root:root/etc/sssd/sssd.conf**

**sudo chmod 600/etc/sssd/sssd.conf**

如果所有权或权限不正确，sssd将拒绝启动。

#### 5.6. 验证nsswitch.conf配置

sssd包的安装后脚本会自动对/etc/nsswitch.conf进行一些修改。它应该是这样的：

密码：compat sss组：compat sss。。。

网络组：nis sss用户：文件sss

#### 5.7. 修改/etc/hosts

将别名添加到/etc/hosts中指定FQDN的localhost条目中。例如：

192.168.1.10 myserver myserver.myubuntu.example.com这与动态DNS更新结合使用非常有用。

#### 5.8. 加入Active Directory

现在，重新启动chrony和samba并启动sssd。

**sudo systemctl restart chrony.service sudo systemctl restart smbd.service nmbd.service**sudo systemctl启动sssd.service

通过获取Kerberos票证来测试配置：**sudokinit管理员**

通过以下方式验证票据：**sudo-klist**

如果已列出过期日期的票证，则是加入域的时候了：

**sudo网络广告加入-k**

关于“未配置DNS域。无法执行DNS更新”的警告。可能意味着/etc/hosts中没有（正确的）别名，并且系统无法提供自己的FQDN作为Active Directory更新的一部分。这是动态DNS更新所必需的。验证上面“Modify/etc/hosts”中描述的/etc/hosts中的别名。

（消息“NT\_STATUS\_UNSUCCESSFUL”表示域加入失败，并且某些内容不正确。请查看前面的步骤，然后继续）。

下面是几个（可选）检查，以验证域加入是否成功。请注意，如果域已成功加入，但其中一个或两个步骤均失败，则可能需要等待1-2分钟，然后重试。有些更改似乎是异步的。

验证选项#1：

检查Active Directory中计算机帐户的默认组织单位，以验证计算机帐户是否已创建。（Active Directory中的组织单位是本指南范围之外的主题）。

验证选项#2

为特定广告用户（如管理员）执行此命令

**getent密码用户名**

如果在sssd.conf中设置了enumerate=true，则不带username参数的getent passwd将列出所有域用户。这可能对测试有用，但速度较慢，不建议用于生产。

#### 5.9. 测试认证

现在应该可以使用Active Directory用户的凭据进行身份验证：**su-用户名**

如果这样做有效，那么其他登录方法（getty、ssh）也应该有效。

如果创建了计算机帐户，表明系统已“加入”到域，但身份验证未成功，则查看/etc/pam.d和nssswitch.conf以及本指南前面描述的文件更改可能会有所帮助。

#### 5.10[158]. 带有pam\_mkhomedir的主目录（可选）

使用Active Directory用户帐户登录时，用户可能没有主目录。这可以通过pam\_mkdhomedir.so修复，它将在登录时创建用户的主目录。编辑/etc/pam.d/common session，并将此行直接添加到session required pam\_unix.so:session required pam\_mkhomedir.so skel=/etc/skel/umask=0022之后

这可能还需要覆盖sssd.conf中的\u homedir才能正常工作，因此请确保已设置。

#### 5.11. 桌面Ubuntu身份验证

也可以使用Active Directory帐户验证Ubuntu桌面的登录。广告帐户不会显示在本地用户的选择列表中，因此需要修改lightdm。编辑文件/etc/

lightdm/lightdm.conf.d/50-unity-greeter.conf并附加以下两行：

迎宾员显示手动登录=真迎宾员隐藏用户=真

重新启动以重新启动lightdm。现在应该可以使用用户名或用户名使用域帐户登录/username@domain总体安排

#### 5.12. 资源

•GitHub SSSD项目62

•Active Directory DNS区域条目[159]•Kerberos配置选项[160]

# 第八章。域名服务（DNS）

域名服务（DNS）是一种将IP地址和完全限定域名（FQDN）相互映射的Internet服务。通过这种方式，DNS减轻了记住IP地址的需要。运行DNS的计算机称为名称服务器。Ubuntu附带BIND（Berkley Internet命名守护程序），这是在Linux上维护名称服务器最常用的程序。

## 1.安装

在终端提示下，输入以下命令以安装dns：**sudoapt安装bind9**

dnsutils包是测试和排除DNS问题的一个非常有用的包。通常这些工具已经安装，但要检查和/或安装dnsutils，请输入以下内容：

**sudo apt安装dnsutils**

## 2.配置

有很多方法可以配置BIND9。一些最常见的配置包括缓存名称服务器、主主机和辅助主机。

•当配置为缓存名称服务器时，BIND9将找到名称查询的答案，并在再次查询域时记住答案。

•作为主服务器，BIND9从其主机上的文件读取区域数据，并对该区域具有权威性。

•在辅助主配置中，BIND9从另一个具有区域权威的名称服务器获取区域数据。

#### 2.1. 概述

DNS配置文件存储在/etc/bind目录中。主要配置文件是/etc/bind/named.conf。

include行指定包含DNS选项的文件名。/etc/bind/named.conf.options文件中的目录行告诉DNS在哪里查找文件。绑定使用的所有文件都将与此目录相关。

名为/etc/bind/db.root的文件描述了世界上的根名称服务器。服务器会随着时间的推移而变化，因此必须不时维护/etc/bind/db.root文件。这通常作为对bind9包的更新来完成。区域部分定义了一个主服务器，它存储在文件选项中提到的文件中。

可以将同一服务器配置为缓存名称服务器、主主机和辅助主机。服务器可以是一个区域的授权起点（SOA），同时为另一个区域提供辅助服务。始终为本地LAN上的主机提供缓存服务。

#### 2.2. 缓存名称服务器

默认配置设置为充当缓存服务器。只需添加ISP DNS服务器的IP地址即可。只需在/etc/bind/named.conf.options中取消注释并编辑以下内容：

货代{1.2.3.4；

5.6.7.8;

};

用实际名称服务器的IP地址替换1.2.3.4和5.6.7.8。

现在重新启动DNS服务器，以启用新配置。从终端提示符：

**sudo systemctl重启bind9.service**

有关测试缓存DNS服务器的信息，请参见第3.1.2节“挖掘”[p.174]。

#### 2.3. 主控

在本节中，BIND9将被配置为域example.com的主控主机。只需将example.com替换为FQDN（完全限定域名）。

##### 2.3.1. 转发区域文件

要向BIND9添加DNS区域，将BIND9转换为主主服务器，第一步是编辑/etc/bind/named.conf.local：

区域“example.com”{type master；

文件“/etc/bind/db.example.com”；}；

（注意，如果bind将接收到与DDNS一样的文件自动更新，则在此处和下面的copy命令中使用/var/lib/bind/db.example.com而不是/etc/bind/db.example.com。）现在使用现有区域文件作为模板创建/etc/bind/db.example.com文件：**sudo cp/etc/bind/db.local/etc/bind/db.example.com**

编辑新区域文件/etc/bind/db.example.com更改localhost。添加到服务器的FQDN，并在末尾保留附加的“.”。将127.0.0.1更改为名称服务器的IP地址，将root.localhost更改为有效的电子邮件地址，但使用“.”而不是通常的“@”符号，最后再次保留“.”。更改注释以指示此文件所针对的域。

为基本域（example.com）创建A记录。另外，为ns.example.com（本例中的名称服务器）创建一个A记录：

; ; 绑定example.com的数据文件

;

TTL 604800美元

@在SOA example.com中。root.example.com。(

2.序列号

604800；刷新

86400；重试

2419200；到期日604800）；192.168.1.10中的负缓存TTL

; @ 在NS.example.com中。

@在192.168.1.10中

@在AAAA中：192.168.1.10中的1 ns

每次更改区域文件时，必须增加序列号。如果在重新启动BIND9之前进行了多次更改，只需将序列号增加一次。

现在，您可以将DNS记录添加到区域文件的底部。详见第4.1节“通用记录类型”[p.178]。

许多管理员喜欢使用最后编辑的日期作为区域的序列号，例如2012010100，它是yyyymmddss（其中ss是序列号）

对区域文件进行更改后，需要重新启动BIND9以使更改生效：**sudo systemctl重启bind9.service**

##### 2.3.2. 反向区域文件

现在区域已经设置好，并且将名称解析为IP地址，还需要一个反向区域。反向区域允许DNS将地址解析为名称。

编辑/etc/bind/named.conf.local并添加以下内容：

区域“1.168.192.in addr.arpa”{type master；file”/etc/bind/db.192；}；

将1.168.192替换为您正在使用的任何网络的前三个八位字节。另外，将区域文件命名为/etc/bind/db.192。它应该匹配网络的第一个八位组。

现在创建/etc/bind/db.192文件：**sudo cp/etc/bind/db.127/etc/bind/db.192**

接下来编辑/etc/bind/db.192，更改与/etc/bind/db.example.com基本相同的选项：

; ; 为本地192.168.1.XXX网络绑定反向数据文件

;

TTL 604800美元

@在SOA ns.example.com中。root.example.com。(

2.序列号

604800；刷新

86400；重试

2419200；到期日604800）；负缓存TTL

;

@在NS中。

10在PTR ns.example.com。

反向区域中的序列号也需要在每次更改时递增。对于在/etc/bind/db.example.com中配置的每个A记录，即不同地址的A记录，您需要在/etc/bind/db.192中创建一个PTR记录。

创建反向区域文件后，请重新启动BIND9：**sudo systemctl重启bind9.service**

#### 2.4. 中学校长

配置主主机后，需要一个辅助主机，以便在主主机不可用时保持域的可用性。

首先，在主主服务器上，需要允许区域传输。将“允许传输”选项添加到/etc/bind/named.conf.local中的正向和反向区域定义示例中：

区域“example.com”{type master；file”/etc/bind/db.example.com”；允许传输{192.168.1.11；}；}；

区域“1.168.192.in addr.arpa”{type master；file”/etc/bind/db.192；允许传输{192.168.1.11；}；}；

将192.168.1.11替换为辅助名称服务器的IP地址。

在主主机上重新启动BIND9：**sudo systemctl重启bind9.service**

接下来，在辅助主机上，以与主主机相同的方式安装bind9包。然后编辑/etc/bind/named.conf.local并为正向和反向区域添加以下声明：

区域“example.com”{type slave；

文件“db.example.com”；masters{192.168.1.10；}；}；}；

分区“1.168.192地址arpa”{

输入slave；文件“db.192”；masters{192.168.1.10；}；}；}；

用主名称服务器的IP地址替换192.168.1.10。

在辅助主机上重新启动BIND9：**sudo systemctl重启bind9.service**

在/var/log/syslog中，您应该看到类似的内容（一些行已拆分以适合本文档的格式）：

客户端192.168.1.10#39448:已收到区域“1.168.192.in addr.arpa”区域1.168.192.in-addr.arpa/in的通知：传输已开始。从192.168.1.10#53转移&apos;100.18.172.地址arpa/in&apos;：

使用192.168.1.11#37531连接

区域1.168.192.in-addr.arpa/in：从192.168.1.10#53传输“100.18.172.in-addr.arpa/in”的串行5传输：传输完成：1条消息，6条记录，212字节，0.002秒（106000字节/秒）区域1.168.192.in-addr.arpa/in：发送通知（串行5）

客户端192.168.1.10#20329:已收到“example.com”区域example.com/IN的通知：传输已开始。从192.168.1.10#53传输&apos;example.com/IN&apos;：使用192.168.1.11连接#38577 zone example.com/IN:传输串行5

从192.168.1.10#53传输&apos;example.com/IN&apos;：传输完成：1条消息，8条记录，225字节，0.002秒（112500字节/秒）

注意：仅当主设备上的序列号大于辅助设备上的序列号时，才会传输区域。如果您想让主DNS通知辅助DNS服务器区域更改，还可以添加notify{ipaddress；}；在to/etc/bind/named.conf.local中，如下例所示：

区域“example.com”{type master；

文件“/etc/bind/db.example.com”；允许传输{192.168.1.11；}；同时通知{192.168.1.11；}；}；

区域“1.168.192.in addr.arpa”{type master；file”/etc/bind/db.192；允许传输{192.168.1.11；}；也通知{192.168.1.11；}；}；

非权威区域文件的默认目录是/var/cache/bind/。此目录也在AppArmor中配置为允许指定的守护进程向其写入。有关AppArmor的更多信息，请参见第4节“AppArmor”[p.194]。

## 3.故障排除

本节介绍在DNS和BIND9出现问题时帮助确定原因的方法。

#### 3.1. 测试

##### 3.1.1. 决议

测试BIND9的第一步是将名称服务器的IP地址添加到主机解析程序。应将主名称服务器与另一台主机配置为双重检查。有关向网络客户端添加名称服务器地址的详细信息，请参阅第1.3.1节“DNS客户端配置”[p.44]，然后检查文件/etc/resolv.conf是否包含（对于本例）：

名称服务器192.168.1.10名称服务器192.168.1.11

在127.\*侦听的名称服务器负责将自己的IP地址添加到resolv.conf（使用resolvconf）。通过文件/etc/default/bind9将RESOLVCONF=no行更改为

RESOLVCONF=是。

还应添加辅助名称服务器的IP地址，以防主名称服务器不可用。3.1.2. 挖掘

如果安装了dnsutils软件包，则可以使用DNS查找实用程序测试设置：

•安装BIND9后，使用环回接口的dig，确保它正在监听端口53。从终端提示符：**dig-X127.0.0.1**

您应该在命令输出中看到类似于以下内容的行：

;; 查询时间：1毫秒

;; 服务器：192.168.1.10#53（192.168.1.10）

•如果您已将BIND9配置为缓存名称服务器“挖掘”外部域以检查查询时间：**挖掘ubuntu.com**

请注意命令输出结束时的查询时间：

;; 查询时间：49毫秒

第二次挖掘后，应进行改进：

;; 查询时间：1毫秒

##### 3.1.3. 发出砰的声响

现在演示应用程序如何使用DNS解析主机名，使用ping实用程序发送ICMP回显请求。在终端提示中输入：**pingexample.com**

这将测试名称服务器是否可以将名称ns.example.com解析为IP地址。命令输出应类似于：

PING ns.example.com（192.168.1.10）56（84）字节的数据。

192.168.1.10中的64字节：icmp\_seq=1 ttl=64时间=0.800毫秒192.168.1.10中的64字节：icmp\_seq=2 ttl=64时间=0.813毫秒

##### 3.1.4. 命名检查区

测试区域文件的一个好方法是使用与bind9包一起安装的命名checkzone实用程序。此实用程序允许您在重新启动BIND9并使更改生效之前确保配置正确。

•要测试示例转发区域文件，请在命令提示符下输入以下内容：**命名为checkzone example.com/etc/bind/db.example.com**

如果所有配置都正确，您将看到类似以下内容的输出：

zone example.com/IN:加载的串行6正常

•同样，要测试反向区域文件，请输入以下内容：输出应类似于：**命名为checkzone 1.168.192.in-addr.arpa/etc/bind/db.192**

1.168.192.in-addr.arpa/in区：加载的串行3正常

区域文件的序列号可能不同。

#### 3.2. 登录中

BIND9有多种可用的日志配置选项。主要有两种选择。通道选项配置日志的去向，类别选项确定要记录的信息。

如果未配置任何日志记录选项，则默认选项为：

伐木{

类别默认值{default\u syslog；默认值{u debug；}；类别不匹配{null；}；}；

本节介绍如何配置BIND9将与DNS查询相关的调试消息发送到单独的文件。

•首先，我们需要配置一个通道，以指定将消息发送到哪个文件。编辑/etc/bind/named.conf.local并添加以下内容：

伐木{

channel query.log{file”/var/log/query.log；严重性调试3；}；

};

•接下来，配置一个类别以将所有DNS查询发送到查询文件：

伐木{

channel query.log{file”/var/log/query.log；严重性调试3；}；

类别查询{query.log；}；}；

注意：调试选项可以设置为1到3。如果未指定级别，则默认为级别1。

•由于指定的守护进程以绑定用户身份运行，因此必须创建/var/log/query.log文件并更改所有权：

**sudo touch/var/log/query.log sudo chown bind/var/log/query.log**

•在命名守护进程写入新日志文件之前，必须更新AppArmor配置文件。首先，编辑/etc/apparmor.d/usr.sbin.named并添加：

/var/log/query.log w，

接下来，重新加载配置文件：**cat/etc/apparmor.d/usr.sbin.named | sudo apparmor\_解析器-r**

有关AppArmor的更多信息，请参见第4节“AppArmor”[p.194]

•现在重新启动BIND9以使更改生效：**sudo systemctl重启bind9.service**

您应该看到文件/var/log/query.log中填充了查询信息。这是一个简单的示例

BIND9日志记录选项。有关高级选项的涵盖范围，请参见第4.2节“更多信息”[p.178]。

## 4.工具书类

#### 4.1. 常见记录类型

本节介绍一些最常见的DNS记录类型。

•记录：此记录将IP地址映射到主机名。www.inta 192.168.1.12*A.*

•记录：用于为现有记录创建别名。无法创建指向另一个CNAME记录的CNAME记录。CNAME www中的web*CNAME*

•记录：用于定义电子邮件应发送到的位置。必须指向A记录，而不是CNAME。*MX*

在MX 1 mail.example.com中。

在192.168.1.13中邮寄

•记录：用于定义哪些服务器提供区域副本。它必须指向A记录，而不是CNAME。这是定义主服务器和辅助服务器的地方。*NS*

在NS.example.com中。在NS ns2.example.com中。

192.168.1.10中的ns 192.168.1.11中的ns2

#### 4.2. 更多信息

•ubuntuwiki中的BIND9服务器HOWTO[161]有很多有用的信息。

•Linux文档项目中的DNS HOWTO[162]也有很多关于配置BIND9的信息。

•Bind9.net[163]链接到大量DNS和Bind9资源。

•DNS和BIND[164]是一本很受欢迎的书，目前已发行第五版。现在还有一本关于IPv6的DNS和绑定的书[165]。

•在freenode上的#Ubuntu服务器IRC频道[166]是一个请求BIND9帮助并参与Ubuntu服务器社区的好地方。

# 第九章。安全

在安装、部署和使用任何类型的计算机系统时，应始终考虑安全性。虽然新安装的Ubuntu在互联网上立即使用相对安全，但基于部署后如何使用它，平衡地了解系统的安全态势是很重要的。

本章概述了与Ubuntu 18.04 LTS Server Edition相关的安全主题，并概述了保护服务器和网络免受任何潜在安全威胁的简单措施。

## 1.用户管理

用户管理是维护安全系统的关键部分。无效的用户和权限管理通常会导致许多系统受损。因此，了解如何通过简单有效的用户帐户管理技术来保护服务器非常重要。

1.1. 根在哪里？

Ubuntu开发人员做出了一个认真的决定，在所有应用程序中默认禁用管理根帐户

Ubuntu安装。这并不意味着根帐户已被删除或无法访问。它只获得了一个与可能的加密值不匹配的密码，因此可能无法自己直接登录。

相反，鼓励用户使用名为sudo的工具来执行系统管理职责。Sudo允许授权用户使用自己的密码临时提升其权限，而不必知道属于根帐户的密码。这种简单而有效的方法为所有用户操作提供了责任，并使管理员能够精确地控制用户可以使用所述权限执行哪些操作。

•如果出于某种原因，您希望启用根帐户，只需给它一个密码：

不支持使用根密码的配置。

**sudopasswd**

Sudo将提示您输入密码，然后要求您为root用户提供新密码，如下所示：

[sudo]用户名密码：（输入您自己的密码）

输入新的UNIX密码：（为root用户输入新密码）重新输入新的UNIX密码：（为root用户重复新密码）passwd:password已成功更新

•要禁用根帐户密码，请使用以下passwd语法：**sudo passwd-l根**

但是，要禁用根帐户本身，请使用以下命令：**usermod—过期日期1**

•您应该通过阅读手册页了解更多关于Sudo的内容：**曼苏多**

默认情况下，Ubuntu安装程序创建的初始用户是组“sudo”的成员，该组作为授权sudo用户添加到文件/etc/sudoers中。如果您希望通过sudo为任何其他帐户提供完全root访问权限，只需将它们添加到sudo组即可。

#### 1.2. 添加和删除用户

管理本地用户和组的过程非常简单，与大多数其他用户和组几乎没有什么不同

GNU/Linux操作系统。Ubuntu和其他基于Debian的发行版鼓励使用“adduser”包进行帐户管理。

•要添加用户帐户，请使用以下语法，并按照提示为帐户提供密码和可识别特征，如全名、电话号码等。**sudo adduser用户名**

•要删除用户帐户及其主要组，请使用以下语法：**sudodeluser用户名**

删除帐户不会删除其各自的主文件夹。由您决定是否手动删除文件夹或根据所需的保留策略保留文件夹。

请记住，如果您没有采取必要的预防措施，则以后添加的任何用户（其UID/GID与以前的所有者相同）现在都可以访问此文件夹。

您可能希望将这些UID/GID值更改为更合适的值，例如根帐户，甚至可能重新定位文件夹以避免将来发生冲突：

**sudo chown-R root:root/home/username/sudo mkdir/home/archived\_users/sudo mv/home/username/home/archived\_users/**

•要临时锁定或解锁用户帐户，请分别使用以下语法：

**sudo passwd-l用户名sudo passwd-u用户名**

•要添加或删除个性化组，请分别使用以下语法：

**sudo addgroup groupname sudo delgroup groupname**

•要将用户添加到组中，请使用以下语法：

**sudo adduser用户名groupname**

#### 1.3. 用户配置文件安全

创建新用户时，adduser实用程序将创建一个名为/home/username的全新主目录。默认概要文件是根据/etc/skel目录中的内容建模的，该目录包含所有概要文件的基础知识。

如果您的服务器将是多个用户的家，则应密切注意用户的主目录权限，以确保机密性。默认情况下，Ubuntu中的用户主目录是使用世界读取/执行权限创建的。这意味着所有用户都可以浏览和访问其他用户主目录的内容。这可能不适合您的环境。

•要验证当前用户主目录权限，请使用以下语法：**ls-ld/home/username**

以下输出显示目录/home/username具有世界可读权限：drwxr-xr-x 2 username username 4096 2007-10-02 20:03 username

•您可以使用以下语法删除全球可读权限：**sudo chmod 0750/home/username**

有些人倾向于不加区别地使用递归选项（-R），它会修改所有子文件夹和文件，但这不是必需的，并且可能会产生其他不希望的结果。仅父目录就足以防止未经授权访问父目录下的任何内容。

更有效的方法是在创建用户主文件夹时修改adduser全局默认权限。只需编辑文件/etc/adduser.conf并将DIR\_MODE变量修改为适当的值，这样所有新的主目录都将获得正确的权限。

DIR\_模式=0750

•使用上述任何技术更正目录权限后，使用以下语法验证结果：**ls-ld/home/username**

下面的结果显示世界可读权限已被删除：drwxr-x---2用户名用户名4096 2007-10-02 20:03用户名

#### 1.4. 密码策略

强大的密码策略是安全态势的最重要方面之一。许多成功的安全漏洞涉及针对弱密码的简单暴力和字典攻击。如果您打算提供涉及本地密码系统的任何形式的远程访问，请确保充分满足最低密码复杂性要求、最长密码生存期以及对身份验证系统的频繁审核。

##### 1.4.1. 最小密码长度

默认情况下，Ubuntu需要至少6个字符的密码长度，以及一些基本的熵检查。这些值在文件/etc/pam.d/common-password中控制，如下所述。密码[success=1 default=ignore]pam\_unix.so

如果要将最小长度调整为8个字符，请将相应的变量更改为min=8。修改概述如下。密码[success=1 default=ignore]pam\_unix.so minlen=8

基本密码熵检查和最小长度规则不适用于使用sudo级别命令设置新用户的管理员。

##### 1.4.2. 密码过期

在创建用户帐户时，您应该制定一项策略，规定密码的最短期限和最长期限，强制用户在密码过期时更改密码。

•要轻松查看用户帐户的当前状态，请使用以下语法：**sudo chage-l用户名**

下面的输出显示了有关用户帐户的有趣事实，即没有应用任何策略：

上次密码更改：2015年1月20日

密码过期：永不

密码无效：从不

帐户过期：永不过期

更改密码之间的最短间隔天数：0

更改密码之间的最大间隔天数：99999

密码过期前的警告天数：7

•要设置这些值中的任何一个，只需使用以下语法，并按照交互式提示进行操作：**sudochage用户名**

以下示例还说明了如何手动将显式过期日期（-E）更改为2015年1月31日，最小密码期限（-m）更改为5天，最大密码期限（-m）更改为90天，密码过期后的非活动期（-I）更改为30天，以及密码过期前的警告期（-W）更改为14天：

**sudo chage-E 01/31/2015-m 5-m 90-I 30-W 14用户名**

•要验证更改，请使用前面提到的相同语法：**sudo chage-l用户名**

下面的输出显示了为该帐户建立的新策略：

上次密码更改：2015年1月20日

密码过期日期：2015年4月19日

密码无效：2015年5月19日

账户到期日：2015年1月31日

更改密码之间的最短间隔天数：5

更改密码之间的最大间隔天数：90

密码过期前的警告天数：14

#### 1.5. 其他安全考虑

许多应用程序使用备用身份验证机制，即使是有经验的系统管理员也很容易忽略这些机制。因此，了解和控制用户如何进行身份验证以及如何访问服务器上的服务和应用程序非常重要。

##### 1.5.1. 被禁用用户的SSH访问

如果用户以前设置过RSA公钥身份验证，则仅禁用/锁定用户帐户不会阻止用户远程登录到您的服务器。他们仍然能够获得对服务器的shell访问，而不需要任何密码。请记住检查用户主目录中是否有允许这种经过身份验证的SSH访问的文件，例如/home/username/.SSH/authorized\_key。

删除或重命名用户主文件夹中的目录.ssh/，以防止进一步的ssh身份验证功能。

请确保检查被禁用的用户是否建立了任何SSH连接，因为它们可能具有现有的入站或出站连接。杀死所有被发现的人。

**谁| grep用户名**（获取pts/#终端）sudo pkill-f pts/#

仅将SSH访问限制为应具有SSH访问权限的用户帐户。例如，您可以创建一个名为“sshlogin”的组，并将组名添加为与文件/etc/ssh/sshd\_config中的AllowGroups变量关联的值。

AllowGroups sshlogin

然后将允许的SSH用户添加到组“sshlogin”，并重新启动SSH服务。

**sudo adduser用户名sshlogin**

**sudo systemctl重新启动sshd.service**

##### 1.5.2. 外部用户数据库身份验证

大多数企业网络要求对所有系统资源进行集中身份验证和访问控制。如果已将服务器配置为根据外部数据库对用户进行身份验证，请确保在外部和本地禁用用户帐户。这样可以确保不可能进行本地回退身份验证。

## 2.控制台安全

与您为保护服务器而设置的任何其他安全屏障一样，要防范物理访问您的环境的人造成的无法形容的损害（例如，硬盘被盗、电源或服务中断等），是相当困难的。因此，控制台安全应该仅仅作为整体物理安全策略的一个组成部分来解决。锁上的“屏蔽门”可能会阻止偶然犯罪，或者至少会减慢已确定的犯罪速度，因此建议在控制台安全方面采取基本预防措施。

以下说明将有助于保护您的服务器免受可能产生非常严重后果的问题的影响。

#### 2.1. 禁用Ctrl+Alt+Delete

任何具有键盘物理访问权限的人都可以简单地使用Ctrl+Alt+Delete组合键重新启动服务器，而无需登录。虽然有人可以简单地拔下电源，但您仍应防止在生产服务器上使用此组合键。这迫使攻击者采取更严厉的措施重新启动服务器，同时防止意外重新启动。

要禁用按Ctrl+Alt+Delete组合键执行的重新启动操作，请运行以下两个命令：

sudo systemctl掩码ctrl-alt-del.target sudo systemctl后台程序重新加载

## 3.防火墙

#### 3.1. 介绍

Linux内核包括Netfilter子系统，用于操纵或决定进入或通过服务器的网络流量的命运。所有现代Linux防火墙解决方案都使用此系统进行数据包过滤。

如果没有用户空间接口来管理内核的数据包过滤系统，那么它对管理员来说几乎没有用处。这就是iptables的用途：当数据包到达您的服务器时，它将根据用户空间通过iptables提供给它的规则，移交给Netfilter子系统进行接受、操作或拒绝。因此，iptables是管理防火墙所需的全部，如果您熟悉它的话，但是有许多前端可用于简化任务。

#### 3.2. ufw-简单防火墙

Ubuntu的默认防火墙配置工具是ufw。ufw是为简化iptables防火墙配置而开发的，它提供了一种用户友好的方法来创建基于IPv4或IPv6主机的防火墙。默认情况下，ufw最初是禁用的。从ufw手册页：

ufw的目的不是通过其命令界面提供完整的防火墙功能，而是提供一种添加或删除简单规则的简便方法。它目前主要用于基于主机的防火墙

以下是如何使用ufw的一些示例：

•首先，需要启用ufw。在终端提示中输入：**sudoufw启用**

•要打开端口（本例中为SSH）：**sudoufw允许22**

•还可以使用编号格式添加规则：**sudo ufw插件1允许80**

•同样，要关闭打开的端口：**sudo ufw拒绝22**

•要删除规则，请使用删除，然后再使用规则：**sudoufw删除拒绝22**

•还可以允许从特定主机或网络访问端口。以下示例允许SSH从主机192.168.0.2访问此主机上的任何IP地址：

**sudo ufw允许从192.168.0.2到任何端口22的协议tcp**

将192.168.0.2替换为192.168.0.0/24，以允许从整个子网进行SSH访问。

•将--dry run选项添加到ufw命令将输出结果规则，但不会应用它们。例如，如果打开HTTP端口，将应用以下内容：

**sudoufw——允许http干运行**

\*滤器

：ufw用户输入-[0:0]

：ufw用户输出-[0:0]

：ufw用户转发-[0:0]

：ufw用户限制-[0:0]：ufw用户限制接受-[0:0]

###规则###

###元组####允许tcp 80 0.0.0.0/0任何0.0.0.0/0-一个ufw用户输入-p tcp--dport 80-j接受

###结束规则###

-一个ufw用户输入-返回

-一个ufw用户输出-j返回

-ufw用户转发-j返回-A ufw用户限制-m限制--限制3/分钟-j日志--日志前缀“[ufw限制]：”

-ufw用户限制-j拒绝-ufw用户限制接受-j接受

犯罪

规则更新

•可通过以下方式禁用ufw：**sudoufw禁用**

•要查看防火墙状态，请输入：**sudo ufw状态**

•对于更详细的状态信息，请使用：**sudo ufw状态详细**

•要查看编号格式：**sudo ufw状态编号**

如果要打开或关闭的端口是在/etc/services中定义的，则可以使用端口名而不是编号。在上面的示例中，将22替换为ssh。

这是使用ufw的快速介绍。有关更多信息，请参阅ufw手册页。

##### 3.2.1. ufw应用集成

打开端口的应用程序可以包括一个ufw配置文件，其中详细说明了应用程序正常运行所需的端口。配置文件保存在/etc/ufw/applications.d中，如果更改了默认端口，则可以对其进行编辑。

•要查看哪些应用程序安装了配置文件，请在终端中输入以下内容：**sudoufw应用程序列表**

•与允许端口通信类似，使用应用程序配置文件通过输入：**sudoufw允许桑巴舞**

•还提供扩展语法：**ufw允许从192.168.0.0/24到任何Samba应用程序**

用您正在使用的应用程序配置文件和网络的IP范围替换Samba和192.168.0.0/24。

不需要为应用程序指定协议，因为该信息在概要文件中有详细说明。另外，请注意，应用程序名称将替换端口号。

•要查看为应用程序定义的端口、协议等的详细信息，请输入：**sudo ufw应用程序信息Samba**

并非所有需要打开网络端口的应用程序都附带ufw配置文件，但如果您已对应用程序进行了配置文件分析，并希望该文件包含在软件包中，请在Launchpad中针对该软件包提交一个bug。**ubuntu bug包的名称**

#### 3.3. IP伪装

IP伪装的目的是允许网络上具有专用、不可路由IP地址的计算机通过进行伪装的计算机访问Internet。必须对来自专用网络（目的地为Internet）的流量进行操作，以使回复能够路由回发出请求的计算机。要做到这一点，内核必须修改每个数据包的源IP地址，以便将应答路由回它，而不是发送请求的私有IP地址，这在Internet上是不可能的。Linux使用连接跟踪（conntrack）来跟踪哪些连接属于哪些机器，并相应地重新路由每个返回数据包。因此，离开您的专用网络的流量是有限的

“伪装”为源于你的Ubuntu网关机器。此过程在Microsoft文档中称为Internet连接共享。

##### 3.3.1. ufw伪装

IP伪装可以使用自定义ufw规则实现。这是可能的，因为ufw的当前后端是使用位于/etc/ufw/\*.rules中的规则文件进行iptables恢复。这些文件是添加未使用ufw的遗留iptables规则以及与网络网关或网桥更相关的规则的好地方。

这些规则分为两个不同的文件，即应该在ufw命令行规则之前执行的规则和在ufw命令行规则之后执行的规则。

•首先，需要在ufw中启用数据包转发。需要调整两个配置文件，在/etc/default/ufw中将默认转发策略更改为“接受”：

默认转发策略=“接受”

然后编辑/etc/ufw/sysctl.conf并取消注释：net/ipv4/ip\_forward=1

类似地，对于IPv6转发取消注释：net/IPv6/conf/default/forwarding=1

•现在将规则添加到/etc/ufw/before.rules文件中。默认规则仅配置筛选器表，要启用伪装，需要配置nat表。将以下内容添加到文件顶部标题注释之后：

#nat表规则

\*纳特

：发送后接受[0:0]

#将流量从eth1转发到eth0。

-后路由-s192.168.0.0/24-o eth0-j伪装

#不要删除“提交”行，否则将不会处理这些nat表规则

犯罪

这些注释并不是绝对必要的，但记录您的配置被认为是良好的做法。此外，在修改/etc/ufw中的任何规则文件时，请确保这些行是每个修改表的最后一行：

#不要删除“提交”行，否则将不会处理这些规则

犯罪

对于每个表，都需要相应的COMMIT语句。在这些示例中，仅显示nat和筛选器表，但也可以为原始表和mangle表添加规则。

在上面的示例中，将eth0、eth1和192.168.0.0/24替换为适合您网络的适当接口和IP范围。

•最后，禁用并重新启用ufw以应用更改：**sudo ufw disable&&sudo ufw enable**

现在应该启用IP伪装。您还可以向/etc/ufw/before.rules添加任何其他转发规则。建议在前向链之前将这些附加规则添加到ufw中。

3.3.2. iptables伪装iptables还可用于启用伪装。

•与ufw类似，第一步是通过编辑/etc/sysctl.conf并取消注释以下行来启用IPv4数据包转发：net.IPv4.ip\_forward=1

如果希望同时启用IPv6转发，请取消注释：net.IPv6.conf.default.forwarding=1

•接下来，执行sysctl命令以启用配置文件中的新设置：**sudosysctl-p**

•IP伪装现在可以使用单个iptables规则完成，该规则可能会根据您的网络配置略有不同：sudo iptables-t nat-a POSTROUTING-s 192.168.0.0/16-o ppp0-j伪装

上述命令假定您的专用地址空间为192.168.0.0/16，并且您的面向Internet的设备为ppp0。语法细分如下：

•-t nat——规则是进入nat表

•-A后路由——规则将被附加（-A）到后路由链

•-s 192.168.0.0/16——该规则适用于源自指定地址空间的流量

•-o ppp0——该规则适用于计划通过指定网络设备路由的流量

•-j伪装——符合此规则的流量将“跳转”（-j）到要操纵的伪装目标，如上所述

•此外，过滤器表（默认表，以及大多数或所有数据包过滤发生的位置）中的每个链都有默认的接受策略，但如果您在网关设备之外创建防火墙，则可能已将策略设置为删除或拒绝，在这种情况下，您的伪装流量需要通过前向链才能使用上述规则：

sudo iptables-A FORWARD-s 192.168.0.0/16-o ppp0-j ACCEPT sudo iptables-A FORWARD-d 192.168.0.0/16-m state \--状态已建立，相关-i ppp0-j ACCEPT

上述命令将允许从本地网络到Internet的所有连接以及与这些连接相关的所有流量返回到启动这些连接的计算机。

•如果您希望在重新启动时启用伪装，您可能会这样做，请编辑/etc/rc.local并添加上面使用的任何命令。例如，添加没有过滤的第一个命令：iptables-tnat-apostrouting-s192.168.0.0/16-opppp0-j MASQUERADE

#### 3.4. 日志

防火墙日志对于识别攻击、排除防火墙规则故障以及注意网络上的异常活动至关重要。但是，您必须在防火墙中包含日志规则才能生成这些规则，并且日志规则必须位于任何适用的终止规则（具有决定数据包命运的目标的规则，如接受、丢弃或拒绝）之前。

如果您使用的是ufw，则可以通过在终端中输入以下内容来打开日志记录：**sudoufw登录**

要在ufw中关闭日志记录，只需在上述命令中将on替换为off。

如果使用iptables而不是ufw，请输入：

sudo iptables-A INPUT-m state--state NEW-p tcp--dport 80 \-j LOG--LOG前缀“NEW\_HTTP\_CONN:”

然后，来自本地计算机的端口80上的请求将在dmesg中生成如下所示的日志（单行拆分为3以适合此文档）：

[4304885.870000]新的\u HTTP\_CONN:IN=lo OUT=MAC=00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP

SPT=53981 DPT=80窗口=32767分辨率=0x00同步URGP=0

上述日志也将出现在/var/log/messages、/var/log/syslog和/var/log/kern.log中。可以通过适当编辑/etc/syslog.conf或通过安装和配置ulogd并使用ULOG目标而不是日志来修改此行为。ulogd守护进程是一个用户空间服务器，它侦听内核中专门针对防火墙的日志记录指令，并可以登录到您喜欢的任何文件，甚至可以登录到PostgreSQL或MySQL数据库。通过使用日志分析工具，如logwatch、fwanalog、fwlogwatch或lire，可以简化防火墙日志的意义。

#### 3.5. 其他工具

有许多工具可以帮助您在不熟悉iptables的情况下构建完整的防火墙。带有纯文本配置文件的命令行工具：

•Shorewall[167]是一个非常强大的解决方案，可帮助您为任何网络配置高级防火墙。

#### 3.6. 工具书类

•Ubuntu防火墙[168]wiki页面包含有关ufw开发的信息。

•此外，ufw手册页面包含一些非常有用的信息：man ufw。

•有关使用iptables的更多信息，请参阅数据包过滤指南[169]。

•nat HOWTO[170]包含关于伪装的更多细节。

•Ubuntu wiki中的IPTables HowTo[171]是一个很好的资源。

## 4.公寓

AppArmor是基于名称的强制访问控制的Linux安全模块实现。AppArmor将单个程序限制为一组列出的文件和posix 1003.1e草稿功能。

默认情况下安装并加载AppArmor。它使用应用程序的配置文件来确定应用程序需要哪些文件和权限。一些软件包将安装自己的配置文件，在apparmor配置文件软件包中可以找到其他配置文件。

要从终端提示符安装apparmor profiles软件包，请执行以下操作：**sudo apt安装apparmor配置文件**

AppArmor配置文件有两种执行模式：

•投诉/学习：允许并记录档案违规行为。用于测试和开发新的配置文件。

•强制/限制：强制配置文件策略以及记录违规行为。

#### 4.1. 使用AppArmor

本节存在一个bug（LP#1304134[172]），说明将无法按照广告的方式工作。

apparmor utils包包含命令行实用程序，可用于更改apparmor执行模式、查找配置文件的状态、创建新配置文件等。

•apparmor\_状态用于查看apparmor配置文件的当前状态。**苏多公寓**

•aa投诉将配置文件置于投诉模式。**sudo aa投诉/路径/收件人/邮箱**

•aa强制将配置文件置于强制模式。**sudo aa强制执行/path/to/bin**

•apparmor配置文件位于/etc/apparmor.d目录。它可用于操纵所有配置文件的模式。

输入以下内容以将所有配置文件置于投诉模式：

**sudo aa投诉/etc/apparmor.d/\***

要将所有配置文件置于强制模式，请执行以下操作：**sudo aa强制执行/etc/apparmor.d/\***

•apparmor\_解析器用于将配置文件加载到内核中。还可以使用-r选项重新加载当前加载的配置文件。要加载配置文件，请执行以下操作：

**cat/etc/apparmor.d/profile.name | sudo apparmor\_解析器-a cat/etc/apparmor.d/profile.name | sudo apparmor\_解析器-r**要重新加载配置文件，请执行以下操作：

•systemctl可用于重新加载所有配置文件：**sudo systemctl重新加载安装服务**

•可以将/etc/apparmor.d/disable目录与apparmor\_parser-R选项一起使用，以禁用配置文件。

**sudo ln-s/etc/apparmor.d/profile.name/etc/apparmor.d/disable/sudo apparmor\_解析器-R/etc/apparmor.d/profile.name**

要重新启用禁用的配置文件，请删除/etc/apparmor.d/disable/中指向该配置文件的符号链接。

然后使用-a选项加载配置文件。

**sudo rm/etc/apparmor.d/disable/profile.name**

**cat/etc/apparmor.d/profile.name | sudo apparmor\_解析器-a**

•可通过输入以下命令禁用AppArmor，并卸载内核模块：

**sudo systemctl stop apparmor.service sudo update rc.d-f apparmor remove**

•要重新启用AppArmor，请输入：

**sudo systemctl start apparmor.service sudo update rc.d apparmor默认值**

将profile.name替换为要操作的配置文件的名称。另外，将/path/to/bin/替换为实际的可执行文件路径。例如，对于ping命令，请使用/bin/ping

#### 4.2. 轮廓

AppArmor配置文件是位于/etc/AppArmor.d/中的简单文本文件。这些文件以其配置文件的可执行文件的完整路径命名，将“/”替换为“.”。例如/etc/apparmor.d/bin.ping是/bin/ping命令的apparmor配置文件。

配置文件中使用了两种主要类型的规则：

•详细说明应用程序可以在文件系统中访问哪些文件。*路径条目：*

•确定允许受限流程使用的权限。*能力条目：*

以/etc/apparmor.d/bin.ping为例：

#包括<tunables/global>

/bin/ping标志=（投诉）{

#包括<abstractions/base>

#包括<abstractions/consoles>#包括<abstractions/nameservice>

能力网络原始、能力设置UID、网络inet原始、，

/bin/ping mixr，/etc/modules.conf r，

}

•包括来自其他文件的声明。这允许将与多个应用程序相关的语句放在一个公共文件中。*#包括<tunables/global>：*

•配置文件程序的路径，还将模式设置为投诉。*/bin/ping标志=（投诉）：*

•允许应用程序访问CAP\_NET\_原始Posix.1e功能。*未加工的净能力：*

•允许应用程序读取和执行对文件的访问。*/箱式/平式混合器：*

编辑配置文件后，必须重新加载配置文件。详见第4.1节“使用AppArmor”[p.194]。

##### 4.2.1. 创建配置文件

•尝试思考应用程序应如何运行。测试计划应划分为小测试用例。每个测试用例都应该有一个小的描述，并列出要遵循的步骤。*设计测试计划：*

一些标准测试用例包括：

•启动该计划。

•停止程序。

•重新加载程序。

•测试init脚本支持的所有命令。

•使用aa genprof生成新的配置文件。从终端：*生成新的配置文件：***sudo-aa-genprof可执行文件**

例如：

**sudo-aa-genprof-slapd**

•要将您的新配置文件包含在apparmor profiles软件包中，请在Launchpad中针对apparmor[173]软件包提交一个bug：

•包括您的测试计划和测试用例。

•将您的新配置文件附加到bug。

##### 4.2.2. 更新配置文件

当程序出现异常时，会将审核消息发送到日志文件。aa logprof程序可用于扫描日志文件，查找AppArmor审核消息，查看它们并更新配置文件。从终端：**sudo aa logprof**

#### 4.3. 工具书类

•有关高级配置选项，请参阅AppArmor管理指南[174]。

•有关将AppArmor与其他Ubuntu版本一起使用的详细信息，请参阅AppArmor社区Wiki[175]页面。

•OpenSUSE AppArmor[176]页面是AppArmor的另一个介绍。

•在freenode上的#Ubuntu服务器IRC频道[177]是寻求AppArmor帮助并参与Ubuntu服务器社区的好地方。

## 5.证书

当今最常见的密码学形式之一是公钥密码学。公钥密码使用公钥和私钥。系统通过使用公钥加密信息来工作。然后只能使用私钥对信息进行解密。

公钥加密的一个常见用途是使用安全套接字层（SSL）或传输层安全性（TLS）连接加密应用程序流量。一个示例：配置Apache以提供HTTPS，即通过SSL的HTTP协议。这允许使用本身不提供加密的协议对流量进行加密。

证书是一种用于分发公钥以及有关服务器和负责该服务器的组织的其他信息的方法。证书可以由证书颁发机构或CA进行数字签名。

CA是一个受信任的第三方，它已确认证书中包含的信息是准确的。

#### 5.1. 证书类型

要使用公钥加密设置安全服务器，在大多数情况下，您需要向CA发送证书请求（包括公钥）、公司身份证明和付款。CA会验证证书请求和您的身份，然后发回安全服务器的证书。或者，您可以创建自己的自签名证书。

请注意，在大多数生产环境中不应使用自签名证书。

继续HTTPS示例，CA签名证书提供了自签名证书所不具备的两个重要功能：

•浏览器（通常）自动识别证书，并允许在不提示用户的情况下建立安全连接。

•当CA颁发签名证书时，它保证向浏览器提供网页的组织的身份。

大多数支持SSL的Web浏览器和计算机都有一个CA列表，它们会自动接受这些CA的证书。如果浏览器遇到授权CA不在列表中的证书，浏览器会要求用户接受或拒绝连接。此外，其他应用程序在使用自签名证书时可能会生成错误消息。

从CA获取证书的过程相当简单。简要概述如下：

1.    创建私有和公共加密密钥对。

2.    基于公钥创建证书请求。证书请求包含有关您的服务器和托管该服务器的公司的信息。

3.    将证书请求以及证明您身份的文档发送到CA。我们无法告诉您选择哪个证书颁发机构。你的决定可能基于你过去的经验，或者你的朋友或同事的经验，或者纯粹基于金钱因素。

一旦您决定了CA，您需要按照他们提供的关于如何从他们那里获得证书的说明进行操作。

4.    当CA确信您确实是您声称的人时，他们会向您发送数字证书。

5.    在安全服务器上安装此证书，并配置适当的应用程序以使用该证书。

#### 5.2. 生成证书签名请求（CSR）

无论您是从CA获取证书还是生成自己的自签名证书，第一步都是生成密钥。

如果证书将由服务守护进程（如Apache、Postfix、Dovecot等）使用，则不带密码短语的密钥通常是合适的。没有密码短语允许服务在无需手动干预的情况下启动，这通常是启动守护程序的首选方式。

本节将介绍如何生成带有密码短语的密钥，以及如何生成不带密码短语的密钥。然后，非密码密钥将用于生成可用于各种服务守护进程的证书。

在没有密码短语的情况下运行安全服务很方便，因为您不需要在每次启动安全服务时输入密码短语。但它是不安全的，密钥的泄露也意味着服务器的泄露。

要生成证书签名请求（CSR）的密钥，请从终端提示符运行以下命令：**openssl genrsa-des3-out server.key 2048**

正在生成RSA私钥，2048位长模数为65537（0x10001）。请为服务器输入密码短语。密钥：

您现在可以输入您的密码短语。为获得最佳安全性，它至少应包含八个字符。指定-des3时的最小长度为四个字符。它应该包括数字和/或标点符号，而不是字典中的单词。还要记住，您的密码短语区分大小写。

重新键入要验证的密码短语。正确地重新键入后，将生成服务器密钥并将其存储在server.key文件中。

现在，创建不安全的密钥，即没有密码短语的密钥，并将密钥名称洗牌：

**openssl rsa-in server.key-out server.key.unsecure mv server.key server.key.secure mv server.key.unsecure server.key.unsecure server.key**

不安全的密钥现在命名为server.key，您可以使用此文件生成CSR，而无需密码短语。

要创建CSR，请在终端提示符下运行以下命令：**openssl req-new-key server.key-out server.csr**

它将提示您输入密码短语。如果您输入正确的密码短语，它将提示您输入公司名称、站点名称、电子邮件Id等。一旦您输入所有这些详细信息，您的CSR将被创建并存储在server.CSR文件中。

您现在可以将此CSR文件提交给CA进行处理。CA将使用此CSR文件并颁发证书。另一方面，您可以使用此CSR创建自签名证书。

#### 5.3. 创建自签名证书

要创建自签名证书，请在终端提示符下运行以下命令：**openssl x509-req-days 365-in server.csr-signkey server.key-out server.crt**

上面的命令将提示您输入密码短语。输入正确的密码短语后，将创建证书并将其存储在server.crt文件中。

如果要在生产环境中使用安全服务器，可能需要CA签名的证书。不建议使用自签名证书。

#### 5.4. 安装证书

通过在终端提示符下运行以下命令，可以安装密钥文件server.key和证书文件server.crt，或CA颁发的证书文件：

**sudo cp server.crt/etc/ssl/certs sudo cp server.key/etc/ssl/private**

现在，只需配置任何能够使用公钥加密的应用程序，即可使用证书和密钥文件。例如，Apache可以提供HTTPS，Dovecot可以提供IMAP和POP3等。

#### 5.5. 证书颁发机构

如果您网络上的服务需要多个自签名证书，则可能值得付出额外的努力来设置您自己的内部证书颁发机构（CA）。使用由您自己的CA签名的证书，允许使用证书的各种服务轻松信任使用同一CA颁发的证书的其他服务。

1.         首先，创建目录以保存CA证书和相关文件：

**sudo mkdir/etc/ssl/CA sudo mkdir/etc/ssl/newcerts**

2.         CA需要几个额外的文件来操作，一个用于跟踪CA使用的最后一个序列号，每个证书必须具有唯一的序列号，另一个文件用于记录已颁发的证书：

**sudosh-c“echo&apos;01&apos;>/etc/ssl/CA/serial”sudotouch/etc/ssl/CA/index.txt**

3.         第三个文件是CA配置文件。虽然不是严格必需的，但在颁发多个证书时非常方便。编辑/etc/ssl/openssl.cnf，并在[CA\_default]更改中：

dir=/etc/ssl#其中所有内容都保存在数据库中=$dir/CA/index.txt#数据库索引文件。证书=$dir/certs/cacert.pem#CA证书序列=$dir/CA/serial#当前序列号private#key=$dir/private/cakey.pem#私钥

4.         接下来，创建自签名根证书：

**openssl请求-新建-x509-扩展v3\_ca-keyout cakey.pem-out cacert.pem-第3650天**

然后将要求您输入有关证书的详细信息。

5.         现在安装根证书和密钥：

**sudo mv cakey.pem/etc/ssl/private/sudo mv cacert.pem/etc/ssl/certs/**

6.         您现在可以开始签署证书了。需要的第一项是证书签名请求（CSR），有关详细信息，请参见第5.2节“生成证书签名请求（CSR）”[p.199]。拥有CSR后，输入以下内容以生成由CA签名的证书：**sudo openssl ca-in server.csr-config/etc/ssl/openssl.cnf**

输入CA密钥的密码后，系统将提示您签署证书，然后再次提交新证书。然后，您应该会看到与证书创建相关的大量输出。

7.         现在应该有一个新文件/etc/ssl/newcerts/01.pem，其中包含相同的输出。将所有内容复制并粘贴到一个文件中，该文件以安装证书的服务器的主机名命名，该文件以------开始证书------行开始，然后继续执行------结束证书------行。例如mail.example.com.crt，是一个很好的描述性名称。

后续证书将命名为02.pem、03.pem等。

用您自己的描述性名称替换mail.example.com.crt。

8.         最后，将新证书复制到需要它的主机，并配置适当的应用程序来使用它。安装证书的默认位置是/etc/ssl/certs。这使多个服务可以使用同一证书，而无需过度复杂的文件权限。

对于可以配置为使用CA证书的应用程序，还应将/etc/ssl/certs/cacert.pem文件复制到每台服务器上的/etc/ssl/certs/目录。

#### 5.6. 工具书类

•有关使用加密技术的更详细说明，请参阅tldp.org提供的SSL证书HOWTO[178][179]：

•Wikipedia HTTPS13页面包含更多关于HTTPS的信息。

•有关OpenSSL的更多信息，请参阅OpenSSL主页[180]。

•此外，O&apos;Reilly的OpenSSL网络安全[181]是一个很好的深入参考。

## 6.埃克瑞普斯

*埃克瑞普斯*是一个兼容POSIX的Linux企业级堆叠加密文件系统。文件系统层之上的分层eCryptfs保护文件，无论底层文件系统、分区类型等如何。

在安装过程中，可以选择加密/home分区。这将自动配置加密和装载分区所需的一切。

例如，本节将介绍如何使用eCryptfs配置要加密的/srv。

#### 6.1. 使用eCryptfs

首先，安装必要的软件包。在终端提示中输入：现在装载要加密的分区：**sudo apt安装ecryptfs utils sudo安装-t ecryptfs/srv/srv**

然后，系统会提示您提供有关ecryptfs应如何加密数据的一些详细信息。

要测试放置在/srv中的文件是否确实加密，请将/etc/default文件夹复制到/srv:Now卸载/srv，并尝试查看文件：**sudo cp-r/etc/default/srv**

**sudo umount/srv cat/srv/default/cron**

使用ecryptfs重新安装/srv将使数据再次可见。

#### 6.2. 自动装载加密分区

有两种方法可以在引导时自动装载ecryptfs加密的文件系统。此示例将使用包含装载选项的/root/.ecryptfsrc文件，以及驻留在USB密钥上的密码短语文件。

首先，创建/root/.ecryptfsrc，其中包含：

key=passphrase:passphrase\_passwd\_file=/mnt/usb/passwd\_file.txt ecryptfs\_sig=5826dd62cf81c615 ecryptfs\_cipher=aes ecryptfs\_key\_bytes=16 ecryptfs\_passthrough=n ecryptfs\_enable\_filename\_crypto=n

将ecryptfs\_sig调整为/root/.ecryptfs/sig-cache.txt中的签名。

接下来，创建/mnt/usb/passwd\_file.txt密码文件：passphrase\_passwd=[secrets]

现在将必要的行添加到/etc/fstab：

/dev/sdb1/mnt/usb ext3 ro 0

/srv/srv ecryptfs默认值为0 0

确保在加密分区之前安装USB驱动器。

最后，应使用eCryptfs重新启动和安装/srv。

#### 6.3. 其它工具

ecryptfs utils包还包括几个其他有用的实用程序：

•创建~/Private目录以包含加密信息。此实用程序可由非特权用户运行，以使数据对系统上的其他用户保密。*ecryptfs设置专用：*

•和ecryptfs umount private将装载和卸载用户的~/private目录。*埃克瑞夫斯私人山酒店*

•向内核密钥环添加新的密码短语。*ecryptfs添加密码短语：*

•管理eCryptfs对象，如密钥。*秘书长：*

•允许您查看文件的ecryptfs元信息。*ecryptfs统计数据：*

#### 6.4. 工具书类

•有关eCryptfs的更多信息，请参见Launchpad项目页面[182]。

•还有一篇Linux杂志[183]文章介绍了eCryptfs。

•此外，有关更多ecryptfs选项和详细信息，请参阅ecryptfs手册页[184]。

# 第十章。监测

## 1.概述

对基本服务器和服务的监视是系统管理的一个重要部分。大多数网络服务都会受到性能和/或可用性的监控。本节将介绍用于可用性监控的Nagios和用于性能监控的Munin的安装和配置。

本节中的示例将使用主机名为server01和server02的两台服务器。Server01将配置Nagios以监控自身和server02上的服务。Server01还将与munin软件包一起设置，以从网络收集信息。使用munin节点包，server02将被配置为向server01发送信息。

希望这些简单的示例能够让您监视网络上的其他服务器和服务。

## 2.纳吉奥斯

#### 2.1. 安装

首先，在server01上安装nagios软件包。在终端中输入：**sudo apt安装nagios3 nagios nrpe插件**

将要求您输入nagiosadmin用户的密码。用户的凭据存储在/etc/nagios3/htpasswd.users中。要更改nagiosadmin密码，或向Nagios CGI脚本添加其他用户，请使用apache2 utils包中的htpasswd。

例如，要更改nagiosadmin用户的密码，请输入：要添加用户：**sudo htpasswd/etc/nagios3/htpasswd.users nagiosadmin sudo htpasswd/etc/nagios3/htpasswd.users**

接下来，在server02上安装nagios nrpe服务器包。从server02上的终端输入：**sudo apt安装nagios nrpe服务器**

NRPE允许您在远程主机上执行本地检查。通过其他Nagios插件以及其他检查，还有其他方法可以实现这一点。

#### 2.2. 配置概述

有几个目录包含Nagios配置和检查文件。

•/etc/nagios3：包含nagios守护程序操作的配置文件、CGI文件、主机等。

•/etc/nagios插件：包含服务检查的配置文件。

•/etc/nagios：远程主机上包含nagios nrpe服务器配置文件。

•/usr/lib/nagios/plugins/：检查二进制文件的存储位置。要查看复选框的选项，请使用-h选项。

##### 例如：/usr/lib/nagios/plugins/check\u dhcp-h

Nagios可以配置为对任何给定主机执行大量检查。对于本例，Nagios将配置为检查磁盘空间、DNS和MySQL主机组。DNS检查将在server02上进行，MySQL主机组将同时包括server01和server02。

有关设置Apache的详细信息，请参见第1节“HTTPD-Apache2 Web服务器”[p.214]，第8章域名服务（DNS）[p.166]用于DNS，第1节“MySQL”[p.233]用于DNS

MySQL。

此外，有一些术语一旦解释过，有望使理解Nagios配置变得更容易：

•：被监控的服务器、工作站、网络设备等。*主办*

•：一组类似的主机。例如，您可以对所有web服务器、文件服务器等进行分组。*主机组*

•：主机上正在监视的服务。例如HTTP、DNS、NFS等。*服务*

•：允许您将多个服务组合在一起。例如，这对于分组多个HTTP非常有用。*服务组*

•：事件发生时应通知的人员。Nagios可以配置为发送电子邮件、短信等。*联系*

默认情况下，Nagios配置为检查本地主机上的HTTP、磁盘空间、SSH、当前用户、进程和负载。Nagios还将ping检查网关。

大型Nagios安装的配置可能相当复杂。通常，最好从一个或两个小型主机开始，按照您喜欢的方式进行配置，然后扩展。

#### 2.3. 配置

• 1. 首先，为server02创建主机配置文件。除非另有规定，否则在server01上运行所有这些命令。在终端中输入：

**sudo cp/etc/nagios3/conf.d/localhost\u nagios2.cfg\/etc/nagios3/conf.d/server02.cfg**

在上面和下面的命令示例中，替换“server01”、“server02”

*172.18.100.100*，和172.18.100.101，以及服务器的主机名和IP地址。

     2.接下来，编辑/etc/nagios3/conf.d/server02.cfg：

定义主机{

使用通用主机；主机模板的名称来使用主机\u Name server02 alias Server 02 address 172.18.100.101}

#检查DNS服务。

定义服务{

使用通用服务主机名称server02服务描述DNS

check\_命令check\_dns！172.18.100.101}

     3.重新启动nagios守护程序以启用新配置：

**sudo systemctl重新启动nagio3.service**

• 1. 现在，通过将以下内容添加到/etc/nagios3/conf.d/services\u nagios2.cfg，为MySQL检查添加服务定义：

#检查MySQL服务器。

定义服务{

主机组名称mysql服务器服务描述mysql

check\_命令check\_mysql\_cmdlinecred！nagios！secret！$HOSTADDRESS使用通用服务

通知\_interval0；如果要重新命名，请设置>0}

2.         现在需要定义mysql服务器主机组。编辑/etc/nagios3/conf.d/hostgroups\u nagios2.cfg添加：

#MySQL主机组。定义主机组{

主机组\u名称mysql服务器别名mysql服务器成员localhost，server02}

3.         Nagios检查需要对MySQL进行身份验证。要将nagios用户添加到MySQL，请输入：

**mysql-u root-p-e“创建由&apos;secret&apos;标识的用户nagios”**

需要将nagios用户添加到mysql服务器主机组中的所有主机。

4.         重新启动nagios以开始检查MySQL服务器。

**sudo systemctl重新启动nagios3.service**

• 1. 最后，配置NRPE以检查server02上的磁盘空间。

在server01上，将服务检查添加到/etc/nagios3/conf.d/server02.cfg：

#磁盘检查。定义服务{

使用通用服务主机\u名称server02服务\u说明nrpe磁盘

check\_命令check\_nrpe\_1arg！检查所有磁盘！172.18.100.101}

2.         现在在server02上编辑/etc/nagios/nrpe.cfg更改：

允许的\_主机=172.18.100.100

和下面的命令定义区域中添加：

命令[check\_all\_disk]=/usr/lib/nagios/plugins/check\_disk-w 20%-c 10%-e

3.         最后，重新启动nagios nrpe服务器：

**sudo systemctl重新启动nagios-nrpe-server.service**

4.         另外，在server01上重新启动nagios：

**sudo systemctl重新启动nagios3.service**

您现在应该能够在Nagios CGI文件中看到主机和服务检查。要访问它们，请指向浏览器http://server01/nagios3. 然后会提示您输入nagiosadmin用户名和密码。

#### 2.4. 工具书类

本节刚刚触及Nagios功能的表面。nagios插件extra和nagios snmpplugins包含更多的服务检查。

•有关更多信息，请参见Nagios[185]网站。

•特别是在线文档[186]网站。

•还有一份与Nagios和网络监控相关的书籍清单[187]：

•Nagios Ubuntu Wiki[188]页面也有更多细节。

## 3.雾尼

#### 3.1. 安装

在server01上安装Munin之前，需要安装apache2。默认配置适用于运行munin服务器。有关更多信息，请参阅第1节“HTTPD-Apache2 Web服务器”[p.214]。

首先，在server01上安装munin。在终端中输入：**sudo安装munin**

现在在server02上安装munin节点包：**sudo apt安装munin节点**

#### 3.2. 配置

在server01上编辑/etc/munin/munin.conf，添加server02的IP地址：

##首先是我们的“正常”主人。[服务器02]

地址172.18.100.101

用服务器的实际主机名和IP地址替换server02和172.18.100.101。

接下来，在server02上配置munin节点。编辑/etc/munin/munin-node.conf以允许server01访问：允许^172\.18\.100\.100$

将^172\.18\.100\.100$替换为munin服务器的IP地址。

现在在server02上重新启动munin节点，以使更改生效：**sudo systemctl重新启动munin-node.service**

最后，在浏览器中转到http://server01/munin，并且您应该可以看到显示磁盘、网络、进程和系统的标准munin插件信息的精美图形链接。

因为这是一个新的安装，所以图表可能需要一些时间来显示任何有用的内容。

#### 3.3. 附加插件

munin插件额外软件包包含性能检查附加服务，如DNS、DHCP、Samba等。要安装软件包，请从终端输入：

**sudo apt额外安装munin插件**

请确保在服务器和节点计算机上安装该软件包。

#### 3.4. 工具书类

•更多详情请参见Munin[189]网站。

•具体而言，Munin文档[190]页面包含关于附加插件、编写插件等的信息。

# 第十一章。网络服务器

Web服务器是一种软件，负责接受来自客户端（称为Web浏览器）的HTTP请求，并为其提供HTTP响应和可选数据内容，这些内容通常是网页，如HTML文档和链接对象（图像等）。

## 1.HTTPD-Apache2网络服务器

Apache是Linux系统上最常用的Web服务器。Web服务器用于为客户端计算机请求的网页提供服务。客户端通常使用Firefox、Opera、Chromium或Internet Explorer等Web浏览器应用程序请求和查看网页。

用户输入统一资源定位器（URL）以通过其完全限定的方式指向Web服务器

域名（FQDN）和所需资源的路径。例如，要查看Ubuntu网站[191]的主页，用户只需输入FQDN：**www.ubuntu.com**

要查看社区[192]子页面，用户将输入FQDN，后跟路径：**www.ubuntu.com/community**

用于传输网页的最常见协议是超文本传输协议（HTTP）。还支持安全套接字层上的超文本传输协议（HTTPS）和文件传输协议（FTP）（用于上传和下载文件的协议）等协议。

ApacheWeb服务器通常与MySQL数据库引擎、超文本预处理器（PHP）脚本语言以及其他流行的脚本语言（如Python和Perl）结合使用。这种配置被称为LAMP（Linux、Apache、MySQL和Perl/Python/PHP），为基于Web的应用程序的开发和部署提供了强大而健壮的平台。

#### 1.1. 安装

Apache2 web服务器在Ubuntu Linux中可用。要安装Apache2：

•在终端提示下，输入以下命令：

**sudo apt安装apache2**

#### 1.2. 配置

Apache2是通过在纯文本配置文件中放置指令来配置的。这些指令在以下文件和目录之间分开：

•主Apache2配置文件。包含Apache2的全局设置。*apache2.conf：*

•历史上主要的Apache2配置文件，以httpd守护程序命名。现在该文件不存在。在较旧版本的Ubuntu中，该文件可能存在，但为空，因为所有配置选项都已移动到下面引用的目录中。*httpd.conf：*

•此目录包含可用的配置文件。以前位于/etc中的所有文件/*可提供的配置文件：*

apache2/conf.d应移到/etc/apache2/conf-available。

•保存指向/etc/apache2/conf中文件的符号链接。当配置文件被符号链接时，它将在下次重新启动apache2时启用。*已启用配置：*

•设置Apache2环境变量的文件。*环境变量：*

•此目录包含加载模块和配置模块的配置文件。但是，并非所有模块都有特定的配置文件。*可提供的mods：*

•保存指向/etc/apache2/mods中文件的符号链接。当模块配置文件被符号链接时，它将在下次重新启动apache2时启用。*已启用mods：*

•包含确定Apache2正在侦听的TCP端口的指令。*ports.conf：*

•此目录包含Apache2虚拟主机的配置文件。虚拟主机允许为具有单独配置的多个站点配置Apache2。*可用站点：*

•与启用mods一样，启用的站点包含指向/etc/apache2/sitesavailable目录的符号链接。类似地，当可用站点中的配置文件被符号链接时，它配置的站点将在Apache2重新启动后处于活动状态。*启用的站点：*

•根据文件的前几个字节确定MIME类型的说明。*魔术：*

此外，可以使用Include指令添加其他配置文件，并且可以使用通配符包含许多配置文件。任何指令都可以放在这些配置文件中。主配置文件的更改只有在Apache2启动或重新启动时才能被识别。

服务器还读取包含mime文档类型的文件；文件名由TypesConfig指令设置，通常通过/etc/apache2/mods available/mime.conf设置，其中可能还包括添加和重写，默认情况下为/etc/mime.types。

##### 1.2.1. 基本设置

本节介绍Apache2服务器的基本配置参数。有关更多详细信息，请参阅Apache2文档[193]。

•Apache2附带虚拟主机友好的默认配置。也就是说，它配置有一个默认虚拟主机（使用VirtualHost指令），如果您有一个站点，则可以按原样修改或使用该虚拟主机；如果您有多个站点，则可以将其用作其他虚拟主机的模板。如果不使用，默认虚拟主机将用作默认站点，或者站点用户将看到他们输入的URL是否与任何自定义站点的ServerName指令不匹配。要修改默认虚拟主机，请编辑文件/etc/apache2/sites available/000-default.conf。

为虚拟主机设置的指令仅适用于该特定虚拟主机。如果指令是在服务器范围内设置的，并且未在虚拟主机设置中定义，则使用默认设置。例如，您可以定义网站管理员电子邮件地址，而不是为每个虚拟主机定义单独的电子邮件地址。

如果要配置新的虚拟主机或站点，请使用所选名称将该文件复制到同一目录中。例如：

**sudo cp/etc/apache2/sites available/000-default.conf/etc/apache2/sites available/mynewsite.conf**

使用下面描述的一些指令编辑新文件以配置新站点。

•ServerAdmin指令指定要为服务器管理员播发的电子邮件地址。默认值为webmaster@localhost. 应将其更改为发送给您的电子邮件地址（如果您是服务器管理员）。如果您的网站出现问题，Apache2将显示一条错误消息，其中包含要向其报告问题的电子邮件地址。在/etc/apache2/sites available中的站点配置文件中找到此指令。

•Listen指令指定Apache2应侦听的端口和可选IP地址。如果未指定IP地址，Apache2将侦听分配给其运行的机器的所有IP地址。Listen指令的默认值为80。将此更改为127.0.0.1:80以使Apache2仅在环回接口上侦听，从而使其在Internet上不可用；将此更改为（例如）81以更改其侦听的端口，或使其保持正常运行状态。该指令可以在其自己的文件/etc/apache2/ports.conf中找到并更改

•ServerName指令是可选的，它指定站点应响应的FQDN。默认虚拟主机未指定ServerName指令，因此它将响应与另一虚拟主机中的ServerName指令不匹配的所有请求。如果您刚刚获得域名ubuntrocks.com并希望将其托管在Ubuntu服务器上，那么虚拟主机配置文件中的ServerName指令的值应该是ubuntrocks.com。将此指令添加到先前创建的新虚拟主机文件（/etc/apache2/sites available/mynewsite.conf）。

您可能还希望您的站点响应www.ubunturocks.com，因为许多用户会认为www前缀是合适的。为此使用ServerAlias指令。您还可以在ServerAlias指令中使用通配符。

例如，以下配置将导致您的站点响应以.ubunturocks.com结尾的任何域请求。

ServerAlias\*.ubunturocks.com

•DocumentRoot指令指定Apache2应在何处查找构成站点的文件。默认值为/var/www/html，如/etc/apache2/sites available/000-default.conf中所指定。如果需要，请在站点的虚拟主机文件中更改此值，并记住在必要时创建该目录！

使用a2ensite实用程序启用新的VirtualHost并重新启动Apache2：

**苏多a2ensite mynewsite**

**sudo systemctl重新启动apache2.service**

请确保为VirtualHost使用更具描述性的名称替换mynewsite。一种方法是以VirtualHost的ServerName指令命名文件。

类似地，使用A2Dispatite实用程序禁用站点。这在对多个VirtualHost的配置问题进行故障排除时非常有用：

**苏多火山灰岩**

**sudo systemctl重新启动apache2.service**

##### 1.2.2. 默认设置

本节介绍Apache2服务器默认设置的配置。例如，如果添加虚拟主机，则为该虚拟主机配置的设置优先于该虚拟主机。对于虚拟主机设置中未定义的指令，将使用默认值。

•当用户通过在目录名称末尾指定正斜杠（/）来请求目录索引时，DirectoryIndex是服务器提供的默认页面。

例如，当用户请求页面时http://www.example.com/this\_directory/，他或她将获得DirectoryIndex页面（如果存在）、服务器生成的目录列表（如果不存在且指定了Indexes选项），或者权限拒绝页面（如果两者都不存在）。服务器将尝试查找DirectoryIndex指令中列出的一个文件，并返回找到的第一个文件。如果找不到这些文件中的任何一个，并且为该目录设置了选项索引，服务器将以HTML格式生成并返回该目录中的子目录和文件的列表。在/etc/apache2/mods available/dir.conf中找到的默认值是“index.html index.cgi index.pl index.php index.xhtml index.htm”。因此，如果Apache2在请求的目录中找到与这些名称中的任何一个匹配的文件，则会显示第一个名称。

•ErrorDocument指令允许您为Apache2指定用于特定错误事件的文件。例如，如果用户请求不存在的资源，将发生404错误。默认情况下，Apache2只返回HTTP 404返回代码。阅读/etc/apache2/conf available/localized-errorpages.conf，了解使用ErrorDocument的详细说明，包括示例文件的位置。

•默认情况下，服务器将传输日志写入文件/var/log/apache2/access.log。您可以使用CustomLog指令在虚拟主机配置文件中对每个站点进行更改，也可以将其忽略为

接受/etc/apache2/conf available/other-vhosts-access-log.conf中指定的默认值。您还可以通过ErrorLog指令指定记录错误的文件，该指令的默认值为/var/log/apache2/error.log。这些日志与传输日志分开保存，以帮助您解决Apache2服务器的问题。您还可以指定日志级别（默认值为“warn”）和日志格式（默认值见/etc/apache2/apache2.conf）。

•某些选项是按目录而不是按服务器指定的。选项是这些指令之一。目录节包含在类似XML的标记中，如下所示：

<Directory/var/www/html/mynewsite>。。。

</Directory>

目录节中的Options指令接受以下一个或多个值（除其他值外），以空格分隔：

•-允许执行CGI脚本。如果未选择此选项，则不会执行CGI脚本。**执行CGI**

大多数文件不应作为CGI脚本执行。这将是非常危险的。CGI脚本应保存在DocumentRoot之外的独立目录中，并且仅此目录应设置ExecCGI选项。这是默认值，也是的默认位置

CGI脚本是/usr/lib/CGI-bin。

•-允许服务器端包含。服务器端包含允许HTML文件包含其他文件。有关更多信息，请参阅ApacheSSI文档（Ubuntu社区）[194]。**包括**

•-允许服务器端包含，但禁用CGI脚本中的#exec和#include命令。**包括noexec**

•-如果请求的目录中不存在DirectoryIndex（如index.html），则显示目录内容的格式化列表。**索引**

出于安全原因，通常不应设置此选项，当然也不应在DocumentRoot目录上设置此选项。仅当您确定希望用户查看目录的全部内容时，才在每个目录的基础上仔细启用此选项。

•-支持内容协商多视图；出于安全原因，默认情况下禁用此选项。请参阅有关此选项的Apache2文档[195]。**多画面**

•-如果目标文件或目录与链接具有相同的所有者，则仅遵循符号链接。**符号链接所有者匹配**

##### 1.2.3. httpd设置

本节介绍一些基本的httpd守护程序配置设置。

**锁文件**-LockFile指令设置使用USE\_FCNTL\_SERIALIZED\_ACCEPT或USE\_FLOCK\_SERIALIZED\_ACCEPT编译服务器时使用的锁文件的路径。它必须存储在计算机上

本地磁盘。除非日志目录位于NFS共享上，否则应将其保留为默认值。如果是这种情况，则应将默认值更改为本地磁盘上的某个位置以及仅由root用户可读的目录。

**PidFile**-PidFile指令设置服务器记录其进程ID（pid）的文件。此文件只能由root用户读取。在大多数情况下，应将其保留为默认值。

**使用者**-User指令设置服务器用于应答请求的userid。此设置确定服务器的访问权限。此用户无法访问的任何文件也将无法访问您的网站访问者。用户的默认值为“www数据”。

除非您确切知道自己在做什么，否则不要将用户指令设置为root。使用root作为用户将为Web服务器创建较大的安全漏洞。

**组**-Group指令与User指令类似。组设置服务器将在其下应答请求的组。默认组也是“www数据”。

##### 1.2.4. Apache2模块

Apache2是一个模块化服务器。这意味着核心服务器中只包含最基本的功能。扩展功能通过可加载到Apache2中的模块提供。默认情况下，编译时服务器中包含一组基本模块。如果将服务器编译为使用动态加载的模块，则可以单独编译模块，并随时使用LoadModule指令添加模块。

否则，必须重新编译Apache2才能添加或删除模块。

Ubuntu编译Apache2以允许动态加载模块。通过将配置指令封装在<IfModule>块中，配置指令可以有条件地包含在特定模块的存在上。

您可以安装其他Apache2模块，并将其用于Web服务器。例如，在终端提示符下运行以下命令以安装MySQL身份验证模块：**sudo apt安装libapache2 mod auth mysql**

有关其他模块，请参阅/etc/apache2/mods可用目录。

使用a2enmod实用程序启用模块：

**sudo a2enmod auth\_mysql**

**sudo systemctl重新启动apache2.service**同样，a2dismod将禁用模块：

**sudoa2dismodauth\_mysql**

**sudo systemctl重新启动apache2.service**

#### 1.3. HTTPS配置

mod\_ssl模块为Apache2服务器添加了一项重要功能—加密通信的能力。

因此，当您的浏览器使用SSL进行通信时，https://前缀将用于浏览器导航栏中统一资源定位器（URL）的开头。

mod\_ssl模块在apache2通用软件包中提供。在终端提示下执行以下命令以启用mod\_ssl模块：**sudoa2enmodssl**

在/etc/apache2/sites available/default-ssl.conf中有一个默认的HTTPS配置文件。为了让Apache2提供HTTPS，还需要证书和密钥文件。默认HTTPS配置将使用ssl证书包生成的证书和密钥。它们适用于测试，但自动生成的证书和密钥应替换为特定于站点或服务器的证书。有关生成密钥和获取证书的信息，请参见第5节“证书”[p.198]

要为HTTPS配置Apache2，请输入以下内容：

**sudoa2ensite默认ssl**

目录/etc/ssl/certs和/etc/ssl/private是默认位置。如果在其他目录中安装证书和密钥，请确保适当更改SSLCertificateFile和SSLCertificateKeyFile。

Apache2现在配置为HTTPS，请重新启动服务以启用新设置：**sudo systemctl重新启动apache2.service**

根据您获得证书的方式，您可能需要在Apache2启动时输入密码短语。

您可以通过键入来访问安全服务器页面https://your\_hostname/url/ 在浏览器地址栏中。

#### 1.4. 共享写入权限

要使多个用户能够写入同一目录，必须向他们共享的组授予写入权限。以下示例将/var/www/html的共享写入权限授予组“网站管理员”。

**sudo chgrp-R webmasters/var/www/html**

**sudofind/var/www/html-type d-execchmod g=rwxs“{}”；sudofind/var/www/html-type f-execchmod g=rw“{}”；**

这些命令递归地将/var/www/html中所有文件和目录的组权限设置为读写并设置用户id。这具有使文件和目录从其各自继承组和权限的效果。许多管理员发现这对于允许多个用户编辑目录树中的文件很有用。

如果必须为每个目录向多个组授予访问权限，请启用访问控制列表（ACL）。

#### 1.5. 工具书类

•Apache2文档[196]包含有关Apache2配置指令的深入信息。另外，请参阅apache2文档包以了解正式的apache2文档。

•有关更多SSL相关信息，请参阅Mod SSL文档[197]网站。

•O&apos;Reilly的Apache Cookbook[198]是完成特定Apache2配置的良好资源。

•对于Ubuntu特定的Apache2问题，请在freenode.net上的#Ubuntu服务器IRC频道中提问[199]。

•通常与PHP和MySQL集成，Apache MySQL PHP Ubuntu Wiki[200]页面是一个很好的资源。

## 2.PHP-脚本语言

PHP是一种适合Web开发的通用脚本语言。PHP脚本可以嵌入到HTML中。本节介绍如何使用Apache2和Linux在Ubuntu系统中安装和配置PHP

MySQL。

本节假设您已经安装并配置了Apache2 Web服务器和MySQL数据库服务器。您可以参考本文档中的Apache2和MySQL部分来分别安装和配置Apache2和MySQL。

#### 2.1. 安装

PHP在Ubuntu Linux中可用。与基本系统中安装的python和perl不同，必须添加PHP。

•要安装PHP和Apache PHP模块，您可以在终端提示符下输入以下命令：

**sudo apt安装php libapache2 mod php**

您可以在终端提示符下运行PHP脚本。要在终端提示符下运行PHP脚本，应安装PHP cli包。要安装php cli，可以在终端提示符下输入以下命令：**sudoapt安装php-cli**

您也可以在不安装apachephp模块的情况下执行PHP脚本。要实现这一点，您应该安装php cgi包。可以在终端提示符下运行以下命令来安装php cgi包：**sudoapt安装php-cgi**

要在PHP中使用MySQL，您应该安装PHP MySQL包。要安装php mysql，可以在终端提示符下输入以下命令：**sudoapt安装php-mysql**

类似地，要在PHP中使用PostgreSQL，您应该安装PHP pgsql包。要安装php pgsql，可以在终端提示符下输入以下命令：**sudoapt安装php-pgsql**

#### 2.2. 配置

如果已安装libapache2 mod php或php cgi包，则可以从web浏览器运行php脚本。如果已安装php cli包，则可以在终端提示符下运行php脚本。

默认情况下，当安装libapache2 mod php时，apache2 Web服务器被配置为运行php脚本。换句话说，当您安装PHP模块时，PHP模块将在Apache Web服务器中启用。

请验证文件/etc/apache2/mods enabled/php7.0.conf和/etc/apache2/mods enabled/php7.0.load是否存在。如果它们不存在，可以使用a2enmod命令启用模块。

一旦安装了与PHP相关的软件包并启用了Apache PHP模块，就应该重新启动Apache2 Web服务器以运行PHP脚本。可以在终端提示下运行以下命令以重新启动web服务器：**sudo systemctl重新启动apache2.service**

#### 2.3. 测试

要验证安装，可以运行以下PHP phpinfo脚本：

<？php phpinfo（）；？>

您可以将内容保存在文件phpinfo.php中，并将其放在

Apache2Web服务器。将浏览器指向http://hostname/phpinfo.php 将显示各种PHP配置参数的值。

#### 2.4. 工具书类

•有关更深入的信息，请参阅php.net[201]文档。

•关于PHP的书籍太多了。O&apos;Reilly的一本好书是学习PHP[202]。PHP Cook Book[203]也不错，但尚未针对PHP7进行更新。

•此外，有关更多信息，请参见Apache MySQL PHP Ubuntu Wiki[204]页面。

## 3.Squid-代理服务器

Squid是一个功能齐全的web代理缓存服务器应用程序，为用户提供代理和缓存服务

超文本传输协议（HTTP）、文件传输协议（FTP）和其他流行的网络协议。

Squid可以实现安全套接字层（SSL）请求的缓存和代理，以及域名服务器（DNS）查找的缓存，并执行透明缓存。Squid还支持多种缓存协议，如Internet缓存协议（ICP）、超文本缓存协议（HTCP）、缓存阵列路由协议（CARP）和Web缓存协调协议（WCCP）。

Squid代理缓存服务器是满足各种代理和缓存服务器需求的优秀解决方案，可从分支机构扩展到企业级网络，同时通过简单网络管理协议（SNMP）提供广泛、精细的访问控制机制和关键参数监控。当选择计算机系统作为许多用户的专用Squid缓存代理服务器时，请确保它配置了大量物理内存，因为Squid会维护内存缓存以提高性能。

#### 3.1. 安装

在终端提示下，输入以下命令以安装Squid服务器：**sudoapt安装squid**

#### 3.2. 配置

通过编辑/etc/Squid/Squid.conf配置文件中包含的指令来配置Squid。

以下示例说明了一些可能会修改以影响Squid服务器行为的指令。有关Squid的更深入配置，请参阅参考资料部分。

在编辑配置文件之前，应复制原始文件并防止其写入，以便将原始设置作为参考，并在必要时重新使用。制作此副本并使用以下命令防止写入：

**sudo cp/etc/squid/squid.conf/etc/squid/squid.conf.original sudo chmod a-w/etc/squid/squid.conf.original**

•要将Squid服务器设置为在TCP端口888而不是默认的TCP端口3128上侦听，请更改http\_端口指令：http\_端口8888

•更改visible\_hostname指令，以便为Squid服务器提供特定的主机名。此主机名不一定必须是计算机的主机名。在本例中，它被设置为weezie

可见的

•使用Squid的访问控制，您可以将Squid代理的互联网服务的使用配置为仅具有特定互联网协议（IP）地址的用户可用。例如，我们将说明用户仅可访问192.168.42.0/24子网：

将以下内容添加到/etc/squid/squid.conf文件的ACL部分底部：ACL fortytwo\_network src 192.168.42.0/24

然后，将以下内容添加到/etc/squid/squid.conf文件的http\_访问部分的顶部：http\_访问允许fortytwo\_网络

•使用Squid出色的访问控制功能，您可以将Squid代理的互联网服务的使用配置为仅在正常工作时间可用。例如，我们将举例说明在周一至周五上午9:00至下午5:00之间运营的企业员工的访问，该企业使用10.1.42.0/24子网络：

将以下内容添加到/etc/squid/squid.conf文件ACL部分的底部：

acl业务网络src 10.1.42.0/24 acl业务时间M T W T F 9:00-17:00

然后，将以下内容添加到/etc/squid/squid.conf文件的http\_访问部分的顶部：http\_访问允许商务网络商务小时

更改/etc/squid/squid.conf文件后，保存该文件并重新启动squid服务器应用程序，以使用在终端提示符下输入的以下命令进行更改：**sudo systemctl重新启动squid.service**

如果以前使用定制的squid3将/var/log/squid3处的假脱机设置为装入点，但保留默认配置，则升级将失败。升级尝试根据需要重命名/移动文件，但无法对活动装入点执行此操作。在这种情况下，请调整挂载点或/etc/squid/squid.conf中的配置，使它们匹配。

如果使用include-config语句从/etc/squid3/的旧路径拉入更多文件，则同样适用。在这些情况下，您应该相应地移动和调整配置。

#### 3.3. 工具书类

Squid网站[205]

Ubuntu Wiki Squid[206]页面。

## 4.RubyonRails

RubyonRails是一个用于开发数据库支持的web应用程序的开源web框架。它针对程序员的可持续生产力进行了优化，因为它允许程序员通过支持约定而不是配置来编写代码。

#### 4.1. 安装

在安装Rails之前，您应该安装Apache和MySQL。要安装Apache软件包，请参阅第1节“HTTPD-apache2web服务器”[p.214]。有关安装MySQL的说明，请参阅第1节“MySQL”[p.233]。

一旦安装了Apache和MySQL软件包，就可以安装RubyonRails软件包了。

要安装Ruby base软件包和Ruby on Rails，可以在终端提示符中输入以下命令：**sudoapt安装导轨**

#### 4.2. 配置

修改/etc/apache2/sites available/000-default.conf配置文件以设置域。

首先要更改的是DocumentRoot指令：

DocumentRoot/path/to/rails/application/public

接下来，将<Directory”/path/to/rails/application/public>指令更改为：

<Directory”/path/to/rails/application/public“>选项索引后跟ymlinks多视图ExecCGI

AllowOverride All Order allow，deny allow from All AddHandler cgi script.cgi

</Directory>

您还应该为Apache启用mod\_重写模块。要启用mod\_重写模块，请在终端提示符中输入以下命令：**sudoa2enmod重写**

最后，您需要将/path/to/rails/application/public和/path/to/rails/application/tmp目录的所有权更改为用于运行Apache进程的用户：

**sudo chown-R www-data:www-data/path/to/rails/application/public sudo chown-R www-data:www-data/path/to/rails/application/tmp**

就这样！现在您已经为Ruby on Rails应用程序准备好了服务器。

#### 4.3. 工具书类

•有关更多信息，请访问Ruby on Rails[207]网站。

•此外，使用Rails进行敏捷开发[208]是一个很好的资源。

•另一个获取更多信息的地方是Ruby on Rails Ubuntu Wiki[209]页面。

## 5.阿帕奇雄猫

ApacheTomcat是一个web容器，允许您为Java servlet和JSP（Java服务器页面）web应用程序提供服务。

Ubuntu支持Tomcat6和7的软件包。Tomcat6是旧版本，Tomcat7是当前版本，其中实现了新功能。两者都被认为是稳定的。本指南将重点介绍Tomcat7，但大多数配置细节对这两个版本都有效。

Ubuntu中的Tomcat包支持两种不同的运行Tomcat的方式。您可以将它们安装为一个典型的唯一的系统范围实例，该实例将在启动时启动，并作为tomcat7（或tomcat6）非特权用户运行。但您也可以部署私有实例，这些实例将使用您自己的用户权限运行，并且您应该自己启动和停止。第二种方法在开发服务器环境中特别有用，因为多个用户需要在他们自己的私有Tomcat实例上进行测试。

#### 5.1. 全系统安装

要安装Tomcat服务器，可以在终端提示符中输入以下命令：**sudoapt安装tomcat7**

这将安装一个Tomcat服务器，其中只有一个默认的根webapp，默认情况下显示一个最小的“ItWorks”页面。

#### 5.2. 配置

Tomcat配置文件可以在/etc/tomcat7中找到。这里只介绍一些常见的配置调整，更多信息请参见Tomcat 7.0文档[210]。

##### 5.2.1. 更改默认端口

默认情况下，Tomcat在端口8080上运行HTTP连接器，在端口8009上运行AJP连接器。您可能希望更改这些默认端口，以避免与系统上的其他应用程序发生冲突。这是通过更改/etc/tomcat7/server.xml中的以下行来完成的：

<Connector port=“8080”protocol=“HTTP/1.1”connectionTimeout=“20000”redirectPort=“8443”/<连接器端口=“8009”协议=“AJP/1.3”重定向端口=“8443”/

##### 5.2.2. 更改使用的JVM

默认情况下，Tomcat最好与OpenJDK JVM一起运行，然后尝试Sun JVM，然后尝试其他一些

JVM。通过在/etc/default/tomcat7中设置JAVA\_HOME，可以强制Tomcat使用特定的JVM：

JAVA\_HOME=/usr/lib/jvm/JAVA-6-sun

##### 5.2.3. 声明用户和角色

用户名、密码和角色（组）可以在Servlet容器中集中定义。这在/etc/tomcat7/tomcat-users.xml文件中完成：

<role rolename=“admin”/><user username=“tomcat”password=“s3cret”roles=“admin”/

#### 5.3. 使用Tomcat标准webapps

Tomcat附带了webapps，您可以安装这些webapps用于文档、管理或演示目的。

##### 5.3.1. Tomcat文档

tomcat7文档包包含Tomcat文档，打包为webapp，默认情况下您可以在http://yourserver:8080/docs. 您可以通过在终端提示符中输入以下命令来安装它：**sudo apt安装tomcat7文档**

##### 5.3.2. Tomcat管理webapps

tomcat7管理包包含两个WebApp，可用于使用web界面管理Tomcat服务器。您可以通过在终端提示符中输入以下命令来安装它们：**sudo-apt安装tomcat7-admin**

第一个是manager webapp，默认情况下您可以在http://yourserver:8080/manager/ html。它主要用于获取服务器状态和重新启动webapps。

默认情况下，对manager应用程序的访问受到保护：您需要在/etc/tomcat7/tomcat-users.xml中定义一个角色为“manager gui”的用户，然后才能访问它。

第二个是主机管理器webapp，默认情况下您可以在http://yourserver:8080/hostmanager/html. 它可用于动态创建虚拟主机。

默认情况下，对host manager应用程序的访问也受到保护：您需要在/etc/tomcat7/tomcat-users.xml中定义一个角色为“admin gui”的用户，然后才能访问它。

出于安全原因，默认情况下，tomcat7用户无法写入/etc/tomcat7目录。这些管理webapps中的某些功能（应用程序部署、虚拟主机创建）需要对该目录进行写访问。如果要使用这些功能，请执行以下操作，为tomcat7组中的用户提供必要的权限：

**sudo chgrp-R tomcat7/etc/tomcat7**

**sudo chmod-R g+w/etc/tomcat7**

##### 5.3.3. Tomcat示例webapps

tomcat7示例包包含两个WebApp，可用于测试或演示servlet和JSP功能，默认情况下，您可以在http://yourserver:8080/examples. 您可以通过在终端提示符中输入以下命令来安装它们：**sudoapt安装tomcat7示例**

#### 5.4. 使用私有实例

Tomcat大量用于开发和测试场景，在这些场景中，使用单个系统范围的实例无法满足单个系统上多个用户的需求。Ubuntu中的Tomcat软件包附带了一些工具，可以帮助您部署自己的面向用户的实例，允许系统上的每个用户在使用系统安装的库的同时运行单独的私有实例（无root权限）。

可以并行运行系统范围的实例和私有实例，只要它们不使用相同的TCP端口。

##### 5.4.1. 安装私有实例支持

通过在终端提示符中输入以下命令，可以安装运行私有实例所需的一切：**sudo apt安装tomcat7用户**5.4.2. 创建私有实例

通过在终端提示符中输入以下命令，可以创建私有实例目录：**tomcat7实例创建我的实例**

这将创建一个新的my instance目录，其中包含所有必要的子目录和脚本。例如，您可以在lib/子目录中安装公共库，并在webapps/子目录中部署webapps。默认情况下不部署任何Web应用程序。

##### 5.4.3. 配置您的私有实例

您将在conf/子目录中找到私有实例的经典Tomcat配置文件。例如，您当然应该编辑conf/server.xml文件来更改私有Tomcat实例使用的默认端口，以避免与可能正在运行的其他实例发生冲突。

##### 5.4.4. 启动/停止您的私有实例

您可以通过在终端提示符中输入以下命令来启动私有实例（假设您的实例位于my instance目录中）：

**我的实例/bin/startup.sh**

您应该检查日志/子目录是否有任何错误。如果您有一个java.net.BindException:Address已在使用<null>：8080错误，则表示您正在使用的端口已被占用，您应该对其进行更改。

您可以通过在终端提示符中输入以下命令来停止实例（假设您的实例位于“我的实例”目录中）：**我的实例/bin/shutdown.sh**

#### 5.5. 工具书类

•有关更多信息，请参阅Apache Tomcat[211]网站。

•Tomcat：权威指南[212]是使用Tomcat构建web应用程序的良好资源。

•有关其他书籍，请参阅Tomcat书籍[213]列表页。

# 第十二章。数据库

Ubuntu提供了两种流行的数据库服务器。他们是：

•MySQL™

•PostgreSQL

它们在主存储库中可用。本节介绍如何安装和配置这些数据库服务器。

## 1.MySQL

MySQL是一种快速、多线程、多用户和健壮的SQL数据库服务器。它适用于任务关键型、重载生产系统以及嵌入大规模部署的软件。

#### 1.1. 安装

要安装MySQL，请在终端提示符下运行以下命令：**sudoapt安装mysql服务器**

一旦安装完成，MySQL服务器将自动启动。您可以从终端提示符运行以下命令来检查MySQL服务器是否正在运行：**sudo netstat-tap | grep mysql**

运行此命令时，应该会看到以下行或类似内容：tcp 0 0 localhost:mysql\*：\*LISTEN 2556/mysqld如果服务器运行不正常，可以键入以下命令来启动它：**sudo systemctl重新启动mysql.service**

#### 1.2. 配置

您可以编辑/etc/mysql/my.cnf文件来配置基本设置——日志文件、端口号等。例如，要将mysql配置为侦听来自网络主机的连接，请将bind address指令更改为服务器的IP地址：

绑定地址=192.168.0.5

用适当的地址替换192.168.0.5。

更改/etc/mysql/my.cnf后，需要重新启动mysql守护程序：**sudo systemctl重新启动mysql.service**

#### 1.3. 数据库引擎

虽然Ubuntu软件包提供的MySQL的默认配置完全是功能性的，性能良好，但在您继续进行之前，您可能需要考虑这些问题。

MySQL的设计允许以不同的方式存储数据。这些方法称为数据库或存储引擎。您会对两个主要引擎感兴趣：InnoDB和MyISAM。存储引擎对最终用户是透明的。MySQL将以不同的方式处理表面下的事情，但无论使用哪个存储引擎，您都将以相同的方式与数据库交互。

每种发动机各有优缺点。

虽然在表级别上混合和匹配数据库引擎是可能的，而且可能是有利的，但这样做会降低性能调整的效率，因为您将在两个引擎之间拆分资源，而不是将它们专用于一个引擎。

•MyISAM是两人中年龄较大的一个。在某些情况下，它可以比InnoDB更快，并且支持只读工作负载。一些web应用程序已经围绕MyISAM进行了调优（尽管这并不意味着它们在InnoDB下会变慢）。MyISAM还支持全文数据类型，允许对大量文本数据进行非常快速的搜索。但是，MyISAM只能锁定整个表进行写入。这意味着一次只能有一个进程更新一个表。任何使用表格缩放的应用程序都可能会遇到阻碍。它还缺少日志记录，这使得数据在崩溃后很难恢复。下面的链接提供了一些关于在生产数据库上使用MyISAM的注意事项[214]。

•InnoDB是一个更现代的数据库引擎，其设计符合ACID[215]，可确保可靠地处理数据库事务。写锁定可以在表中的行级别发生。这意味着一个表上可以同时发生多个更新。数据缓存也在数据库引擎中的内存中处理，允许在更高效的行级别而不是文件块上进行缓存。为了满足ACID合规性，所有事务都独立于主表进行日志记录。这使得数据恢复更加可靠，因为可以检查数据一致性。

从MySQL 5.5开始，InnoDB是默认的引擎，强烈建议您不要使用MyISAM，除非您特别需要该引擎特有的功能。

#### 1.4. 高级配置

##### 1.4.1. 创建优化的my.cnf文件

MySQL的配置文件中有许多参数可以调整，这些参数允许您随着时间的推移提高服务器的性能。对于初始设置，您可能会发现Percona的my.cnf生成工具[216]非常有用。此工具将帮助生成my.cnf文件，该文件将根据您的特定服务器功能和需求进行优化。

*不要*如果已经将数据加载到数据库中，请将现有的my.cnf文件替换为Percona的文件。文件中的一些更改将不兼容，因为它们改变了数据在硬盘上的存储方式，您将无法启动MySQL。如果您确实希望使用它，并且您拥有现有数据，则需要执行mysqldump并重新加载：

mysqldump--所有数据库--例程-u root-p>~/fulldump.sql

这将在创建数据副本之前提示您输入根密码。建议确保在此期间没有其他用户或进程使用数据库。根据数据库中的数据量，这可能需要一些时间。在此过程中，您不会在屏幕上看到任何内容。

完成转储后，关闭MySQL：**sudo systemctl stop mysql.service**

现在备份原始my.cnf文件并替换为新文件：

**sudo cp/etc/mysql/my.cnf/etc/mysql/my.cnf.backup sudo cp/path/to/new/my.cnf/etc/mysql/my.cnf**

然后删除并重新初始化数据库空间，并在重新启动MySQL之前确保所有权正确：

**sudorm-rf/var/lib/mysql/\*sudomysql\u安装\u db**

**sudo chown-R mysql:/var/lib/mysql sudo systemctl start mysql.service**

最后，剩下的就是重新导入数据。为了让我们了解导入过程已经走了多远，您可能会发现“Pipe Viewer”实用程序pv非常有用。下面展示了如何在这种情况下安装和使用pv，但是如果您不想使用它，只需在下面的命令中将pv替换为cat即可。忽略pv产生的任何ETA时间，它们基于处理文件每一行所需的平均时间，但插入速度可能因mysqldumps的不同而有很大差异：

**sudo apt install pv~/fulldump.sql | mysql**

一旦完成，一切都很好！

这不是所有my.cnf更改所必需的。即使在服务器运行时，您可能希望更改以提高性能的大多数变量都是可调整的。与其他方法一样，在进行更改之前，请确保拥有配置文件和数据的良好备份副本。

##### 1.4.2. MySQL调谐器

MySQL Tuner是一个有用的工具，它可以连接到正在运行的MySQL实例，并为如何为您的工作负载进行最佳配置提供建议。服务器运行的时间越长，mysqltuner提供的建议就越好。在生产环境中，在运行该工具之前考虑至少等待24小时。您可以从Ubuntu存储库获取安装mysqltuner：

**sudo apt安装mysqltuner**

然后，在安装后，运行它：**mysqltuner**

等待最终报告。顶部部分提供有关数据库服务器的一般信息，底部部分提供在my.cnf中修改的优化建议。其中大多数都可以在服务器上实时更改，而无需重新启动。请查看官方MySQL文档（参考资料部分中的链接），以了解在生产中要更改的相关变量。以下是来自生产数据库的示例报告的一部分，该报告显示增加查询缓存量可能会带来一些好处：

--------建议------------------------------------------一般建议：

运行“优化表”对表进行碎片整理以获得更好的性能逐渐增加表\u缓存以避免文件描述符限制要调整的变量：

键缓存大小（>1.4G）查询缓存大小（>32M）表缓存大小（>64）

innodb\_缓冲区\_池\_大小（>=22G）

关于调优数据库的最后一点意见：虽然我们可以大致上说某些设置是最好的，但性能可能因应用程序而异。例如，对Wordpress最有效的可能不是对Drupal、Joomla或专有应用程序最有效的。性能取决于查询的类型、索引的使用、数据库设计的效率等等。您可能会发现，花一些时间根据您使用数据库的应用程序来搜索数据库调优技巧是很有用的。一旦超过某一点，所做的任何调整都只会带来微小的改进，您最好改进应用程序，或者通过使用更强大的硬件或添加从属服务器来扩展数据库环境。

#### 1.5. 资源

•有关更多信息，请参见MySQL主页[217]。

•MySQL开发者门户网站提供在线和离线格式的完整文档[218]

•有关一般SQL信息，请参阅Rafe Colburn的《使用SQL特别版》[219]。

•Apache MySQL PHP Ubuntu Wiki[220]页面也有有用的信息。

## 2.PostgreSQL

PostgreSQL是一种对象关系数据库系统，具有传统商业数据库系统的特点，并在下一代DBMS系统中得到了增强。

#### 2.1. 安装

要安装PostgreSQL，请在命令提示符下运行以下命令：**sudoapt安装postgresql**

安装完成后，您应该根据需要配置PostgreSQL server，尽管默认配置是可行的。

#### 2.2. 配置

PostgreSQL支持多种客户端身份验证方法。身份验证方法用于postgres和本地用户，除非另有配置。如果要配置Kerberos等替代方案，请参阅PostgreSQL管理员指南[221]。

下面的讨论假设您希望启用TCP/IP连接并使用MD5方法进行客户端身份验证。postgresql配置文件存储在/etc/postgresql/<version>/main目录中。例如，如果安装PostgreSQL 9.5，则配置文件存储在/etc中/

postgresql/9.5/main目录。

要配置ident身份验证，请将条目添加到/etc/postgresql/9.5/main/pg\_ident.conf文件中。文件中有详细的注释可供您参考。

要使其他计算机能够连接到您的PostgreSQL server，请编辑文件/etc/PostgreSQL/9.5/main/PostgreSQL.conf

找到行#listen\_addresses=&apos;localhost&apos;，并将其更改为：listen\_addresses=&apos;\*&apos;

若要同时允许IPv4和IPv6连接，请将“localhost”替换为“：”

如果您知道自己在做什么，还可以编辑所有其他参数！有关详细信息，请参阅配置文件或PostgreSQL文档。

现在我们可以连接到PostgreSQL server，下一步是为postgres用户设置密码。

在终端提示下运行以下命令以连接到默认的PostgreSQL模板数据库：

**sudo-u postgres psql模板1**

上面的命令以用户postgres的身份连接到PostgreSQL数据库template1。连接到PostgreSQL server后，将出现SQL提示符。您可以在psql提示符下运行以下SQL命令来配置用户postgres的密码。

**使用加密密码“your\_password”更改用户postgres；**

配置密码后，编辑文件/etc/postgresql/9.5/main/pg\_hba.conf，对postgres用户使用MD5身份验证：local all postgres MD5

最后，您应该重新启动PostgreSQL服务以初始化新配置。在终端提示中输入以下内容以重新启动PostgreSQL：**sudo systemctl重启postgresql.service**

以上配置无论如何都不完整。请参阅PostgreSQL管理员指南[222]以配置更多参数。

您可以使用PostgreSQL客户端测试来自其他机器的服务器连接。

**sudo apt安装postgresql客户端psql-h postgres.example.com-U postgres-W**

将域名替换为实际的服务器域名。

#### 2.3. 备份

应定期备份PostgreSQL数据库。有关不同的方法，请参阅PostgreSQL管理员指南[223]。

#### 2.4. 资源

•如上所述，《PostgreSQL管理员指南》[224]是一个极好的资源。该指南也可以在postgresql-doc-9.5包中找到。在终端中执行以下操作以安装软件包：**sudo apt安装postgresql-doc-9.5**

要查看指南，请输入file:///usr/share/doc/postgresql-doc-9.5/html/index.html 进入浏览器的地址栏。

•有关一般SQL信息，请参阅Rafe Colburn的《使用SQL特别版》[225]。

•此外，有关更多信息，请参见PostgreSQL Ubuntu Wiki[226]页面。

# 第十三章。灯的应用

## 1.概述

LAMP安装（Linux+Apache+MySQL+PHP/Perl/Python）是Ubuntu服务器的流行设置。有大量使用LAMP应用程序堆栈编写的开源应用程序。一些流行的LAMP应用程序是Wiki、内容管理系统和管理软件，如phpMyAdmin。

LAMP的一个优点是对不同的数据库、web服务器和脚本语言具有极大的灵活性。MySQL的流行替代品包括PostgreSQL和SQLite。Python、Perl和Ruby也经常被用来代替PHP。而Nginx、Cherokee和Lighttpd可以取代Apache。

最快的入门方法是使用tasksel安装LAMP。Tasksel是一个Debian/Ubuntu工具，它将多个相关软件包作为一个协调的“任务”安装到您的系统上。要安装LAMP服务器，请执行以下操作：

•在终端提示下，输入以下命令：

**sudo tasksel安装lamp服务器**

安装后，您可以通过以下方式安装大多数LAMP应用程序：

•下载包含应用程序源文件的存档。

•通常在web服务器可访问的目录中解压归档文件。

•根据提取源的位置，配置web服务器以提供文件。

•将应用程序配置为连接到数据库。

•运行脚本或浏览应用程序页面，以安装应用程序所需的数据库。

•完成上述步骤或类似步骤后，即可开始使用应用程序。

使用这种方法的一个缺点是应用程序文件没有以标准方式放置在文件系统中，这可能会导致应用程序安装位置的混淆。另一个更大的缺点是更新应用程序。发布新版本时，应用更新需要与安装应用程序相同的过程。

幸运的是，许多LAMP应用程序已经为Ubuntu打包，并且可以以与非LAMP应用程序相同的方式进行安装。但是，根据应用程序的不同，可能需要一些额外的配置和设置步骤。

本节介绍如何安装一些LAMP应用程序。

## 2.莫因·莫因

MoinMoin是一个用Python实现的wiki引擎，基于PikiPiki wiki引擎，并根据

GNU GPL。

#### 2.1. 安装

要安装MoinMoin，请在命令提示符下运行以下命令：**sudoapt安装pythonmoin**

您还应该安装apache2 web服务器。关于安装apache2 web服务器，请参阅第1节“HTTPD-apache2 web服务器”[p.214]小节中的第1.1节“安装”[p.214]小节。

#### 2.2. 配置

要配置第一个wiki应用程序，请运行以下命令集。假设您正在创建一个名为mywiki的wiki：

**cd/usr/share/moin sudo mkdir mywiki sudo cp-R data mywiki sudo cp-R underlay mywiki sudo cp server/moin.cgi mywiki sudo chown-R www data:www data mywiki sudo chmod-R ug+rwX mywiki sudo chmod-R o-rwX mywiki**

现在，您应该配置MoinMoin以查找新的wiki mywiki。要配置MoinMoin，请打开/etc/moin/mywiki.py文件并更改以下行：data\_dir=&apos;/org/mywiki/data&apos;

到

data\_dir=&apos;/usr/share/moin/mywiki/data&apos;

此外，在数据目录选项下面添加数据参考底图目录：数据参考底图目录=&apos;/usr/share/moin/mywiki/underlay&apos;

如果/etc/moin/mywiki.py文件不存在，则应将/usr/share/moin/config/wikifarm/mywiki.py文件复制到/etc/moin/mywiki.py文件，并进行上述更改。

如果您已将您的wiki命名为my\_wiki\_name，则应在/etc/moin/farmconfig.py文件中的“（“mywiki”，r“\*”）行后面插入一行“（“mywiki”，r“\*”）。

配置MoinMoin以查找第一个wiki应用程序mywiki后，应配置apache2并为wiki做好准备。

您应该在“<VirtualHost\*>”标记内的/etc/apache2/sites available/000-default.conf文件中添加以下行：

###moin ScriptAlias/mywiki”/usr/share/moin/mywiki/moin.cgi“alias/moin\_static<version>”/usr/share/moin/htdocs“<Directory/usr/share/moin/htdocs>订单允许，拒绝来自所有目录的允许

###端模

上例中的版本通过运行以下命令确定：

$moin--版本

如果输出显示版本1.9.7，那么第二行应该是：alias/moin\_static197“/usr/share/moin/htdocs”

配置apache2 web服务器并为wiki应用程序做好准备后，应该重新启动它。

可以运行以下命令重新启动apache2 web服务器：**sudo systemctl重新启动apache2.service**

#### 2.3. 验证

您可以通过将web浏览器指向以下URL来验证Wiki应用程序并查看其是否工作：http://localhost/mywiki

有关更多详细信息，请参阅MoinMoin[227]网站。

#### 2.4. 工具书类

•有关更多信息，请参阅moinmoin Wiki[228]。

•另外，请参见Ubuntu Wiki MoinMoin[229]页面。

## 3.数据库管理

phpMyAdmin是专门为管理MySQL服务器而编写的LAMP应用程序。phpMyAdmin用PHP编写，通过web浏览器访问，为数据库管理任务提供了图形界面。

#### 3.1. 安装

在安装phpMyAdmin之前，您需要访问与phpMyAdmin安装在同一主机上的MySQL数据库，或者访问可通过网络访问的主机上的MySQL数据库。有关更多信息，请参见第1节“MySQL”[p.233]。在终端提示中输入：**sudo apt安装phpmyadmin**

在提示下，选择要为phpMyAdmin配置的web服务器。本节的其余部分将使用Apache2作为web服务器。

在浏览器中，转到http://servername/phpmyadmin，将服务器名替换为服务器的实际主机名。在登录页面中，输入root作为用户名，或者输入另一个MySQL用户（如果您有任何设置），然后输入MySQL用户的密码。

登录后，您可以根据需要重置根密码、创建用户、创建/销毁数据库和表等。

#### 3.2. 配置

phpMyAdmin的配置文件位于/etc/phpMyAdmin中。主配置文件是/etc/phpmyadmin/config.inc.php。此文件包含全局应用于phpMyAdmin的配置选项。

要使用phpMyAdmin管理托管在另一台服务器上的MySQL数据库，请在/etc/phpMyAdmin/config.inc.php中调整以下内容：

$cfg[&apos;Servers&apos;][$i][&apos;host&apos;]=&apos;db\_server&apos;；

用实际的远程数据库服务器名称或IP地址替换db\_服务器。另外，请确保phpMyAdmin主机具有访问远程数据库的权限。

配置完成后，从phpMyAdmin注销并重新登录，您应该可以访问新服务器。

config.header.inc.php和config.footer.inc.php文件用于向phpMyAdmin添加HTML页眉和页脚。

另一个重要的配置文件是/etc/phpmyadmin/apache.conf，该文件被符号链接到/etc/apache2/conf available/phpmyadmin.conf，一旦启用，该文件将用于配置apache2以服务于phpmyadmin站点。该文件包含从终端类型加载PHP、目录权限等的指令：

**sudo ln-s/etc/phpmyadmin/apache.conf/etc/apache2/conf available/phpmyadmin.conf sudo a2enconf phpmyadmin.conf sudo systemctl reload apache2.service**

有关配置Apache2的更多信息，请参阅第1节“HTTPD-Apache2 Web服务器”[p.214]。

#### 3.3. 工具书类

•phpMyAdmin文档随软件包一起安装，可通过phpMyAdmin徽标下的phpMyAdmin文档链接（一个带方框的问号）访问。官方文件也可以在phpMyAdmin[230]网站上访问。

•此外，掌握phpMyAdmin[231]也是一个很好的资源。

•第三个资源是phpMyAdmin Ubuntu Wiki[232]页面。

## 4.WordPress

Wordpress是一个博客工具、发布平台和CMS，用PHP实现，并在GNU GPLv2下获得许可。

#### 4.1. 安装

要安装WordPress，请在命令提示符下运行以下命令：sudo apt install WordPress

您还应该安装apache2 web服务器和mysql服务器。关于安装apache2 web服务器，请参阅第1节“HTTPD-apache2 web服务器”[p.214]小节中的第1.1节“安装”[p.214]小节。关于mysql服务器的安装，请参考第1节“mysql”[p.233]小节中的第1.1节“安装”[p.233]小节。

#### 4.2. 配置

要配置第一个WordPress应用程序，请配置apache站点。打开/etc/apache2/sitesavailable/wordpress.conf并写出以下行：

别名/blog/usr/share/wordpress

<Directory/usr/share/wordpress>

选项如下Symlinks AllowOverride Limit选项文件信息

DirectoryIndex.php

命令允许，拒绝

通融

</Directory><Directory/usr/share/wordpress/wp content>

选项如下符号链接

命令允许，拒绝

通融

</Directory>

启用这个新的WordPress站点SudoA2ensite WordPress

配置apache2 web服务器并为WordPress应用程序做好准备后，应该重新启动它。可以运行以下命令重新启动apache2 web服务器：**sudo systemctl重新启动apache2.service**

为了便于多个WordPress安装，此配置文件的名称基于HTTP请求的主机头。这意味着您可以通过简单地将此配置的主机名部分与您的Apache虚拟主机相匹配来获得每个VirtualHost的配置。e、 g./etc/wordpress/config-10.211.55.50.php、/etc/wordpress/config-hostalias1.php等。这些说明假设您可以通过本地主机名（可能通过使用ssh隧道）访问Apache。如果不能，请将/etc/wordpress/configlocalhost.php替换为您的虚拟主机.php的/etc/wordpress/config-NAME。

一旦编写了配置文件，您就可以为每个WordPress数据库实例选择mysql用户名和密码的约定。本文档仅显示一个localhost示例。

现在将WordPress配置为使用mysql数据库。打开/etc/wordpress/config-localhost.php文件并编写以下行：

<？php

定义（&apos;DB\_NAME&apos;，&apos;wordpress&apos;）；定义（&apos;DB\_USER&apos;，&apos;wordpress&apos;）；定义（&apos;DB\_PASSWORD&apos;，&apos;yourspasswordhere&apos;）；定义（&apos;DB\_HOST&apos;，&apos;localhost&apos;）；

定义（&apos;WP\_CONTENT\_DIR&apos;，&apos;/usr/share/wordpress/WP CONTENT&apos;）；？>

现在创建这个mysql数据库。使用mysql命令wordpress.sql打开一个临时文件，并写入以下行：

创建wordpress数据库；授予选择、插入、更新、删除、创建、删除、更改

在wordpress上\*

到wordpress@localhost由“yourpasswordhere”标识；

同花顺特权；执行这些命令。**cat wordpress.sql | sudo mysql--默认的额外文件=/etc/mysql/debian.cnf**

您的新WordPress现在可以通过访问http://localhost/blog/wp-admin/install.php. （或http://NAME\_OF\_YOUR\_VIRTUAL\_HOST/blog/wp-admin/install.php 如果您的服务器没有GUI，并且您正在通过另一台计算机上运行的web浏览器完成WordPress配置。）请填写网站标题、用户名、密码和电子邮件，然后单击安装WordPress。

记下生成的密码（如果适用），然后单击登录密码。你的WordPress现在可以使用了。

#### 4.3. 工具书类

•WordPress.org法典[233]

•Ubuntu Wiki WordPress[234]

# 第十四章。文件服务器

如果一个网络上有多台计算机。在某些时候，您可能需要在他们之间共享文件。在本节中，我们将介绍如何安装和配置FTP、NFS和CUPS。

## 1.FTP服务器

文件传输协议（FTP）是用于在计算机之间下载文件的TCP协议。在过去，它也被用于上传，但由于该方法不使用加密，用户凭证以及以明文传输的数据很容易被截获。因此，如果您在这里寻找安全上传和下载文件的方法，请参阅第6章“远程管理”中有关OpenSSH的部分[p.103]。

FTP在客户机/服务器模型上工作。服务器组件称为FTP守护进程。它持续侦听来自远程客户端的FTP请求。当收到请求时，它管理登录并建立连接。在会话期间，它执行FTP客户端发送的任何命令。

可以通过两种方式管理对FTP服务器的访问：

•匿名

•认证

在匿名模式下，远程客户端可以使用名为“匿名”或“FTP”的默认用户帐户并发送电子邮件地址作为密码来访问FTP服务器。在身份验证模式下，用户必须具有帐户和密码。后一种选择非常不安全，除非在特殊情况下，否则不应使用。如果您希望安全地传输文件，请参阅OpenSSH服务器部分中的SFTP。用户对FTP服务器目录和文件的访问权限取决于为登录时使用的帐户定义的权限。一般来说，FTP守护进程将隐藏FTP服务器的根目录，并将其更改为FTP主目录。这会对远程会话隐藏文件系统的其余部分。

#### 1.1. vsftpd-FTP服务器安装

vsftpd是Ubuntu中可用的FTP守护程序。它易于安装、设置和维护。要安装vsftpd，可以运行以下命令：**sudo apt安装vsftpd**

#### 1.2. 匿名FTP配置

默认情况下，vsftpd未配置为允许匿名下载。如果要启用匿名下载，请通过更改：anonymous\_enable=Yes来编辑/etc/vsftpd.conf

在安装过程中，会创建一个ftp用户，其主目录为/srv/ftp。这是默认的FTP目录。

如果要将此位置更改为/srv/files/ftp（例如），只需在另一个位置创建一个目录并更改ftp用户的主目录：

**sudo mkdir/srv/files/ftp sudo usermod-d/srv/files/ftp**

进行更改后，重新启动vsftpd：**sudo systemctl重新启动vsftpd.service**

最后，将您希望通过匿名FTP提供的任何文件和目录复制到/srv/files/FTP或/srv/FTP（如果您希望使用默认设置）。

#### 1.3. 用户验证的FTP配置

默认情况下，vsftpd配置为对系统用户进行身份验证并允许他们下载文件。如果希望用户能够上载文件，请编辑/etc/vsftpd.conf:write\_enable=YES立即重新启动vsftpd:**sudo systemctl重新启动vsftpd.service**

现在，当系统用户登录到FTP时，他们将从他们的主目录开始，在那里他们可以下载、上载、创建目录等。

同样，默认情况下，不允许匿名用户将文件上载到FTP服务器。要更改此设置，应取消注释以下行，然后重新启动vsftpd:anon\u upload\u enable=YES

启用匿名FTP上载可能会带来极大的安全风险。最好不要在直接从Internet访问的服务器上启用匿名上载。

配置文件由许多配置参数组成。配置文件中提供了有关每个参数的信息。或者，您可以参考手册页man 5 vsftpd.conf了解每个参数的详细信息。

#### 1.4. 保护FTP

/etc/vsftpd.conf中有一些选项可以帮助提高vsftpd的安全性。例如，可以通过取消注释：chroot\u local\u user=YES将用户限制在其主目录中

您还可以将特定的用户列表限制为仅包含其主目录：

chroot\u list\u enable=是

chroot\u list\u文件=/etc/vsftpd.chroot\u list

在取消对上述选项的注释后，创建一个/etc/vsftpd.chroot\_列表，其中包含每行一个用户的列表。然后重新启动vsftpd：

**sudo systemctl重新启动vsftpd.service**

另外，/etc/ftpusers文件是不允许FTP访问的用户列表。默认列表包括root、daemon、nobody等。要禁用其他用户的FTP访问，只需将他们添加到列表中即可。

FTP也可以使用FTPS进行加密。与SFTP不同，FTPS是安全套接字层（SSL）上的FTP。SFTP是通过加密SSH连接进行的类似FTP的会话。一个主要的区别是SFTP的用户需要在系统上有一个shell帐户，而不是一个nologin shell。为所有用户提供shell对于某些环境（例如共享web主机）可能并不理想。但是，可以将此类帐户仅限于SFTP并禁用shell交互。有关更多信息，请参阅OpenSSH服务器部分。

要配置FTP，请编辑/etc/vsftpd.conf，并在底部添加：ssl\_enable=Yes

另外，请注意证书和密钥相关选项：

rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

默认情况下，这些选项设置为ssl证书包提供的证书和密钥。在生产环境中，应使用为特定主机生成的证书和密钥替换这些证书和密钥。有关证书的更多信息，请参见第5节“证书”[p.198]。

现在重新启动vsftpd，非匿名用户将被迫使用FTPS：**sudo systemctl重新启动vsftpd.service**

要允许shell为/usr/sbin/nologin的用户访问FTP，但没有shell访问权限，请编辑/etc/shell添加nologin shell：

#/etc/shell：有效的登录shell

/bin/csh

/垃圾箱/垃圾箱

/usr/bin/es

/usr/bin/ksh

/bin/ksh

/usr/bin/rc

/usr/bin/tcsh

/垃圾箱/垃圾箱

/usr/bin/esh

/垃圾箱/破折号

/bin/bash

/bin/rbash

/usr/bin/screen

/usr/sbin/nologin

这是必要的，因为默认情况下，vsftpd使用PAM进行身份验证，/etc/PAM.d/vsftpd配置文件包含：auth required PAM\_shell.so

shells PAM模块限制对/etc/shells文件中列出的Shell的访问。

大多数流行的FTP客户端可以配置为使用FTP进行连接。lftp命令行FTP客户端也可以使用FTPS。

#### 1.5. 工具书类

•有关更多信息，请参见vsftpd网站[235]。

•有关详细的/etc/vsftpd.conf选项，请参阅vsftpd.conf手册页[236]。

## 2.网络文件系统（NFS）

NFS允许系统通过网络与其他人共享目录和文件。通过使用NFS，用户和程序几乎可以像访问本地文件一样访问远程系统上的文件。

NFS可以提供的一些最显著的好处是：

•本地工作站使用更少的磁盘空间，因为常用数据可以存储在一台机器上，并且其他人仍然可以通过网络访问。

•用户无需在每台网络机器上拥有单独的主目录。主目录可以在NFS服务器上设置并在整个网络中可用。

•存储设备（如软盘、CDROM驱动器和USB拇指驱动器）可供网络上的其他机器使用。这可能会减少整个网络中可移动媒体驱动器的数量。

#### 2.1. 安装

在终端提示下，输入以下命令以安装NFS服务器：**sudoapt安装nfs内核服务器**

#### 2.2. 配置

您可以通过将目录添加到/etc/exports文件来配置要导出的目录。例如：

/ubuntu\*（ro、同步、无根挤压）

/主\*（rw、同步、无根挤压）

您可以将\*替换为其中一种主机名格式。使主机名声明尽可能具体，以便不需要的系统无法访问NFS装载。

要启动NFS服务器，可以在终端提示符下运行以下命令：**sudo systemctl启动nfs-kernel-server.service**

#### 2.3. NFS客户端配置

使用mount命令从另一台计算机装载共享NFS目录，方法是在终端提示符下键入类似于以下内容的命令行：**sudo mount example.hostname.com:/ubuntu/local/ubuntu**

挂载点目录/local/ubuntu必须存在。/local/ubuntu目录中不应有任何文件或子目录。

从另一台机器装载NFS共享的另一种方法是在/etc/fstab文件中添加一行。该行必须说明NFS服务器的主机名、要导出的服务器上的目录以及要装入NFS共享的本地计算机上的目录。

/etc/fstab文件中的行的一般语法如下：example.hostname.com:/ubuntu/local/ubuntunfs rsize=8192、wsize=8192、timeo=14、intr

如果在装载NFS共享时遇到问题，请确保在客户端上安装了NFS公用程序包。要安装nfs common，请在终端提示符下输入以下命令：**sudo-apt安装nfs-common**

#### 2.4. 工具书类

Linux NFS常见问题解答[237]

Ubuntu Wiki NFS Howto[238]

## 3.发起者

*iSCSI*（Internet小型计算机系统接口）是一种允许通过网络传输SCSI命令的协议。通常，iSCSI在SAN（存储区域网络）中实施，以允许服务器访问大量存储的硬盘空间。iSCSI协议将客户端称为启动器，将iSCSI服务器称为目标。

Ubuntu服务器可以配置为iSCSI启动器和目标。本指南提供了用于设置iSCSI启动器的命令和配置选项。假设您的本地网络上已经有一个iSCSI目标，并且具有连接到该目标的相应权限。设置目标的说明因硬件提供商而异，因此请参阅供应商文档以配置特定的iSCSI目标。

#### 3.1. iSCSI启动器安装

要将Ubuntu服务器配置为iSCSI启动器，请安装open iSCSI软件包。在终端中输入：**sudo apt安装开放式iscsi**

#### 3.2. iSCSI启动器配置

安装open iscsi软件包后，编辑/etc/iscsi/iscsid.conf更改以下内容：node.startup=automatic

您可以使用iscsiadm实用程序检查哪些目标可用。在终端中输入以下内容：**sudo iscsiadm-m discovery-t st-p 192.168.0.10**

•确定iscsiadm执行的模式。*-m:*

•指定发现的类型。*-t:*

•选项指示目标IP地址。*-p:*

将示例192.168.0.10更改为网络上的目标IP地址。

如果目标可用，您将看到类似于以下内容的输出：

192.168.0.10:3260,1 iqn.1992-05.com.emc:SL7B9203050000-2

上面的iqn号和IP地址将因硬件而异。

您现在应该能够连接到iSCSI目标，并且根据您的目标设置，您可能需要输入用户凭据。登录到iSCSI节点：

**sudo iscsiadm-m节点--登录**

检查以确保已使用dmesg检测到新磁盘：

**dmesg | grep sd**

[4.322384]sd 2:0:0:0:连接的scsi通用sg1类型0[4.322797]sd 2:0:0:0:[sda]41943040 512字节逻辑块：（21.4 GB/20.0 GiB）

[4.322843]sd 2:0:0:0:[sda]写保护已关闭

[4.322846]sd 2:0:0:0[sda]模式检测：03 00

[4.322896]sd 2:0:0:0:[sda]缓存数据不可用[4.322899]sd 2:0:0:0:[sda]假设驱动器缓存：直写

[4.323230]sd 2:0:0:0:[sda]缓存数据不可用[4.323233]sd 2:0:0:0:[sda]假设驱动器缓存：直写

[4.325312]sda:sda1 sda2<sda5>

[4.325729]sd 2:0:0:0:[sda]缓存数据不可用[4.325732]sd 2:0:0:0:[sda]假设驱动器缓存：直写

[4.325735]sd 2:0:0:0:[sda]连接的SCSI磁盘

[2486.941805]sd 4:0:0:3:连接的scsi通用sg3类型0[2486.952093]sd 4:0:0:3:[sdb]1126400000 512字节逻辑块：（576 GB/537 GiB）

[2486.954195]sd 4:0:0:3:[sdb]写保护已关闭

[2486.954200]sd 4:0:0:3:[sdb]模式检测：8f 00 00 08[2486.954692]sd 4:0:0:3:[sdb]写缓存：禁用，读缓存：启用，不支持DPO或FUA[2486.960577]sdb:sdb1

[2486.964862]sd 4:0:0:3:[sdb]连接的SCSI磁盘

在上面的输出中，sdb是新的iSCSI磁盘。记住这只是一个例子；您在屏幕上看到的输出将有所不同。

接下来，创建一个分区，格式化文件系统，并装载新的iSCSI磁盘。在终端中输入：

**sudo fdisk/dev/sdb n p输入w**

上述命令来自fdisk实用程序内部；有关详细说明，请参阅man fdisk。

此外，cfdisk实用程序有时更便于用户使用。

现在格式化文件系统并将其装载到/srv，例如：

**sudo mkfs.ext4/dev/sdb1 sudo mount/dev/sdb1/srv**

最后，在/etc/fstab中添加一个条目，以便在引导期间装载iSCSI驱动器：

/dev/sdb1/srv ext4默认值，自动，\_netdev0

最好通过重新启动服务器来确保一切正常工作。

#### 3.3. 工具书类

打开iSCSI网站[239]

Debian打开iSCSI页面[240]

## 4.CUPS-打印服务器

Ubuntu打印和打印服务的主要机制是通用UNIX打印系统（CUPS）。此打印系统是一个免费提供的便携式打印层，它已成为大多数Linux发行版中打印的新标准。

CUPS管理打印作业和队列，并使用标准Internet打印协议（IPP）提供网络打印，同时支持从点阵到激光等多种打印机。CUPS还支持PostScript打印机描述（PPD）和网络打印机的自动检测，并具有一个简单的基于web的配置和管理工具。

#### 4.1. 安装

要在Ubuntu计算机上安装CUPS，只需使用sudo和apt命令，并将要安装的软件包作为第一个参数。一个完整的CUPS安装有许多软件包依赖项，但它们可能都在同一命令行中指定。在终端提示下输入以下内容以安装CUPS：**sudo-apt-install-cups**

在使用您的用户密码进行身份验证后，应无误地下载和安装软件包。

安装完成后，CUPS服务器将自动启动。

出于故障排除的目的，您可以通过位于：/var/log/CUPS/error\u log的错误日志文件访问CUPS服务器错误。如果错误日志没有显示足够的信息来解决您遇到的任何问题，那么可以通过将配置文件（下面讨论）中的LogLevel指令更改为“debug”甚至“debug2”（默认值为“info”）来增加CUPS日志的详细性。如果进行了此更改，请记住在解决问题后将其重新更改，以防止日志文件变得过大。

#### 4.2. 配置

通用UNIX打印系统服务器的行为通过文件/etc/cups/cupsd.conf中包含的指令进行配置。CUPS配置文件遵循与Apache HTTP服务器主配置文件相同的语法，因此熟悉编辑Apache配置文件的用户在编辑CUPS配置文件时应该感到轻松。此处将提供一些您可能希望最初更改的设置示例。

在编辑配置文件之前，应复制原始文件并防止其被写入，以便将原始设置作为参考，并在必要时重新使用。

复制/etc/cups/cupsd.conf文件，并使用在终端提示下发出的以下命令防止其写入：

**sudo cp/etc/cups/cupsd.conf/etc/cups/cupsd.conf.original sudo chmod a-w/etc/cups/cupsd.conf.original**

•：要配置CUPS服务器指定管理员的电子邮件地址，只需使用首选文本编辑器编辑/etc/CUPS/cupsd.conf配置文件，并相应地添加或修改ServerAdmin行。例如，如果您是CUPS服务器的管理员，并且您的电子邮件地址为&apos;bjoy@somebigco.com，然后修改ServerAdmin行，使其显示为：**服务器管理员**

服务器管理员bjoy@somebigco.com

•：默认情况下，在Ubuntu上，CUPS服务器安装仅侦听IP地址为127.0.0.1的环回接口。为了指示CUPS服务器侦听实际网络适配器的IP地址，必须通过添加listen指令来指定主机名、IP地址或可选的IP地址/端口配对。例如，如果您的CUPS服务器位于IP地址为192.168.10.250的本地网络上，并且您希望该子网络上的其他系统可以访问该服务器，则您可以编辑/etc/CUPS/cupsd.conf并添加一个Listen指令，例如：**听**

侦听127.0.0.1:631#现有环回侦听

侦听/var/run/cups/cups.sock#现有套接字侦听

监听192.168.10.250:631#监听局域网接口，端口631（IPP）

在上面的示例中，如果您不希望cupsd侦听该接口，而是希望它只侦听局域网（LAN）的以太网接口，则可以注释掉或删除对环回地址（127.0.0.1）的引用。要启用对绑定了特定主机名的所有网络接口（包括环回）的侦听，可以为主机名创建侦听条目，如下所示：

听，苏格拉底，在所有接口上听主机名“苏格拉底”

或者省略Listen指令，改用Port，如中所示：

端口631#监听所有接口上的端口631

有关CUPS服务器配置文件中配置指令的更多示例，请在终端提示符下输入以下命令，以查看相关的系统手册页面：**man cupsd.conf**

无论何时更改/etc/cups/cupsd.conf配置文件，都需要在终端提示符下键入以下命令来重新启动cups服务器：

**sudo systemctl重新启动cups.service**

#### 4.3. 网络界面

可以使用web界面配置和监视CUPS，默认情况下，web界面位于http://localhost:631/admin。web界面可用于执行所有打印机管理任务。

为了通过web界面执行管理任务，必须在服务器上启用根帐户，或者作为lpadmin组中的用户进行身份验证。出于安全原因，CUPS不会对没有密码的用户进行身份验证。

要将用户添加到lpadmin组，请在终端提示符下运行：**sudo usermod-aG lpadmin用户名**

更多文档可在web界面的文档/帮助选项卡中找到。

#### 4.4. 工具书类

杯赛网站[241]

Debian打开iSCSI页面[242]

# 第15章。电子邮件服务

通过网络或互联网从一个人向另一个人发送电子邮件的过程涉及多个系统协同工作。必须正确配置这些系统中的每一个，才能使流程正常工作。发件人使用邮件用户代理（MUA）或电子邮件客户端，通过一个或多个邮件传输代理（MTA）发送邮件，最后一个MTA将邮件传递到邮件传递代理（MDA）以传递到收件人的邮箱，收件人的电子邮件客户端通常通过POP3或IMAP服务器从中检索邮件。

## 1.后缀

Postfix是Ubuntu中默认的邮件传输代理（MTA）。它试图做到快速、易于管理和安全。它与MTA sendmail兼容。本节介绍如何安装和配置postfix。它还解释了如何使用安全连接（用于安全发送电子邮件）将其设置为SMTP服务器。

本指南不包括设置后缀虚拟域，有关虚拟域和其他高级配置的信息，请参阅第1.7.4节“参考”[p.268]。

#### 1.1. 安装

要安装后缀，请运行以下命令：**sudoapt安装后缀**

当安装过程中出现问题时，只需按return键，下一阶段将更详细地完成配置。

#### 1.2. 基本配置

要配置后缀，请运行以下命令：**sudo dpkg重新配置后缀**

将显示用户界面。在每个屏幕上，选择以下值：

•互联网网站

•mail.example.com

•史蒂夫

•mail.example.com、localhost.localdomain、localhost

•没有

•127.0.0.0/8[：：ffff:127.0.0]/104[：：1]/128 192.168.0.0/24

• 0

• +

•所有

将mail.example.com替换为要接收电子邮件的域，将192.168.0.0/24替换为邮件服务器的实际网络和类别范围，将steve替换为适当的用户名。

现在是决定要使用哪种邮箱格式的好时机。默认情况下，Postfix将使用mbox作为邮箱格式。您可以使用postconf命令配置所有后缀参数，而不是直接编辑配置文件。配置参数将存储在/etc/postfix/main.cf文件中。稍后，如果希望重新配置特定参数，可以运行该命令或在文件中手动更改它。

要配置Maildir的邮箱格式，请执行以下操作：

**sudo postconf-e&apos;home\u mailbox=Maildir/&apos;**

这将在/home/username/Maildir中放置新邮件，因此您需要配置邮件传递代理（MDA）以使用相同的路径。

#### 1.3. SMTP身份验证

SMTP-AUTH允许客户端通过身份验证机制（SASL）识别自身。传输层安全性（TLS）应用于加密身份验证过程。一旦通过身份验证，SMTP服务器将允许客户端中继邮件。

1.         使用SASL（Dovecot SASL）为SMTP-AUTH配置后缀：

sudo postconf-e&apos;smtpd\_sasl\_type=dovecot&apos;sudo postconf-e&apos;smtpd\_sasl\_path=private/auth&apos;sudo postconf-e&apos;smtpd\_sasl\_local\_domain=&apos;1

sudo postconf-e&apos;smtpd\u sasl\u security\u options=noanonymous&apos;sudo postconf-e&apos;breaked\u sasl\u auth\u clients=yes&apos;sudo postconf-e&apos;smtpd\u sasl\u auth\u enable=yes&apos;sudo postconf-e&apos;smtpd\u接收方限制=\

允许\u sasl \u认证，允许\u mynetworks，拒绝\u unauth \u destination&apos;

smtpd\_sasl\_路径配置是相对于后缀队列目录的路径。

2.         接下来，生成或获取TLS的数字证书。详情见第5节“证书”[p.198]。此示例还使用证书颁发机构（CA）。有关生成CA证书的信息，请参见第5.5节“证书颁发机构”[p.200]。

通过TLS连接到邮件服务器的MUA需要识别用于TLS的证书。这可以使用来自商业CA的证书或用户手动安装/接受的自签名证书来完成。对于MTA到MTA，未经受影响组织事先同意，不得验证TLS证书。对于MTA到MTA TLS，除非本地策略需要，否则没有理由不使用自签名证书。有关更多详细信息，请参阅第5.3节“创建自签名证书”[p.200]。

3.         获得证书后，配置Postfix为传入和传出邮件提供TLS加密：

sudo postconf-e&apos;smtp\u tls\u security\u level=may&apos;sudo postconf-e&apos;smtpd\u tls\u security\u level=may&apos;sudo postconf-e&apos;smtp\u tls\u note\u starttls\u offer=yes&apos;

sudo postconf-e&apos;smtpd\_tls\_key\_file=/etc/ssl/private/server.key&apos;sudo postconf-e&apos;smtpd\_tls\_cert\_file=/etc/ssl/certs/server.crt&apos;sudo postconf-e&apos;smtpd\_tls\_loglevel=1&apos;sudo postconf-e&apos;smtpd\_tls\_received\_\_头=yes&apos;sudo postconf-e&apos;e&apos;myhostname=mail.example.com&apos;

4.         如果您使用自己的证书颁发机构签署证书，请输入：

**sudo postconf-e&apos;smtpd\_tls\_CAfile=/etc/ssl/certs/cacert.pem&apos;**

同样，有关证书的更多详细信息，请参见第5节“证书”[p.198]。

运行所有命令后，将为SMTP-AUTH配置Postfix，并为TLS加密创建自签名证书。

现在，文件/etc/postfix/main.cf应该如下所示：

#请参阅/usr/share/postfix/main.cf.dist，以获取更完整的注释版本

smtpd\_banner=$myhostname ESMTP$mail\_name（Ubuntu）biff=no

#附加.domain是MUA的工作。追加\点\我的域=否

#取消注释下一行以生成“延迟邮件”警告#延迟\_警告\_时间=4h

myhostname=server1.example.com别名\映射=散列：/etc/aliases别名\数据库=散列：/etc/aliases myorigin=/etc/mailname

mydestination=server1.example.com、localhost.example.com、localhost relayhost=mynetworks=127.0.0.0/8

邮箱\u命令=procmail-a“$EXTENSION”邮箱\u大小\u限制=0收件人\u分隔符=+inet\u接口=所有smtpd\u sasl\u本地\u域=smtpd\u sasl\u身份验证\u启用=是smtpd\u sasl\u安全\u选项=无异常损坏\u sasl\u身份验证\u客户端=是smtpd\u收件人\u限制=

permit\_sasl\_认证，permit\_mynetworks，拒绝(unauth)(destination smtpd)(u tls)(u auth)(u destination smtpd)(u tls)(u auth)only=no smtpd(u tls)u security)level=may smtpd(tls)安全(vel=may smtpd)tls(security)security)level)smtpd(smtpd(cert)cert)cert(smtpd\_tls\_会话\_缓存\_超时=3600s tls\_随机\_源=dev:/dev/uradom

后缀初始配置已完成。运行以下命令以重新启动后缀守护程序：**sudo systemctl重新启动postfix.service**

Postfix支持RFC2554[243]中定义的SMTP-AUTH。它基于SASL[244]。但是，在使用SMTP-AUTH之前，仍然需要设置SASL身份验证。

#### 1.4. 配置SASL

Postfix支持两种SASL实现Cyrus SASL和Dovecot SASL。要启用Dovecot SASL，需要安装Dovecot core软件包。在终端提示中输入以下内容：**sudo apt安装dovecot型芯**

接下来需要编辑/etc/dovecot/conf.d/10-master.conf。更改以下内容：

默认情况下，服务auth{#auth\_socket\_路径指向这个userdb socket

#由dovecot lda、doveadm、可能的imap进程等使用。默认为

#权限使它只能由root用户读取，但您可能需要放宽这些权限

#权限。有权访问此套接字的用户可以获取所有用户名的列表，并获取每个人的userdb查找结果。unix\_listener auth userdb{#mode=0600

#用户=

#组=

}

#后缀smtp验证

unix\_listener/var/spool/postfix/private/auth{mode=0660 user=postfix group=postfix}

为了让Outlook客户端使用SMTP-AUTH，请在/etc/dovecot/conf.d/10-AUTH.conf的“身份验证机制”部分更改以下行：AUTH\_mechaniss=plain

对此：auth\_mechaniss=普通登录

配置好Dovecot后，使用以下命令重新启动：

**sudo systemctl重新启动dovecot.service**

#### 1.5.邮件堆栈传递

为SMTP-AUTH配置Postfix的另一个选项是使用邮件堆栈传递包（以前打包为dovecot Postfix）。此包将安装dovecot并配置Postfix以将其用于SASL身份验证和邮件传递代理（MDA）。

您可能希望也可能不希望在邮件服务器上运行IMAP、IMAPS、POP3或POP3。例如，如果将服务器配置为邮件网关、垃圾邮件/病毒过滤器等。如果是这种情况，则使用上述命令为SMTP-AUTH配置后缀可能比使用邮件堆栈传递更容易。

要安装软件包，请在终端提示符下输入：**sudo apt安装邮件堆栈交付**

您现在应该有一个工作的邮件服务器，但您可能希望进一步自定义一些选项。例如，包使用ssl证书（自签名）包中的证书和密钥，在生产环境中，您应该使用为主机生成的证书和密钥。请参阅第5节“证书”[p.198]更多细节。

拥有主机的自定义证书和密钥后，在/etc/postfix/main.cf中更改postfix的以下选项以匹配新密钥：

smtpd\_tls\_证书文件=#您的证书文件#smtpd\_tls\_密钥文件=#您的密钥文件#

对于/etc/Dovecot/conf.d/10-ssl.conf中的Dovecot：

ssl#U证书=<#您的证书文件#ssl#U密钥=<#您的密钥文件#然后重新启动后缀：**sudo systemctl重新启动postfix.service**

#### 1.6.测试

SMTP-AUTH配置已完成。现在是测试安装程序的时候了。

要查看SMTP-AUTH和TLS是否正常工作，请运行以下命令：

**telnet mail.example.com 25**

建立与postfix邮件服务器的连接后，键入：ehlo mail.example.com

如果您在其他行中看到以下行，那么一切都正常工作。键入quit退出。

250-STARTTLS

250-AUTH普通登录

250-AUTH=普通登录

250 8比特MIME

#### 1.7.故障排除

本节介绍在出现问题时确定原因的一些常用方法。

##### 1.7.1.逃逸chroot

出于安全原因，Ubuntu postfix软件包将默认安装到chroot环境中。这会在故障排除时增加更大的复杂性。

要关闭chroot操作，请在/etc/postfix/master.cf配置文件中找到以下行：

smtp inet n--smtpd并将其修改如下：smtp inet n-n--smtpd

然后，您需要重新启动Postfix以使用新配置。在终端提示中输入：**sudo systemctl重新启动postfix.service**

##### 1.7.2.Smtps

如果需要smtps，请编辑/etc/postfix/master.cf并取消注释以下行：

smtps inet n-----smtpd-o smtpd\_tls\_wrappermode=是

-o smtpd\_sasl\_auth\_enable=yes-o smtpd\_client\_restrictions=permit\_sasl\_authenticated，reject-o milter\_macro\_daemon\_name=origing

##### 1.7.3.日志文件

Postfix将所有日志消息发送到/var/log/mail.log。但是，错误和警告消息有时会在正常日志输出中丢失，因此它们也会分别记录到/var/log/mail.err和/var/log/mail.warn。

要实时查看输入日志的消息，可以使用tail-f命令：**tail-f/var/log/mail.err**

可以增加日志中记录的详细信息量。下面是一些用于增加上述某些区域的日志级别的配置选项。

•要增加TLS活动日志记录，请将smtpd\_TLS\_loglevel选项的值设置为1到4。**sudo postconf-e&apos;smtpd\_tls\_loglevel=4&apos;**

•如果您在从特定域发送或接收邮件时遇到问题，可以将该域添加到debug\_peer\_list参数中。**sudo postconf-e&apos;debug\u peer\u list=problem.domain&apos;**

•您可以通过编辑/etc/Postfix/master.cf并在条目后添加-v来增加任何后缀守护进程的详细程度。例如，编辑smtp条目：smtp unix----smtp-v

需要注意的是，在进行上述日志记录更改之后，需要重新加载后缀进程，以便识别新配置：sudo systemctl reload Postfix.service

•为了增加SASL故障排除时记录的信息量，您可以在/etc/dovecot/conf.d/10-logging.conf中设置以下选项

验证调试=是验证调试密码=是

就像Postfix一样，如果您更改了Dovecot配置，则需要重新加载进程：sudo systemctl reload Dovecot.service。

上面的某些选项可能会大幅增加发送到日志文件的信息量。请记住在更正问题后将日志级别恢复到正常状态。然后重新加载相应的守护程序，使新配置生效。

##### 1.7.4.参考文献

管理Postfix服务器可能是一项非常复杂的任务。在某个时候，您可能需要向Ubuntu社区寻求更有经验的帮助。

在freenode[245]上的#Ubuntu服务器IRC频道是一个请求Postfix帮助并参与Ubuntu服务器社区的好地方。您也可以在其中一个Web论坛[246]上发布消息。

对于深入的后缀信息，Ubuntu开发者强烈推荐：后缀之书[247]。

最后，Postfix[248]网站还提供了关于所有不同配置选项的大量文档。

此外，Ubuntu Wiki后缀[249]页面还有更多信息。

## 2.进出口4

EXIM4是剑桥大学开发的一种用于连接到Internet的UNIX系统上的另一种消息传输代理（MTA）。EXIM可以代替SeNemail安装，尽管EXIM的配置与SeNemail的配置完全不同。

#### 2.1.安装

要安装exim4，请运行以下命令：**sudo apt安装exim4**

#### 2.2.配置

要配置Exim4，请运行以下命令：**sudo dpkg重新配置exim4配置**

将显示用户界面。用户界面允许您配置许多参数。例如，在Exim4中，配置文件被拆分为多个文件。如果您希望将它们放在一个文件中，可以在此用户界面中进行相应配置。

在用户界面中配置的所有参数都存储在/etc/exim4/update-exim4.conf.conf文件中。如果要重新配置，请重新运行配置向导或使用常用编辑器手动编辑此文件。配置后，可以运行以下命令生成主配置文件：**sudo update-exim4.conf**

将生成主配置文件，并将其存储在/var/lib/exim4/config.autogenerated中。

在任何时候，都不应手动编辑主配置文件/var/lib/exim4/config.autogenerated。每次运行updateexim4.conf时，它都会自动更新

您可以运行以下命令来启动Exim4守护进程。**sudo systemctl启动exim4.service**

#### 2.3.SMTP身份验证

本节介绍如何将Exim4配置为在TLS和SASL中使用SMTP-AUTH。

第一步是创建用于TLS的证书。在终端提示符中输入以下内容：

**sudo/usr/share/doc/exim4 base/exim-gencert**

现在需要通过编辑/etc/Exim4/conf.d/main/03\u exim4config\u TLS选项为TLS配置Exim4，添加以下内容：

MAIN\u TLS\u ENABLE=是

接下来，您需要将Exim4配置为使用saslauthd进行身份验证。编辑/etc/Exim4/conf.d/auth/30\_Exim4-config\_示例，并取消注释plain\_saslauthd\_服务器和login\_saslauthd\_服务器部分：

纯文本\u saslauthd\u服务器：驱动程序=纯文本公共\u名称=纯文本

服务器\条件=${if saslauthd{{$auth2}{$auth3}{1}{0}}服务器\设置\ id=$auth2服务器\提示=：.ifndef AUTH \服务器\允许\不允许\密码

服务器广告条件=${if eq{$tls\u cipher}{}{}{}{\*}}.endif{35; login\_saslauthd\_服务器：driver=明文公共\u name=login

server\_prompts=“Username:：：Password:：”#不要通过未加密的连接发送系统密码server\_condition=${if saslauthd{{$auth1}{$auth2}}{1}{0}}}server\_set\_id=$auth1.ifndef AUTH\_server\_允许使用密码

服务器{u播发{u条件=${if eq{$tls\_cipher}{}{}{\*}}.endif

此外，为了使外部邮件客户端能够连接到新的exim服务器，需要使用以下命令将新用户添加到exim中。**sudo/usr/share/doc/exim4 base/examples/exim adduser**

用户应使用以下命令保护新的exim密码文件。

**sudo chown root:Debian exim/etc/exim4/passwd sudo chmod 640/etc/exim4/passwd**

最后，更新Exim4配置并重新启动服务：

**sudo update-exim4.conf**

**sudo systemctl重启exim4.service**

#### 2.4.配置SASL

本节提供了有关配置saslauthd为Exim4提供身份验证的详细信息。

第一步是安装sasl2 bin包。从终端提示符输入以下内容：**sudo-apt安装sasl2-bin**

要配置saslauthd，请编辑/etc/default/saslauthd配置文件并将START=no设置为：

开始=是

接下来，Debian exim用户需要成为sasl组的一部分，以便Exim4使用saslauthd服务：现在启动saslauthd服务：**sudo adduser Debian exim sasl sudo systemctl start saslauthd.service**

Exim4现在使用TLS和SASL身份验证配置SMTP-AUTH。

#### 2.5.参考资料

•更多信息请参见exim.org[250]。

•还有一本Exim4图书[251]可供选择。

•另一个资源是Exim4 Ubuntu Wiki[252]页面。

## 3.Dovecot服务器

Dovecot是一个邮件传递代理，主要考虑安全性。它支持主要的邮箱格式：mbox或Maildir。本节介绍如何将其设置为imap或pop3服务器。

#### 3.1.安装

要安装具有常用pop3和imap功能的基本Dovecot服务器，请在命令提示符下运行以下命令：**sudo apt安装dovecot imapd dovecot-pop3d**

还有其他各种Dovecot模块，如Dovecot sieve（邮件过滤）、Dovecot solr（全文搜索）。。。

#### 3.2.配置

要配置Dovecot，您可以编辑文件/etc/Dovecot/Dovecot.conf及其包含在/etc/Dovecot/conf.d/中的配置文件。默认情况下，所有已安装的协议都将通过/etc/Dovecot/Dovecot.conf中的include指令启用。

！include\_try/usr/share/dovecot/protocols.d/\*.protocol

IMAP和POP3更安全，因为它们使用SSL加密进行连接。基本的自签名SSL证书由软件包SSL cert自动设置，并由/etc/dovecot/conf.d/10ssl.conf中的dovecot使用。

默认情况下，配置了mbox格式，如果需要，您也可以使用maildir。有关更多信息，请访问/etc/dovecot/conf.d//10-mail.conf上的注释。更多好处和详细信息，请访问dovecot网站[253]。

如果您的邮件传输代理（MTA）与您配置的邮箱不同，则应将其配置为将传入邮件传输到选定的邮箱类型。

配置好dovecot后，重新启动dovecot守护程序以测试您的设置：**sudo systemctl重新启动dovecot.service**

如果已启用imap或pop3，也可以尝试使用命令telnet localhost pop3或telnet localhost imap2登录。如果您看到以下类似情况，则说明安装已成功：

bhuvan@rainbow：~$telnet本地主机pop3正在尝试127.0.0.1。。。

已连接到localhost.localdomain。

转义字符为“^]”。

+好的，准备好了。

#### 3.3.Dovecot SSL配置

Dovecot现在自动配置为使用SSL。它使用提供自签名证书的软件包SSL cert。如果要设置自定义证书，可以编辑文件/etc/Dovecot/conf.d/10-SSL.conf并修改以下行（有关详细信息，请参阅第5节“证书”[p.198]）：

ssl\_cert=</etc/dovecot/private/dovecot.pem ssl\_key=</etc/dovecot/private/dovecot.key

您可以从证书颁发机构获得SSL证书，也可以创建自签名SSL证书。请参阅第5节“证书”[p.198]有关如何创建自签名SSL证书的详细信息，请参阅。创建证书后，将有一个密钥文件和一个证书文件，您希望在上面显示的配置中公开该文件。

#### 3.4.电子邮件服务器的防火墙配置

要从另一台计算机访问邮件服务器，必须将防火墙配置为允许通过必要的端口连接到服务器。

•IMAP-143

•IMAPS-993

•POP3-110

•流行音乐-995

#### 3.5.参考资料

•有关更多信息，请参见Dovecot网站[254]。

•此外，Dovecot Ubuntu Wiki[255]页面还有更多详细信息。

## 4.邮递员

Mailman是一个用于管理电子邮件讨论和电子通讯列表的开源程序。许多开源邮件列表（包括所有Ubuntu邮件列表[256]）使用Mailman作为其邮件列表软件。

它功能强大，易于安装和维护。

#### 4.1.安装

Mailman为管理员和用户提供web界面，使用外部邮件服务器发送和接收电子邮件。它与以下邮件服务器完美配合：

•后缀

•进出口银行

•发送邮件

•Qmail

我们将了解如何使用、Apache web服务器以及Postfix或Exim邮件服务器安装和配置Mailman。如果您希望使用其他邮件服务器安装Mailman，请参阅参考资料部分。

您只需要安装一个邮件服务器，Postfix是默认的Ubuntu邮件传输代理。

4.1.1.亚太地区2

要安装apache2，请参阅第1.1节“安装”[p.214]了解详细信息。

##### 4.1.2.后缀

有关安装和配置后缀的说明，请参阅第1节“后缀”[p.262]4.1.3.Exim4

要安装Exim4，请参阅第2节“Exim4”[p.270]。

安装exim4后，配置文件存储在/etc/exim4目录中。在Ubuntu中，默认情况下，exim4配置文件被拆分为不同的文件。您可以通过更改/etc/exim4/update-exim4.conf文件中的以下变量来更改此行为：dc\u use\u split\u config=&apos;true&apos;

##### 4.1.4.邮递员

要安装Mailman，请在终端提示符下运行以下命令：

**sudoapt安装邮递员**

它复制/var/lib/mailman目录中的安装文件。它在/usr/lib/CGI-bin/mailman目录中安装CGI脚本。它创建list linux用户。它创建list linux组。mailman进程将归此用户所有。

#### 4.2.配置

本节假设您已成功安装mailman、apache2和postfix或exim4。现在您只需要配置它们。

##### 4.2.1. Apache2

示例Apache配置文件随Mailman一起提供，位于/etc/Mailman/Apache.conf中。为了让Apache使用配置文件，需要将其复制到/etc/apache2/sites：**sudo cp/etc/mailman/apache.conf/etc/apache2/sites available/mailman.conf**

这将为Mailman管理站点设置一个新的Apache VirtualHost。现在启用新配置并重新启动Apache：

**sudo a2ensite mailman.conf sudo systemctl restart apache2.service**

Mailman使用apache2呈现其CGI脚本。mailman CGI脚本安装在/usr/lib/CGI-bin/mailman目录中。因此，邮递员url将是http://hostname/cgi-bin/mailman/. 如果希望更改此行为，可以更改/etc/apache2/sites available/mailman.conf文件。

##### 4.2.2. 后缀

对于Postfix集成，我们将把domain lists.example.com与邮件列表关联起来。请将lists.example.com替换为您选择的域。

您可以使用postconf命令向/etc/postfix/main.cf添加必要的配置：

**sudo postconf-e&apos;relay\u domains=lists.example.com&apos;sudo postconf-e&apos;transport\u maps=hash:/etc/postfix/transport&apos;sudo postconf-e&apos;mailman\u destination\u recipient\u limit=1&apos;**

在/etc/postfix/master.cf中，仔细检查您是否具有以下传输：

mailman unix-n n--pipe flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py${nexthop}${user}

当邮件发送到列表时，它调用postfix-to-mailman.py脚本。

将domain lists.example.com与带有传输映射的邮递员传输相关联。编辑文件/etc/postfix/transport：

lists.example.com邮递员：

现在，让Postfix通过在终端提示符下输入以下内容来构建交通地图：**sudo邮戳-v/etc/postfix/transport**

然后重新启动Postfix以启用新配置：**sudo systemctl重新启动postfix.service**

##### 4.2.3. Exim4

安装Exim4后，您可以在终端提示符下使用以下命令启动Exim服务器：**sudo systemctl启动exim4.service**

为了使mailman能够使用Exim4，您需要配置Exim4。如前所述，默认情况下，Exim4使用多个不同类型的配置文件。有关详细信息，请参阅进出口银行[257]网站。要运行mailman，我们应该向以下配置类型添加新的配置文件：

•主要

•运输

•路由器

Exim通过对所有这些小配置文件进行排序来创建主配置文件。因此，这些配置文件的顺序非常重要。4.2.4. 主要的

属于main类型的所有配置文件都存储在/etc/exim4/conf.d/main/目录中。

您可以将以下内容添加到名为04\_exim4-config\_mailman的新文件中：

#为你的邮递员安装启动#Home dir——也就是邮递员的前缀#目录。

#在Ubuntu上应该是“/var/lib/mailman”#这通常与~mailman MM\_HOME=/var/lib/mailman相同

#

#Mailman的用户和组应与您的--with mail gid#切换到Mailman的配置脚本相匹配。值通常为“mailman”

MM\_UID=列表

MM\_GID=列表

#

#列表中的域-冒号分隔列表#您可能希望将这些域添加到本地域以及domainlist mm\_Domains=hostname.com#-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

#

#这些值是从上面的值派生出来的，不需要编辑，除非您已经安装了mailman

##邮件包装器脚本MM\_WRAP=MM\_HOME/mail/Mailman的路径

##列表配置文件的路径（在

#验证列表地址）MM\_LISTCHK=MM\_HOME/lists/${lc:：$local\_part}/config.pck

#结束

##### 4.2.5. 运输

属于传输类型的所有配置文件都存储在/etc/exim4/conf.d/transport/目录中。您可以将以下内容添加到名为40\_exim4-config\_mailman的新文件中：

mailman\u transport:driver=pipe command=MM\u WRAP\&apos;${if def:local\u part\u suffix\{${sg{$local\u part\u suffix}{-（\\w+）（\\\+.\*）{\$1}}\

{post}&apos;\$local\u part current\u directory=MM\u HOME\u directory=MM\u HOME user=MM\u UID group=MM\u GID4.2.6. 路由器

属于路由器类型的所有配置文件都存储在/etc/exim4/conf.d/router/目录中。

您可以将以下内容添加到名为101\_exim4-config\_mailman的新文件中：

邮递员路由器：驱动程序=接受

require\_files=MM\_HOME/lists/$local\_part/config.pck local\_part\_suffix\u可选

本地\部分\后缀=-反弹：-反弹+\*：\-确认+\*：-加入：-离开：-所有者：-请求：-管理员传输=邮递员\传输

主配置文件和传输配置文件的顺序可以是任意顺序。但是，路由器配置文件的顺序必须相同。此特定文件必须出现在200\_exim4config\_主文件之前。这两个配置文件包含相同类型的信息。第一个文件优先。有关更多详细信息，请参阅参考资料部分。

##### 4.2.7. 邮递员

安装mailman后，您可以使用以下命令运行它：**sudo systemctl启动mailman.service**

一旦安装了mailman，您应该创建默认邮件列表。运行以下命令以创建邮件列表：

**sudo/usr/sbin/newlist邮递员**

在ubuntu.com上输入运行列表的人的电子邮件地址：bhuvan初始邮递员密码：要完成创建邮件列表，您必须通过添加以下行编辑/etc/alias（或等效）文件，并可能运行“newalias”程序：

##邮递员邮寄名单

邮差：“|/var/lib/mailman/mail/mailman post mailman”邮差管理员：“|/var/lib/mailman/mail/mailman admin mailman”邮差反弹：“|/var/lib/mailman/mail/mailman bounces mailman”邮差确认：“|/var/lib/mailman/mail/mailman确认邮差”邮差加入：“|/var/lib/mailman/mail/mailman加入mailman”mailman离开：“|/var/lib/mailman/mail/mailman离开mailman”mailman所有者：“|/var/lib/mailman/mail/mailman所有者mailman”mailman请求：“|/var/lib/mailman/mail/mailman请求mailman”mailman订阅：“|/var/lib/mailman/mail/mailman订阅mailman”“邮递员退订：“|/var/lib/mailman/mail/mailman退订邮递员”点击回车键通知邮递员所有者。。。

#

我们已配置Postfix或Exim4来识别来自mailman的所有电子邮件。因此，在/etc/alias中创建任何新条目不是强制性的。如果您对配置文件进行了任何更改，请确保在继续下一节之前重新启动这些服务。

Exim4不使用上述别名将邮件转发给Mailman，因为它使用发现方法。要在创建列表时抑制别名，可以在Mailman中添加MTA=None行

配置文件/etc/mailman/mm\_cfg.py。

#### 4.3. 管理

我们假设您有一个默认安装。mailman cgi脚本仍在/usr/lib/cgi-bin/mailman/目录中。Mailman提供了一个基于web的管理工具。要访问此页面，请将浏览器指向以下url：

http://hostname/cgi-bin/mailman/admin

默认邮件列表mailman将出现在此屏幕中。如果单击邮件列表名称，它将询问您的身份验证密码。如果输入正确的密码，您将能够更改此邮件列表的管理设置。您可以使用命令行实用程序（/usr/sbin/newlist）创建新的邮件列表。或者，您可以使用web界面创建新的邮件列表。

#### 4.4. 使用者

Mailman为用户提供了基于web的界面。要访问此页面，请将浏览器指向以下url：

http://hostname/cgi-bin/mailman/listinfo

默认邮件列表mailman将出现在此屏幕中。如果单击邮件列表名称，它将显示订阅表单。您可以输入您的电子邮件地址、姓名（可选）和密码进行订阅。将向您发送电子邮件邀请。您可以按照电子邮件中的说明进行订阅。

#### 4.5. 工具书类

GNU邮递员-安装手册[258]

如何-同时使用Exim4和Mailman 2.1[259]，请参见Mailman Ubuntu Wiki[260]页面。

## 5.邮件过滤

当今电子邮件最大的问题之一是未经请求的批量电子邮件（UBE）问题。这类邮件也称为垃圾邮件，也可能携带病毒和其他形式的恶意软件。根据一些报道，这些信息构成了互联网上所有电子邮件流量的大部分。

本节将介绍Amavisd new、Spamassassin和ClamAV与Postfix邮件传输代理（MTA）的集成。Postfix还可以通过外部内容过滤器检查电子邮件的有效性。这些过滤器有时可以确定邮件是否为垃圾邮件，而无需使用资源密集型应用程序进行处理。两个常见的过滤器是opendkim和python policyd spf。

•Amavisd new是一个包装程序，可以调用任意数量的内容过滤程序进行垃圾邮件检测、防病毒等。

•Spamassassin使用多种机制根据邮件内容过滤电子邮件。

•ClamAV是一款开源防病毒应用程序。

•opendkim为域密钥识别邮件（DKIM）标准实现了Sendmail邮件过滤器（Milter）。

•python policyd spf支持使用后缀进行发送方策略框架（spf）检查。

这就是各部分如何组合在一起：

•Postfix接受电子邮件。

•在这种情况下，消息通过任何外部过滤器opendkim和python policyd spf传递。

•Amavisd new然后处理消息。

•ClamAV用于扫描信息。如果邮件包含病毒，后缀将拒绝邮件。

•Spamassassin将分析干净的邮件，以确定该邮件是否为垃圾邮件。Spamassassin随后将添加X标题行，以允许Amavisd new进一步操作消息。

例如，如果一封邮件的垃圾邮件评分超过50分，则该邮件可以自动从队列中删除，而不必麻烦收件人。另一种处理标记消息的方法是将它们传递给邮件用户代理（MUA），允许用户根据自己的需要处理消息。

#### 5.1. 安装

有关安装和配置后缀的说明，请参见第1节“后缀”[p.262]。

要安装其余的应用程序，请在终端提示符下输入以下内容：

**sudo apt安装amavisd新的spamassassin clamav守护程序sudo apt安装opendkim后缀策略d spf python**

有一些与Spamassassin集成的可选软件包可以更好地检测垃圾邮件：

**sudo apt安装pyzor剃须刀**

除了主要的过滤应用程序外，还需要压缩实用程序来处理一些电子邮件附件：**sudo apt安装arj Cabo lha nomarch pax rar unrar解压缩**

如果未找到某些包，请检查/etc/apt/sources.list中是否启用了多维存储库

如果对文件进行了更改，请确保在再次尝试安装之前运行sudo apt update。

#### 5.2. 配置

现在将所有内容配置为协同工作并过滤电子邮件。

##### 5.2.1. 病毒检测

ClamAV的默认行为将符合我们的需要。有关更多ClamAV配置选项，请查看/etc/ClamAV中的配置文件。

将clamav用户添加到amavis组，以便Amavisd new能够适当访问扫描文件：

**sudo adduser clamav amavis sudo adduser amavis clamav**

##### 5.2.2. 斯帕马萨辛

Spamassassin会自动检测可选组件，并在它们存在时使用它们。这意味着不需要配置pyzor和razor。

编辑/etc/default/spamassassin以激活spamassassin守护进程。将启用的更改=0更改为：

已启用=1

现在启动守护进程：**sudo systemctl启动spamassassin.service**

##### 5.2.3. 阿玛维斯新酒店

首先通过编辑/etc/amavis/conf.d/15content\u filter\u模式在Amavisd new中激活垃圾邮件和防病毒检测：

严格使用；

#您可以修改此文件以通过spamassassin#重新启用垃圾邮件检查，并重新启用防病毒检查。

#

#默认防病毒检查模式#取消对下面两行的注释以启用它

#

@bypass\u virus\u checks\u maps=（\%bypass\u virus\u checks、\@bypass\u virus\u checks\u acl、\$bypass\u virus\u checks\u re）；

#

#默认垃圾邮件检查模式#取消对下面两行的注释以启用它

#

@绕过垃圾邮件检查\u映射=（\%bypass\u垃圾邮件检查，\@bypass\u垃圾邮件检查\u acl，\$bypass\u垃圾邮件检查\u re）；

1; # 确保固定收益

退回垃圾邮件可能是个坏主意，因为回信地址经常是伪造的。默认行为是放弃。这在/etc/amavis/conf.d/20-debian\_defaults中配置，其中$final\_spam\_destiny设置为d\_DISCARD而不是d\_BOUNCE。

此外，您可能需要调整以下选项以将更多邮件标记为垃圾邮件：

$sa\_tag\_level\_deflt=-999；#如果处于或高于该级别，则添加垃圾邮件信息标题

$sa\_tag2\_level\_deflt=6.0；#在该级别添加“检测到垃圾邮件”标题

$sa\_kill\_level\_deflt=21.0；#触发垃圾邮件规避操作

$sa\_dsn\_截止水平=4；#未发送DSN的垃圾邮件级别

如果服务器的主机名与域的MX记录不同，则可能需要手动设置$myhostname选项。此外，如果服务器接收多个域的邮件，则需要自定义@local\u domains\u acl选项。编辑/etc/amavis/conf.d/50-user文件：

$myhostname=&apos;mail.example.com&apos;；

@本地域名acl=（“example.com”、“example.org”）；

如果要覆盖多个域，可以在/etc/amavis/conf.d/50-user中使用以下内容

@局部域acl=qw（.）；

配置后，需要重新启动Amavisd new：

**sudo systemctl重新启动amavis.service**

*5.2.3.1. DKIM白名单*

Amavisd new可以配置为自动将具有有效域密钥的域中的地址列入白名单。

在/etc/amavis/conf.d/40-policy\_banks中有一些预先配置的域。

有多种方法可以配置域的白名单：

•：将“example.com”域中的任何地址列入白名单。*&apos;example.com&apos;=>&apos;WHITELIST&apos;，*

•：将从“example.com”的任何子域中列出具有有效签名的任何地址。*&apos;.example.com&apos;=>“白名单”，*

•：将使用父域example.com签名的“example.com”子域列入白名单。*&apos;.example.com//@example.com&apos;=>“白名单”，*

•：添加具有来自“example.com”的有效签名的地址。这通常用于签署消息的讨论组。*&apos;.//example.com&apos;=>“白名单”，*

一个域也可以有多个白名单配置。编辑文件后，重新启动amavisd new：**sudo systemctl重新启动amavis.service**

在此上下文中，一旦将域添加到白名单中，邮件将不会收到任何防病毒或垃圾邮件过滤。这可能是您希望域的预期行为，也可能不是。

##### 5.2.4. 后缀

对于Postfix集成，请在终端提示中输入以下内容：Next edit/etc/Postfix/master.cf并将以下内容添加到文件末尾：**sudo postconf-e&apos;content\_filter=smtp amavis:[127.0.0.1]：10024&apos;**

smtp amavis unix----2 smtp-o smtp\u数据\u完成\u超时=1200

-o smtp\u发送\u xforward\u命令=是-o禁用\u dns\u查找=是

-o最大使用量=20

127.0.0.1:10025 inet n----smtpd

-o内容过滤器=

-o本地收件人地图=

-o中继\u收件人\u映射=

-o smtpd\_限制\_类=

-o smtpd\_延迟\_拒绝=否-o smtpd\_客户端\_限制=允许\_我的网络，拒绝

-o smtpd\_helo\_限制=

-o smtpd\_发送方\_限制=

-o smtpd\u接收方\u限制=允许\u我的网络，拒绝-o smtpd\u数据\u限制=拒绝\u未经授权\u管道

-o smtpd\_\_\_结束\_\_\_数据\_限制=

-o mynetworks=127.0.0.0/8

-o smtpd\u错误\u睡眠\u时间=0

-o smtpd软件错误限制=1001

-o smtpd硬件错误限制=1000

-o smtpd\客户端\连接\计数\限制=0-o smtpd\客户端\连接\速率\限制=0-o

接收\覆盖\选项=无\标题\正文\检查、无\未知\接收者\检查、无\接收者\检查还将在“皮卡”传输服务的正下方添加以下两行：

-o内容过滤器=

-o接收\覆盖\选项=无\标题\正文\检查

这将防止为报告垃圾邮件而生成的邮件被归类为垃圾邮件。

现在重新启动后缀：**sudo systemctl重新启动postfix.service**

现在已启用带有垃圾邮件和病毒检测的内容过滤。

##### 5.2.5. 阿玛维斯新和斯帕马萨辛

将Amavisd new与Spamassassin集成时，如果您选择通过编辑/etc/Spamassassin/local.cf禁用bayes筛选并使用cron更新夜间规则，则结果可能会导致大量错误消息通过Amavisd new cron作业发送给amavis用户。

有几种方法可以处理这种情况：

•配置MDA以过滤您不希望看到的消息。

•更改/usr/sbin/amavisd新的cronjob以检查是否使用\u bayes 0。例如，编辑/usr/sbin/amavisd new cronjob并将以下内容添加到测试语句之前的顶部：egrep-q“^[\t]\*use\_bayes[\t]\*0”/etc/spamassassin/local.cf&&exit 0

#### 5.3. 测试

首先，测试Amavisd新SMTP是否正在侦听：

telnet本地主机10024正在尝试127.0.0.1。。。

已连接到本地主机。

转义字符为“^]”。220[127.0.0.1]ESMTP amavisd新服务就绪

^]

在通过内容过滤器的邮件标题中，您应该看到：

X级：

X-Virus-Scanned:Debian amavisd新网址example.com X-Spam-Status:No，点击率=-2.3标记以上=-1000.0必需=5.0测试=AWL，BAYES\u 00 X-Spam-Level:

您的输出会有所不同，但重要的是有X-Virus-Scanned和X-Spam-Status条目。

#### 5.4. 故障排除

找出出错原因的最佳方法是检查日志文件。

•有关后缀日志记录的说明，请参阅第1.7节“故障排除”[p.267]一节。

•Amavisd new使用Syslog向/var/log/mail.log发送消息。通过将$log\_level选项添加到/etc/amavis/conf.d/50-user，并将值从1设置为5，可以增加细节的数量。

$log\_level=2；

当Amavisd新日志输出增加时，Spamassassin日志输出也会增加。

•通过编辑/etc/ClamAV/clad.conf并设置以下选项，可以提高ClamAV日志级别：

LogVerbose-true

默认情况下，ClamAV将向/var/log/ClamAV/ClamAV.log发送日志消息。

更改应用程序日志设置后，请记住重新启动服务以使新设置生效。此外，一旦您正在排除故障的问题得到解决，最好将日志设置更改回正常状态。

#### 5.5. 工具书类

有关筛选邮件的详细信息，请参阅以下链接：

•Amavisd新文档[261]

•ClamAV文档[262]和ClamAV维基[263][264]

•Spamasassin Wiki22

•Pyzor主页[265]

•剃须刀主页[266]

•DKIM.org[267]

•Postfix Amavis New[268]

另外，请在freenode上的#ubuntu服务器IRC频道自由提问[269]。

# 第十六章。聊天应用程序

## 1.概述

在本节中，我们将讨论如何安装和配置IRC服务器ircd-irc2。我们还将讨论如何安装和配置Jabber，一个实例消息服务器。

## 2.IRC服务器

Ubuntu存储库有许多Internet中继聊天服务器。本节介绍如何安装和配置原始IRC服务器ircd-irc2。

#### 2.1. 安装

要安装ircd-irc2，请在命令提示符下运行以下命令：**sudo apt安装ircd-irc2**

配置文件存储在/etc/ircd目录中。这些文档位于/usr/share/doc/ircd-irc2目录中。

#### 2.2. 配置

IRC设置可以在配置文件/etc/ircd/ircd.conf中完成。您可以通过编辑以下行在此文件中设置IRC主机名：

M:irc.localhost:：Debian ircd默认配置：：000A

请确保为IRC主机名添加DNS别名。例如，如果您将irc.livecipher.com设置为irc主机名，请确保irc.livecipher.com可在您的域名服务器中解析。IRC主机名不应与主机名相同。

可以通过编辑以下行来配置IRC管理员详细信息：

A：组织机构，IRC部门：守护进程<ircd@example.irc.org>：客户端服务器：：IRCnet:

您应该添加特定的行来配置要侦听的IRC端口列表、配置操作员凭据、配置客户端身份验证等。有关详细信息，请参阅示例配置文件/usr/share/doc/ircd-irc2/ircd.conf.example.gz。

当用户连接到服务器时，可以在/etc/ircd/ircd.motd文件中设置要在IRC客户端中显示的IRC横幅。

对配置文件进行必要更改后，可以使用以下命令重新启动IRC服务器：**sudo systemctl重新启动ircd-irc2.service**

#### 2.3. 工具书类

您可能还想看看Ubuntu存储库中的其他IRC服务器。它包括ircd、ircu和ircd混合。

•有关IRC服务器的更多详细信息，请参阅IRCD常见问题[270]。

## 3.Jabber即时消息服务器

*急促而含混不清地说*流行的即时消息协议是基于XMPP的，XMPP是即时消息的开放标准，被许多流行的应用程序使用。本节介绍如何在本地局域网上设置Jabberd 2服务器。此配置还可适用于通过互联网向用户提供消息传递服务。

#### 3.1. 安装

要安装jabberd2，请在终端中输入：**sudo apt安装jabberd2**

#### 3.2. 配置

几个XML配置文件将用于为Berkeley DB用户身份验证配置jabberd2。

这是一种非常简单的身份验证形式。但是，jabberd2可以配置为使用LDAP、MySQL、PostgreSQL等进行用户身份验证。

首先，编辑/etc/jabberd2/sm.xml：

<id>jabber.example.com</id>

将jabber.example.com替换为服务器的主机名或其他id。

现在在<storage>部分将<driver>更改为：

<driver>db</driver>

接下来，在<local>部分中编辑/etc/jabberd2/c2s.xml更改：

<id>jabber.example.com</id>

在<authreg>部分中，将<module>部分调整为：

<module>db</module>

最后，重新启动jabberd2以启用新设置：**sudo systemctl重启jabberd2.service**

您现在应该能够使用像Pidgin这样的Jabber客户端连接到服务器。

对用户数据使用Berkeley DB的优点是，配置后不需要额外维护。如果您需要更多地控制用户帐户和凭据，建议使用另一种身份验证方法。

#### 3.3. 工具书类

•Jabberd2网站[271]包含有关配置Jabberd2的更多详细信息。

•有关更多认证选项，请参阅Jabberd2安装指南[272]。

•此外，设置Jabber服务器Ubuntu Wiki[273]页面还有更多信息。

# 第十七章。版本控制系统

版本控制是管理信息更改的艺术。长期以来，它一直是程序员的关键工具，他们通常会花时间对软件进行一些小的更改，然后在第二天撤销这些更改。但是版本控制软件的实用性远远超出了软件开发领域的范围。无论您在哪里可以找到使用计算机管理经常更改的信息的人，都有进行版本控制的空间。

## 1.集市

Bazaar是一个新的版本控制系统，由Ubuntu背后的商业公司Canonical赞助。与只支持中央存储库模型的Subversion和CVS不同，Bazaar还支持分布式版本控制，使人们能够更高效地协作。特别是，Bazaar旨在最大限度地提高社区对开源项目的参与程度。

#### 1.1. 安装

在终端提示下，输入以下命令以安装bzr：**sudoapt安装bzr**

#### 1.2. 配置

要向bzr自我介绍，请使用以下whoami命令：

**$bzr whoami&apos;Joe Doe<Joe。doe@gmail.com>&apos;**

#### 1.3. 学习集市

Bazaar附带了捆绑文档，默认情况下安装在/usr/share/doc/bzr/html中。本教程是一个很好的起点。bzr命令还附带内置帮助：

**$bzr帮助**

要了解有关foo命令的更多信息，请执行以下操作：

**$bzr帮助foo**

#### 1.4. 启动板集成

Bazaar作为一个独立的系统非常有用，但它与Launchpad[274]有很好的可选集成，Launchpad是Canonical和更广泛的开源社区用来管理和扩展Ubuntu本身的协作开发系统。有关如何将Bazaar与Launchpad结合使用以协作开发开源项目的信息，请参阅http://bazaar-vcs.org/LaunchpadIntegration[275].

## 2.吉特

Git是一个开源分布式版本控制系统，最初由Linus Torvalds开发，用于支持linux内核的开发。每个Git工作目录都是一个完整的存储库，具有完整的历史记录和完整的版本跟踪功能，不依赖于网络访问或中央服务器。

#### 2.1. 安装

git版本控制系统是通过以下命令安装的**sudoapt安装git**

#### 2.2. 配置

每个git用户都应该首先通过运行以下两个命令向git介绍自己：

**git config--global user.email“you@example.comgit config--global user.name“您的名字”**

#### 2.3. 基本用法

以上内容已经足以以分布式和安全的方式使用git，前提是用户可以通过SSH访问承担服务器角色的机器。在服务器计算机上，可以通过以下方法创建新存储库：**git init—裸/path/to/repository**

这将创建一个裸存储库，不能直接用于编辑文件。如果您希望在服务器上拥有存储库内容的工作副本，请使用--bare选项。

然后，具有SSH访问权的任何客户端都可以通过以下方式克隆存储库：**git克隆username@hostname：/path/to/repository**

克隆到客户端计算机后，客户端可以编辑文件，然后提交并与以下用户共享：

**cd/path/to/repository#（编辑一些文件**

**git commit-a#将所有更改提交到存储库的本地版本git push origin master#将更改推送到存储库的服务器版本**

#### 2.4.安装gitolite服务器

虽然上述内容足以创建、克隆和编辑存储库，但希望在服务器上安装git的用户很可能希望git像更传统的源代码管理服务器一样工作，具有多个用户和访问权限管理。建议的解决方案是使用以下命令安装gitolite：

**sudo apt安装gitolite**

#### 2.5.Gitolite配置

gitolite服务器的配置与类Unix系统上的大多数其他服务器略有不同。gitolite将其配置存储在git存储库中，而不是/etc/中的传统配置文件。因此，配置新安装的第一步是允许访问配置存储库。

首先，让我们为gitolite创建一个用户，作为用户访问。

**sudoadduser--system--shell/bin/bash--group--disabled password--home/home/git git**

现在我们想让gitolite知道存储库管理员的公共SSH密钥。这假设当前用户是存储库管理员。如果您尚未配置SSH密钥，请参阅第1.4节，

*“SSH密钥”[第105页]***cp~/.ssh/id\_rsa.pub/tmp/$（whoami.pub）**

让我们切换到git用户并将管理员的密钥导入gitolite。

**sudo su-git gl setup/tmp/\*.pub**

Gitolite将允许您在安装过程中对其配置文件进行初始更改。您现在可以从管理员用户（您导入了其公共SSH密钥的用户）克隆和修改Gitolite配置存储库。切换回该用户，然后克隆配置存储库：

**出口**

**git克隆git@$IP\_地址：gitolite-admin.git cd gitolite admin**

gitolite admin包含两个子目录，“conf”和“keydir”。配置文件位于conf dir中，keydir目录包含用户的公共SSH密钥列表。

#### 2.6.管理gitolite用户和存储库

向gitolite添加新用户很简单：只需获取他们的公共SSH密钥并将其添加到keydir目录，如下所示

$DESIRED\_USER\_NAME.pub。请注意，gitolite用户名不必与系统用户名匹配-它们仅在gitolite配置文件中用于管理访问控制。类似地，通过删除用户的公钥文件来删除用户。每次更改后，不要忘了将更改提交到git，并将更改推回服务器th

**git提交-git推送源主机**

存储库是通过编辑conf/gitolite.conf文件来管理的。语法是空格分隔的，只指定存储库列表和一些访问规则。下面是一个默认示例

repo gitolite admin RW+=admin R=alice

回购项目1 RW+=alice

RW=bob

R=丹尼斯

#### 2.7.使用您的服务器

要使用新创建的服务器，用户必须让gitolite管理员将他们的公钥导入gitolite配置存储库，然后他们可以使用以下命令访问他们有权访问的任何项目：**git克隆git@$SERVER\u IP:$PROJECT\u NAME.git**

或者将服务器的项目添加为现有git存储库的远程项目：**git远程添加gitolite git@$SERVER\u IP:$PROJECT\u NAME.git**

## 3.颠覆

Subversion是一个开源版本控制系统。使用Subversion，您可以记录源文件和文档的历史记录。它管理随时间变化的文件和目录。一个文件树被放置到一个中央存储库中。存储库与普通文件服务器非常相似，只是它记住对文件和directori所做的每一次更改锿。

#### 3.1.安装

若要使用HTTP协议访问Subversion存储库，必须安装和配置web服务器。Apache2已被证明可与Subversion一起使用。请参阅Apache2部分中的HTTP小节以安装和配置Apache2。若要使用HTTPS协议访问Subversion存储库，必须安装和配置数字证书请参阅Apache2部分中的HTTPS小节来安装和配置数字证书。

要安装Subversion，请从终端提示符运行以下命令：**sudo apt安装subversion apache2 libapache2 svn**

#### 3.2.服务器配置

本步骤假设您已在系统上安装上述软件包。本节介绍如何创建Subversion存储库并访问项目。

##### 3.2.1.创建Subversion存储库

可以在终端提示符下使用以下命令创建Subversion存储库：**svnadmin创建/path/to/repos/project**

##### 3.2.2.导入文件

创建存储库后，可以将文件导入存储库。若要导入目录，请在终端提示符下输入以下内容：**svn导入/path/to/import/directoryfile:///path/to/repos/project**

#### 3.3.访问方法

Subversion存储库可以通过许多不同的方法进行访问（签出）——在本地磁盘上，或者通过各种网络协议。但是，存储库位置始终是URL。该表描述了不同的URL方案如何映射到可用的访问方法。

##### **表17.1.访问方法**

|  |  |
| --- | --- |
| **模式** | **存取方法** |
| 文件：// | 直接访问存储库（在本地磁盘上） |
| http:// | 通过WebDAV协议访问支持Subversion的Apache2 web服务器 |
| https:// | 与http:///相同，但使用SSL加密 |
| svn：// | 通过自定义协议访问SVN服务服务器 |
| svn+ssh：// | 与svn:///相同，但通过SSH隧道 |

在本节中，我们将了解如何为所有这些访问方法配置Subversion。在这里，我们将介绍基础知识。有关更高级的用法详细信息，请参阅svn书籍[276]。

###### 3.3.1.直接访问存储库（文件：//）

这是所有访问方法中最简单的一种。它不需要运行任何Subversion服务器进程。此访问方法用于从同一台计算机访问Subversion。在终端提示下输入的命令语法如下：或**svn公司file:///path/to/repos/project svn公司file://localhost/path/to/repos/project**

如果未指定主机名，则有三个正斜杠（//），即协议（本例中为文件）的两个正斜杠加上路径中的前斜杠。如果指定主机名，则必须使用两个正斜杠（//）。

存储库权限取决于文件系统权限。如果用户具有读/写权限，他可以从存储库签出并提交到存储库。

###### 3.3.2.通过WebDAV协议访问（http://）

要通过WebDAV协议访问Subversion存储库，必须配置Apache 2 web服务器。请在/etc/apache2/sites available/000-default.conf或其他VirtualHost文件中的<VirtualHost>和<VirtualHost>元素之间添加以下代码段：

<Location/svn>

DAV svn SVNParentPath/path/to/repos AuthType Basic

AuthName“您的存储库名称”AuthUserFile/etc/subversion/passwd

需要有效用户

</Location>

上面的配置代码段假设Subversion存储库是使用svnadmin命令在/path/to/repos目录下创建的，并且HTTP用户对文件具有足够的访问权限（请参见下文）。可以使用http://hostname/svn/repos\_name 网址。

像上面那样更改apache配置需要使用以下命令sudo systemctl reload apache2.service重新加载服务

要通过HTTP将文件导入或提交到Subversion存储库，存储库应由HTTP用户拥有。在Ubuntu系统中，HTTP用户是www data。要更改存储库文件的所有权，请在终端提示符下输入以下命令：sudo chown-R www data:www data/path/To/repos

通过将存储库的所有权更改为www数据，您将无法以www数据以外的任何用户身份运行svn import file:///命令将文件导入或提交到存储库中。

接下来，必须创建包含用户身份验证详细信息的/etc/subversion/passwd文件。要创建文件，请在命令提示符下发出以下命令（这将创建文件并添加第一个用户）：

**sudo htpasswd-c/etc/subversion/passwd用户名**

若要添加其他用户，请忽略“-c”选项，因为此选项将替换旧文件。请改用此表单：**sudo htpasswd/etc/subversion/passwd用户名**

此命令将提示您输入密码。输入密码后，将添加用户。现在，要访问存储库，可以运行以下命令：**svn公司http://servername/svn**

密码以明文形式传输。如果您担心密码被窥探，建议您使用SSL加密。有关详细信息，请参阅下一节。

###### 3.3.3.通过带有SSL加密的WebDAV协议进行访问（https://）

使用SSL加密（https://）通过WebDAV协议访问Subversion存储库与http://类似，只是您必须在Apache2 web服务器中安装和配置数字证书。若要将SSL用于

Subversion将上述Apache2配置添加到/etc/Apache2/sites available/default-ssl.conf。

有关使用SSL设置Apache2的更多信息，请参阅第1.3节“HTTPS配置”[p.219]。

您可以安装由签名机构颁发的数字证书。或者，您可以安装自己的自签名证书。

此步骤假设您已在Apache 2 web服务器中安装并配置了数字证书。现在，要访问Subversion存储库，请参阅上一节！访问方法完全相同，但协议不同。您必须使用https://访问Subversion存储库。

###### 3.3.4.通过自定义协议访问（svn://）

创建Subversion存储库后，您可以配置访问控制。您可以编辑/path/to/repos/project/conf/svnserve.conf文件来配置访问控制。例如，要设置身份验证，您可以取消注释配置文件中的以下行：

#[一般]

#密码db=passwd

取消对上述行的注释后，您可以在passwd文件中维护用户列表。因此，在同一目录中编辑文件passwd并添加新用户。语法如下：username=password

有关更多详细信息，请参阅该文件。

现在，要通过svn://自定义协议从同一台机器或不同的机器访问Subversion，可以使用svnserve命令运行svnserver。语法如下：

$svnserve-d--前景-r/path/to/repos

#-d——守护程序模式#——前台——在前台运行（对调试有用）

#-r--要服务的目录的根目录

有关更多使用详情，请参阅：

$SVN服务--帮助

运行此命令后，Subversion将在默认端口（3690）上开始侦听。若要访问项目存储库，必须从终端提示符运行以下命令：**svn公司svn://hostname/project 项目--用户名用户名称**

根据服务器配置，它会提示输入密码。一旦您通过身份验证，它会从Subversion存储库中签出代码。要使项目存储库与本地副本同步，您可以运行update子命令。在终端提示下输入的命令语法如下：**cd项目目录；svn更新**

有关使用每个Subversion子命令的详细信息，请参阅手册。例如，要了解有关co（签出）命令的详细信息，请在终端提示符下运行以下命令：

**svn公司帮助**

###### 3.3.5.使用SSH加密通过自定义协议进行访问（svn+SSH://）

配置和服务器过程与svn://方法中的过程相同。有关详细信息，请参阅上一节。此步骤假设您已遵循上述步骤并使用svnserve命令启动Subversion服务器。

还假定ssh服务器正在该计算机上运行，并且允许传入连接。要确认，请尝试使用ssh登录到该计算机。如果可以登录，则一切正常。如果无法登录，请在继续之前解决该问题。

svn+ssh://协议用于使用SSL加密访问Subversion存储库。数据传输使用此方法加密。要访问项目存储库（例如签出），必须使用以下命令语法：svn co svn+ssh://ssh\_username@主机名/path/to/repos/project

必须使用完整路径（/path/to/repos/project）来使用此访问方法访问Subversion存储库。

根据服务器配置，它会提示输入密码。您必须输入用于通过ssh登录的密码。

一旦您通过身份验证，它将从Subversion存储库中检出代码。

## 4.参考资料

•集市主页[277]

•发射台[278]

•Git主页[279]

•硅钙石[280]

•Subversion主页[281]

•颠覆书籍[282]

•Easy Bazaar Ubuntu Wiki页面[283]•Ubuntu Wiki颠覆页面[284]

# 第18章桑巴舞

计算机网络通常由不同的系统组成，虽然操作一个完全由Ubuntu桌面和服务器计算机组成的网络肯定会很有趣，但一些网络环境必须由Ubuntu和Microsoft®Windows®系统组成，两者协调工作。Ubuntu服务器指南的这一部分介绍了一些原则d用于配置Ubuntu服务器以与Windows计算机共享网络资源的工具。

## 1.导言

成功地将Ubuntu系统与Windows客户机联网需要提供Windows环境中常见的服务并与之集成。此类服务有助于共享有关网络中涉及的计算机和用户的数据和信息，可分为三大类功能：

• . 使用服务器消息块（SMB）协议促进整个网络中的文件、文件夹、卷共享和打印机共享。**文件和打印机共享服务**

• . 使用轻量级目录访问协议（LDAP）和Microsoft Active Directory®等技术共享有关计算机和网络用户的重要信息。**目录服务**

• . 使用文件权限、组策略和Kerberos身份验证服务等原则和技术，建立计算机或网络用户的身份，并确定计算机或用户有权访问的信息。**身份验证和访问**

幸运的是，您的Ubuntu系统可以为Windows客户端提供所有这些功能，并在它们之间共享网络资源。Ubuntu系统用于Windows网络的主要软件之一是SMB服务器应用程序和工具的Samba套件。

Ubuntu服务器指南的这一部分将介绍一些常见的Samba用例，以及如何安装和配置必要的软件包。有关Samba的更多详细文档和信息，请访问Samba网站[285]。

## 2.文件服务器

将Ubuntu和Windows计算机联网的最常见方法之一是将Samba配置为文件服务器。本节介绍如何设置Samba服务器以与Windows客户端共享文件。

服务器将配置为与网络上的任何客户端共享文件，而无需提示输入密码。如果您的环境需要更严格的访问控制，请参阅第4节“保护文件和打印服务器”[p.312]。

#### 2.1. 安装

第一步是安装samba包。在终端提示中输入：**sudoapt安装samba**

这就是它的全部；现在，您可以将Samba配置为共享文件了。

#### 2.2. 配置

主Samba配置文件位于/etc/Samba/smb.conf中。默认配置文件有大量注释，用于记录各种配置指令。

并非所有可用选项都包含在默认配置文件中。有关更多详细信息，请参阅smb.conf手册页或Samba HOWTO集合[286]。

1.         首先，在/etc/samba/smb.conf的[global]部分编辑以下键/值对：

工作组=示例。。。安全性=用户

安全参数在[global]部分的较低位置，默认情况下会被注释。另外，更改示例以更好地匹配您的环境。

2.         在文件底部创建一个新部分，或取消注释其中一个示例，以便共享目录：

[分享]

comment=Ubuntu文件服务器共享路径=/srv/samba/Share-browsable=yes-guest-ok=yes-read-only=no-create-mask=0755

•股份的简短说明。调整以适应你的需要。*评论：*

•要共享的目录的路径。*路径：*

本例使用/srv/samba/sharename，因为根据文件系统层次结构标准（FHS），/srv[287]是应该提供站点特定数据的地方。从技术上讲，只要权限正确，Samba共享可以放在文件系统的任何位置，但建议遵守标准。

•使Windows客户端能够使用Windows资源管理器浏览共享目录。*可浏览：*

•允许客户端在不提供密码的情况下连接到共享。*嘉宾ok：*

•确定共享是只读还是授予写入权限。如本例所示，仅当值为“否”时才允许写入权限。如果该值为“是”，则对共享的访问权限为只读。*只读：*

•确定创建新文件时将具有的权限。*创建掩码：*

3.         现在Samba已经配置好，需要创建目录并更改权限。从终端输入：

**sudo mkdir-p/srv/samba/share sudo chown nobody:nogroup/srv/samba/share/**

p开关告诉mkdir创建整个目录树（如果它不存在）。

4.         最后，重新启动samba服务以启用新配置：

**sudo systemctl重新启动smbd.service nmbd.service**

同样，上述配置提供了对本地网络上任何客户端的所有访问权限。有关更安全的配置，请参阅第4节“保护文件和打印服务器”[p.312]。

从Windows客户端，您现在应该能够浏览到Ubuntu文件服务器并查看共享目录。如果您的客户端没有自动显示您的共享，请尝试在Windows资源管理器窗口中通过其IP地址访问服务器，例如\\192.168.1.1。要检查一切是否正常，请尝试从Windows创建目录。

要创建其他共享，只需在/etc/samba/smb.conf中创建新的[dir]部分，然后重新启动samba。只需确保您想要共享的目录确实存在并且权限正确即可。

名为“[share]”的文件共享和路径/srv/samba/share只是示例。调整共享名和路径名以适应您的环境。最好以文件系统上的目录命名共享。另一个例子是共享名[qa]，路径为/srv/samba/qa。

#### 2.3. 资源

•有关深入的Samba配置，请参阅Samba HOWTO集合[288]

•指南也有印刷版[289]。

•O&apos;Reilly使用Samba[290]是另一个很好的参考。

•Ubuntu Wiki Samba[291]页面。

## 3.打印服务器

Samba的另一个常见用途是将其配置为在Ubuntu服务器上共享本地或通过网络安装的打印机。与第2节“文件服务器”[p.307]类似，本节将配置Samba，以允许本地网络上的任何客户端使用已安装的打印机，而无需提示输入用户名和密码。

有关更安全的配置，请参阅第4节“保护文件和打印服务器”[p.312]。

#### 3.1. 安装

在安装和配置Samba之前，最好已经安装了一个工作CUPS。有关详细信息，请参见第4节“CUPS-打印服务器”[p.258]。

要安装samba软件包，请从终端输入：**sudoapt安装samba**

#### 3.2. 配置

安装samba后，编辑/etc/samba/smb.conf。将“工作组”属性更改为适合您的网络的属性，并将“安全性”更改为“用户”：

工作组=示例。。。安全性=用户

在[printers]部分，将guest ok选项更改为yes：

可浏览=是客人确定=是

编辑smb.conf后重新启动Samba：**sudo systemctl重新启动smbd.service nmbd.service**

默认的Samba配置将自动共享安装的所有打印机。只需在Windows客户端本地安装打印机即可。

#### 3.3. 资源

•有关深入的Samba配置，请参阅Samba HOWTO集合[292]

•指南也有印刷版[293]。

•O&apos;Reilly使用Samba[294]是另一个很好的参考。

•此外，有关配置CUPS的更多信息，请参见CUPS网站[295][296]。

•Ubuntu Wiki Samba 12页。

## 4.保护文件和打印服务器的安全

#### 4.1. Samba安全模式

通用Internet文件系统（CIFS）网络协议有两个安全级别：用户级别和共享级别。Samba的安全模式实现允许更大的灵活性，提供了四种实现用户级安全的方法和一种实现共享级安全的方法：

•要求客户端提供用户名和密码以连接到共享。Samba用户帐户与系统帐户是分开的，但是libpam winbind包将与Samba用户数据库同步系统用户和密码。*安全性=用户：*

•此模式允许Samba服务器在Windows客户端中显示为主域控制器（PDC）、备份域控制器（BDC）或域成员服务器（DMS）。更多信息，请参见第5节“作为域控制器”[p.317]。*安全性=域：*

•允许Samba服务器作为本机成员加入Active Directory域。有关详细信息，请参见第6节“Active Directory集成”[p.321]。*安全性=广告：*

•此模式是在Samba成为成员服务器之前遗留下来的，由于某些安全问题，不应使用此模式。有关更多详细信息，请参阅Samba指南的服务器安全[297]部分。*安全性=服务器：*

•允许客户端连接到共享，而无需提供用户名和密码。*安全=共享：*

您选择的安全模式将取决于您的环境以及您需要Samba服务器完成的任务。

#### 4.2. 安全性=用户

本节将从第2节“文件服务器”[p.307]和第3节“打印服务器”[p.310]重新配置Samba文件和打印服务器，以要求身份验证。

首先，安装libpam winbind包，该包将系统用户同步到Samba用户数据库：**sudo-apt安装libpam-winbind**

如果在安装过程中选择Samba服务器任务，则已安装libpam winbind。

编辑/etc/samba/smb.conf，并在[share]部分更改：guest ok=no

最后，重新启动Samba以使新设置生效：

**sudo systemctl重新启动smbd.service nmbd.service**

现在，当连接到共享目录或打印机时，应该提示您输入用户名和密码。

如果您选择将网络驱动器映射到共享，则可以选中“登录时重新连接”复选框，这将要求您只输入一次用户名和密码，至少在密码更改之前输入一次。

#### 4.3. 共享安全

有几个选项可用于提高每个单独共享目录的安全性。使用[share]示例，本节将介绍一些常见选项。

##### 4.3.1. 组

组定义对特定网络资源具有共同访问级别的计算机或用户的集合，并在控制对此类资源的访问时提供一定的粒度级别。例如，如果定义了组qa并包含用户freda、danika和rob，并且定义了第二个组支持并由用户danika、jeremy和vincent组成，则配置为允许qa组访问的某些网络资源随后将允许freda、danika和rob访问，但不允许jeremy或vincent访问。由于用户danika同时属于qa组和支持组，因此她将能够访问为这两个组的访问而配置的资源，而所有其他用户将只能访问资源，明确允许他们所属的组。

默认情况下，Samba查找/etc/group中定义的本地系统组，以确定哪些用户属于哪些组。有关在组中添加和删除用户的更多信息，请参见第1.2节“添加和删除用户”[p.181]。

在Samba配置文件/etc/Samba/smb.conf中定义组时，公认的语法是在组名前面加一个“@”符号。例如，如果您希望在/etc/samba/smb.conf的某个部分中定义一个名为sysadmin的组，那么可以通过将组名输入为@sysadmin来实现。

##### 4.3.2. 文件权限

文件权限定义计算机或用户对特定目录、文件或文件集的显式权限。可以通过编辑/etc/samba/smb.conf文件并指定已定义文件共享的显式权限来定义此类权限。

例如，如果您定义了一个名为share的Samba共享，并希望向称为qa的用户组授予只读权限，但希望允许名为sysadmin的组和名为vincent的用户写入该共享，则可以编辑/etc/Samba/smb.conf文件，并在[share]条目下添加以下条目：

读取列表=@qa

写入列表=@sysadmin，vincent

另一种可能的Samba权限是声明对特定共享资源的管理权限。具有管理权限的用户可以读取、写入或修改资源中包含的任何信息，该资源已授予用户明确的管理权限。

例如，如果您想向用户melissa授予共享示例的管理权限，您可以编辑/etc/samba/smb.conf文件，并在[share]条目下添加以下行：admin users=melissa

编辑/etc/samba/smb.conf后，重新启动samba以使更改生效：**sudo systemctl重新启动smbd.service nmbd.service**

为了使读列表和写列表工作，Samba安全模式不能设置为security=share

既然Samba已经配置为限制哪些组可以访问共享目录，那么需要更新文件系统权限。

传统的Linux文件权限无法很好地映射到Windows NT访问控制列表（ACL）。幸运地

POSIX ACL在Ubuntu服务器上可用，提供更细粒度的控制。例如，要在EXT3文件系统的/srv上启用acl，请编辑/etc/fstab并添加acl选项：

UUID=66bcdd2e-8861-4fb0-b7e4-e61c569fe17d/srv ext3 noatime、relatime、acl 0 1然后重新装载分区：**sudo安装-v-o重新安装/srv**

上面的示例假设/srv位于单独的分区上。如果/srv或配置共享路径的任何位置是/partition的一部分，则可能需要重新启动。

为了匹配上面的Samba配置，sysadmin组将被授予/srv/Samba/share的读、写和执行权限，qa组将被授予读和执行权限，文件将由用户名melissa拥有。在终端中输入以下内容：

**sudo chown-R melissa/srv/samba/share/sudo chgrp-R sysadmin/srv/samba/share/sudo setfacl-R-m g:qa:rx/srv/samba/share/**

上面的setfacl命令为/srv/samba/share目录中的所有文件提供执行权限，您可能需要，也可能不需要。

现在，从Windows客户端，您应该注意到新的文件权限已实现。有关POSIX acl的更多信息，请参阅acl和setfacl手册页。

#### 4.4. 桑巴公寓简介

Ubuntu附带AppArmor安全模块，该模块提供强制访问控制。默认值

Samba的AppArmor配置文件需要根据您的配置进行调整。有关使用AppArmor的更多详细信息，请参见第4节“AppArmor”[p.194]。

作为AppArmor配置文件包的一部分，Samba守护程序二进制文件/usr/sbin/smbd和/usr/sbin/nmbd都有默认的AppArmor配置文件。要安装软件包，请在终端提示符下输入：**sudo apt安装设备配置文件设备**

此包包含其他几个二进制文件的配置文件。

默认情况下，smbd和nmbd的配置文件处于投诉模式，允许Samba在不修改配置文件的情况下工作，并且只记录错误。要将smbd配置文件置于强制模式，并使Samba按预期工作，需要修改配置文件以反映共享的任何目录。

编辑/etc/apparmor.d/usr.sbin.smbd从文件服务器示例中添加[共享]的信息：

/srv/samba/share/r，

/srv/samba/share/\*\*rwkix，

现在，将配置文件放入“强制”并重新加载：

**sudo aa enforce/usr/sbin/smbd**

**cat/etc/apparmor.d/usr.sbin.smbd | sudo apparmor\_解析器-r**

现在，您应该能够正常读取、写入和执行共享目录中的文件，smbd二进制文件将只能访问配置的文件和目录。确保为配置Samba以共享的每个目录添加条目。此外，任何错误都将记录到/var/log/syslog。

#### 4.5. 资源

•有关深入的Samba配置，请参阅Samba HOWTO集合[298]

•指南也有印刷版[299]。

•O&apos;Reilly使用Samba[300]也是一个很好的参考。

•Samba HOWTO系列的第18章[301]专门讨论安全性。

•有关Samba和ACL的更多信息，请参阅Samba ACL页面[302]。

•Ubuntu Wiki Samba 19页。



19 https://help.ubuntu.com/community/Samba

## 5.作为域控制器

Samba服务器可以配置为显示为Windows NT4风格的域控制器。此配置的一个主要优点是能够集中用户和计算机凭据。Samba还可以使用多个后端来存储用户信息。

#### 5.1. 主域控制器

本节介绍使用默认smbpasswd后端将Samba配置为主域控制器（PDC）。

1.         首先，通过在终端提示符中输入以下内容，安装Samba和libpam winbind以同步用户帐户：**sudo apt安装samba libpam winbind**

2.         接下来，通过编辑/etc/Samba/smb.conf配置Samba。安全模式应设置为用户，工作组应与您的组织相关：

工作组=示例。。。安全性=用户

3.         在已注释的“域”部分添加或取消注释以下内容（最后一行已拆分以适合本文档的格式）：

域登录=是登录路径=\\%N\%U\profile登录驱动器=H:

登录主页=\\%N\%U登录脚本=logon.cmd

add machine script=sudo/usr/sbin/useradd-N-g machines-c machine-d/var/lib/samba-s/bin/false%u

如果不希望使用漫游配置文件，请保留登录主页和登录路径选项。

•提供netlogon服务，使Samba充当域控制器。*域登录：*

•将用户的Windows配置文件放入其主目录。还可以配置[配置文件]共享，将所有配置文件放在一个目录下。*登录路径：*

•指定主目录本地路径。*登录驱动器：*

•指定主目录位置。*登录主页：*

•确定用户登录后在本地运行的脚本。脚本需要放在[netlogon]共享中。*登录脚本：*

•自动创建工作站加入域所需的机器信任帐户的脚本。*添加计算机脚本：*

在本例中，需要使用addgroup实用程序创建机器组。有关详细信息，请参见第1.2节“添加和删除用户”[p.181]。

4.         取消对[homes]共享的注释以允许映射登录主页：

[家庭]

comment=主目录可浏览=无只读=无创建掩码=0700目录掩码=0700有效用户=%S

5.         当配置为域控制器时，需要配置[netlogon]共享。要启用共享，请取消注释：

[网络登录]

comment=网络登录服务路径=/srv/samba/netlogon来宾确定=是只读=是共享模式=否

最初的netlogon共享路径是/home/samba/netlogon，但根据文件系统层次结构标准（FHS），/srv[303]是系统提供的站点特定数据的正确位置。

6.         现在创建netlogon目录和一个空的（暂时）logon.cmd脚本文件：

**sudo mkdir-p/srv/samba/netlogon sudo touch/srv/samba/netlogon/logon.cmd**

您可以在logon.cmd中输入任何普通的Windows登录脚本命令来自定义客户端环境。

7.         重新启动Samba以启用新的域控制器：

**sudo systemctl重新启动smbd.service nmbd.service**

8.         最后，需要一些附加命令来设置适当的权限。

在默认情况下禁用root的情况下，为了将工作站加入域，需要将系统组映射到Windows域管理员组。使用net实用程序，从终端输入：**sudo net groupmap add ntgroup=“Domain Admins”unixgroup=sysadmin rid=512 type=d**

将sysadmin更改为您喜欢的组。此外，用于加入域的用户需要是sysadmin组的成员，以及system admin组的成员。管理员组允许sudo使用。

如果用户还没有Samba凭据，则可以使用smbpasswd实用程序添加这些凭据，适当更改sysadmin用户名：**sudo smbpasswd-系统管理员**

此外，需要向域管理员组显式提供权限，以允许添加机器脚本（和其他管理功能）工作。这是通过执行以下操作实现的：

**net rpc权限授予-U sysadmin“EXAMPLE\Domain Admins”SeMachineAccountPrivilege\sePrintOperator权限seadUsersPrivilege sediskoOperator权限\**

**seremoteshutdown特权**

9您现在应该能够将Windows客户端加入域，方式与将它们加入Windows服务器上运行的NT4域相同。

#### 5.2. 备份域控制器

如果网络上有一个主域控制器（PDC），最好也有一个备份域控制器（BDC）。这将允许客户端在PDC不可用时进行身份验证。

将Samba配置为BDC时，需要一种将帐户信息与PDC同步的方法。有多种方法可以实现此scp、rsync或使用LDAP作为passdb后端。

使用LDAP是同步帐户信息最可靠的方法，因为两个域控制器可以实时使用相同的信息。但是，对于少数用户和计算机帐户来说，设置LDAP服务器可能过于复杂。有关详细信息，请参见第2节“Samba和LDAP”[p.140]。

1.         首先，安装samba和libpam winbind。从终端输入：

**sudo apt安装samba libpam winbind**

2.         现在，编辑/etc/samba/smb.conf并在[global]中取消注释以下内容：

工作组=示例。。。安全性=用户

3.         在已注释的域中取消注释或添加：

域登录=是域主机=否

4.         确保用户有权读取/var/lib/samba中的文件。例如，要允许admin组中的用户scp文件，请输入：

**sudochgrp-R admin/var/lib/samba**

5.         接下来，同步用户帐户，使用scp从PDC复制/var/lib/samba目录：

**sudo-scp-rusername@pdc：/var/lib/samba/var/lib**

将用户名替换为有效用户名，将pdc替换为实际pdc的主机名或IP地址。

6.         最后，重新启动samba：

**sudo systemctl重新启动smbd.service nmbd.service**

您可以通过停止PDC上的Samba守护程序，然后尝试登录到加入域的Windows客户端，来测试备份域控制器是否正常工作。

要记住的另一件事是，如果您已将登录主目录选项配置为PDC上的目录，并且PDC变得不可用，则访问用户的主驱动器也将不可用。因此，最好将登录主页配置为驻留在与PDC和BDC不同的文件服务器上。

#### 5.3. 资源

•有关深入的Samba配置，请参阅Samba HOWTO集合[304]

•指南也有印刷版[305]。

•O&apos;Reilly使用Samba[306]也是一个很好的参考。

•Samba HOWTO集合的第4章[307]解释了如何设置主域控制器。

•Samba HOWTO系列的第5章[308][309]介绍了如何设置备份域控制器。

•Ubuntu Wiki Samba 26页。

## 6.Active Directory集成

#### 6.1. 访问Samba共享

Samba的另一个用途是集成到现有的Windows网络中。一旦成为Active Directory域的一部分，Samba就可以向AD用户提供文件和打印服务。有关如何加入域的详细信息，请参阅本指南第5节“SSSD和Active Directory”[p.161]一章。

一旦成为Active Directory域的一部分，在终端提示符中输入以下命令：下一步，编辑/etc/samba/smb.conf更改：**sudo apt安装samba cifs utils smbclient**

工作组=示例。。。

security=ads realm=EXAMPLE.COM。。。

idmap后端=LWON idmap uid=50-9999999 idmap gid=50-99999999

重新启动samba以使新设置生效：**sudo systemctl重新启动smbd.service nmbd.service**

您现在应该能够从Windows客户端访问任何Samba共享。但是，请确保为适当的AD用户或组提供对共享目录的访问权限。有关更多详细信息，请参见第4节“保护文件和打印服务器”[p.312]。

#### 6.2. 访问Windows共享

既然Samba服务器是Active Directory域的一部分，您就可以访问任何Windows服务器共享：

•要装载Windows文件共享，请在终端提示符中输入以下内容：**mount.cifs//fs01.example.com/share mount\u point**

也可以访问不属于AD域的计算机上的共享，但需要提供用户名和密码。

•要在启动期间装载共享，请在/etc/fstab中放置一个条目，例如：

//192.168.0.5/share/mnt/windows cifs auto，username=steve，password=secret，rw 0•从windows服务器复制文件的另一种方法是使用smbclient实用程序。要列出Windows共享中的文件，请执行以下操作：

**smbclient//fs01.example.com/share-k-c“ls”**

•要从共享中复制文件，请输入：**smbclient//fs01.example.com/share-k-c“get file.txt”**

这将把文件.txt复制到当前目录中。

•以及将文件复制到共享：**smbclient//fs01.example.com/share-k-c“put/etc/hosts”**

这将把/etc/hosts复制到//fs01.example.com/share/hosts。

•上面使用的-c选项允许您一次性执行smbclient命令。这对于脚本和小文件操作非常有用。要进入smb:\>提示符（类似FTP的提示符，您可以在其中执行普通文件和目录命令），只需执行：**smbclient//fs01.example.com/share-k**

将fs01.example.com/share、//192.168.0.5/share、username=steve、password=secret和file.txt的所有实例替换为服务器的IP、主机名、共享名、文件名以及具有共享权限的实际用户名和密码。

#### 6.3. 资源

有关更多smbclient选项，请参阅手册页：man smbclient，也可在线获取[310]。

mount.cifs手册页[311][312]也可用于获取更多详细信息。

Ubuntu Wiki Samba 29页。

# 第十九章。备份

有很多方法可以备份Ubuntu安装。关于备份，最重要的是制定一个备份计划，包括备份什么、备份到哪里以及如何恢复。

以下各节讨论完成这些任务的各种方法。

## 1.Shell脚本

备份系统最简单的方法之一是使用shell脚本。例如，可以使用脚本配置要备份的目录，并将这些目录作为参数传递给tar实用程序，该实用程序将创建存档文件。然后可以将存档文件移动或复制到其他位置。还可以在远程文件系统（如NFS装载）上创建存档。

tar实用程序从许多文件或目录中创建一个归档文件。tar还可以通过压缩实用程序过滤文件，从而减小归档文件的大小。

#### 1.1. 简单Shell脚本

下面的shell脚本使用tar在远程安装的NFS文件系统上创建归档文件。存档文件名是使用其他命令行实用程序确定的。

#!/bin/bash####################################

##备份到NFS装载脚本。

# ####################################

#备份什么。

backup\_files=“/home/var/spool/mail/etc/root/boot/opt”

#备份到哪里。dest=“/mnt/backup”

#创建归档文件名。日期=$（日期+%A）主机名=$（主机名-s）存档文件=“$hostname-$day.tgz”

#打印开始状态消息。echo“将$backup\u文件备份到$dest/$archive\u文件”日期echo

#使用tar备份文件。

tar czf$dest/$archive\u file$backup\u files

#打印结束状态消息。回响

回显“备份完成”日期

#用$dest检查文件大小的长文件列表。

ls-lh$dest

•一个变量，列出要备份的目录。该列表应根据您的需要进行定制。*$backup\u文件：*

•持有一周中某一天（周一、周二、周三等）的变量。这用于为一周中的每一天创建存档文件，提供七天的备份历史记录。还有其他方法可以实现这一点，包括使用date实用程序。*$day：*

•包含系统短主机名的变量。在存档文件名中使用主机名，可以选择将来自多个系统的每日存档文件放置在同一目录中。*$hostname:*

•完整的存档文件名。*$archive\u文件：*

•归档文件的目标。在执行备份脚本之前，需要创建并装入目录。有关使用NFS的详细信息，请参见第2节“网络文件系统（NFS）”[p.253]。*$dest：*

•使用echo实用程序将可选消息打印到控制台。*状态消息：*

•用于创建归档文件的tar命令。*tar czf$dest/$archive\u file$backup\u文件：*

•创建存档。*c:*

•通过压缩归档文件的gzip实用程序过滤归档文件。*z:*

•输出到存档文件。否则，tar输出将被发送到STDOUT。*f:*

•可选语句以-h人类可读格式打印目标目录的-l长列表。这对于快速检查存档文件的文件大小非常有用。此检查不应取代对存档文件的测试。*ls-左侧$dest：*

这是一个备份shell脚本的简单示例；但是，在这样的脚本中可以包含许多选项。请参阅第1.4节“参考”[p.327]以获取指向提供更深入shell脚本信息的资源的链接。

#### 1.2. 执行脚本

##### 1.2.1. 从终端执行

执行上述备份脚本的最简单方法是将内容复制并粘贴到文件中。例如backup.sh。必须使文件可执行：**chmod u+x backup.sh**

然后从终端提示符：**sudo./backup.sh**

这是测试脚本以确保一切按预期工作的一种好方法。

##### 1.2.2. 使用cron执行

cron实用程序可用于自动化脚本执行。cron守护进程允许在指定的时间和日期执行脚本或命令。

cron是通过crontab文件中的条目配置的。crontab文件分为多个字段：

#m h dom mon dow命令

•命令在0和59之间执行的分钟数。*m:*

•执行命令的时间，介于0和23之间。*h:*

•执行命令的月份日期。*dom:*

•命令执行的月份，介于1和12之间。*周一：*

•执行命令的星期几，介于0和7之间。星期日可以使用0或7指定，这两个值都有效。*陶氏：*

•要执行的命令。*命令：*

要在crontab文件中添加或更改条目，应使用crontab-e命令。此外，可以使用crontab-l命令查看crontab文件的内容。

使用cron执行上面列出的backup.sh脚本。从终端提示中输入以下内容：**sudo crontab-e**

使用sudo和crontab-e命令编辑根用户的crontab。如果您备份的目录只有根用户有权访问，则这是必需的。

将以下条目添加到crontab文件：

#m h dom mon dow命令

0\*\*\*bash/usr/local/bin/backup.sh

backup.sh脚本现在将在每天上午12:00执行。

需要将backup.sh脚本复制到/usr/local/bin/目录，以便正确执行此条目。脚本可以驻留在文件系统的任何位置，只需适当更改脚本路径即可。

有关更深入的crontab选项，请参见第1.4节“参考”[p.327]。

#### 1.3. 从存档中恢复

创建存档后，测试存档非常重要。可以通过列出存档包含的文件来测试存档，但最好的测试是从存档中恢复文件。

•查看归档内容列表。从终端提示类型：**tar-tzvf/mnt/backup/host-Monday.tgz**

•要将文件从存档恢复到其他目录，请输入：

**tar-xzvf/mnt/backup/host-Monday.tgz-C/tmp etc/hosts**

tar的-C选项将提取的文件重定向到指定的目录。上面的示例将/etc/hosts文件提取到/tmp/etc/hosts。tar重新创建它所包含的目录结构。

另外，请注意，前导“/”被保留在要还原的文件路径之外。

•要恢复存档中的所有文件，请输入以下内容：

**光盘/**

**sudo tar-xzvf/mnt/backup/host-Monday.tgz**

这将覆盖文件系统上当前的文件。

#### 1.4. 工具书类

•有关shell脚本的更多信息，请参阅高级Bash脚本指南[313]

•在线提供了《24小时自学Shell编程》一书[314]，这是一本非常好的Shell脚本编写资源。

•CronHowto Wiki页面[315]包含有关高级cron选项的详细信息。

•更多tar选项，请参见GNU tar手册[316]。

•维基百科备份轮换方案[317]文章包含其他备份轮换方案的信息。

•shell脚本使用tar创建归档文件，但也可以使用许多其他命令行实用程序。

例如：

•cpio[318]：用于将文件复制到存档中或从存档中复制文件。

•dd[319]：coreutils包的一部分。可以将数据从一种格式复制到另一种格式的低级实用程序。

•rsnapshot[320]：用于创建整个文件系统副本的文件系统快照实用程序。

•rsync[321]：用于创建文件增量副本的灵活实用程序。

## 2.档案轮换

第1节“shell脚本”[p.324]中的shell脚本只允许七种不同的归档。对于数据不经常更改的服务器，这可能就足够了。如果服务器有大量数据，则应使用更复杂的轮换方案。

#### 2.1. 旋转NFS存档

在本节中，将稍微修改shell脚本以实现祖父-父亲-儿子轮换计划（每月-每周-每天）：

•轮换将在周日至周五进行每日备份。

•周六每周备份一次，每月为您提供四次每周备份。

•每月备份在每月的第一个月进行，根据月份是奇数还是偶数轮流进行两次每月备份。

以下是新脚本：

#!/bin/bash####################################

#

#使用#祖父-父亲-儿子循环备份到NFS装载脚本。

# ####################################

#备份什么。

backup\_files=“/home/var/spool/mail/etc/root/boot/opt”

#备份到哪里。dest=“/mnt/backup”

#存档文件名的设置变量。日期=$（日期+%A）主机名=$（主机名-s）

#找出1-4月的哪一周。如果（$day\_num<=7）），则day\_num=$（date+%-d）；然后week\_file=“$hostname-week1.tgz”elif（$day\_num>7&$day\_num<=14））；然后week\_file=“$hostname-week2.tgz”elif（$day\_num>14&&$day\_num<=21））；然后week\_file=“$hostname-week3.tgz”elif（$day\_num>21&$day\_num<32））；然后week\_file=“$hostname-week4.tgz”fi

#找出这个月是奇数还是偶数。月数=$（日期+%m）月数=$（expr$月数%2）如果[$month-eq 0]；然后

month\_file=“$hostname-month2.tgz”其他

month\_file=“$hostname-month1.tgz”fi

#创建归档文件名。如果[$day\_num==1]；然后归档文件=$month\u文件elif[$day！=“星期六”]；然后归档文件=“$hostname-$day.tgz”或

归档文件=$week\u文件fi

#打印开始状态消息。

echo“将$backup\u文件备份到$dest/$archive\u文件”日期echo

#使用tar备份文件。

tar czf$dest/$archive\u file$backup\u files

#打印结束状态消息。回响

回显“备份完成”日期

#用$dest检查文件大小的长文件列表。ls-lh$dest/

可以使用与第1.2节“执行脚本”相同的方法执行脚本[p.325]。

在发生灾难时，最好将备份介质移出现场。在shell脚本示例中，备份介质是另一台提供NFS共享的服务器。很可能将NFS服务器转移到另一个位置是不实际的。根据连接速度，可以选择通过WAN链接将存档文件复制到另一个位置的服务器。

另一种选择是将归档文件复制到外部硬盘，然后将其移出现场。由于外部硬盘驱动器的价格不断下降，因此为每个归档级别使用两个驱动器可能会更经济划算。这将允许您将一个外部驱动器连接到备份服务器，另一个连接到另一个位置。

#### 2.2. 磁带机

可以使用连接到服务器的磁带机代替NFS共享。使用磁带机可以简化归档文件的轮换，也可以更轻松地将介质移出现场。

使用磁带机时，不需要脚本的文件名部分，因为数据直接发送到磁带设备。需要一些操作磁带的命令。这是使用mt实现的，mt是cpio包的磁带控制实用程序部分。

以下是修改为使用磁带机的shell脚本：

#!/bin/bash####################################

##备份到磁带机脚本。

# ####################################

#备份什么。

backup\_files=“/home/var/spool/mail/etc/root/boot/opt”

#备份到哪里。dest=“/dev/st0”

#打印开始状态消息。

echo“将$backup\u文件备份到$dest”日期echo

#确保磁带已倒带。

mt-f$dest倒带

#使用tar备份文件。tar czf$dest$备份文件

#倒带并弹出磁带。

mt-f$目的地重新收费

#打印结束状态消息。

回响

回显“备份完成”日期

SCSI磁带机的默认设备名为/dev/st0。为您的系统使用适当的设备路径。

从磁带机恢复与从文件恢复基本相同。只需倒带磁带并使用设备路径而不是文件路径。例如，要将/etc/hosts文件恢复到/tmp/etc/hosts，请执行以下操作：

**mt-f/dev/st0倒带**

**tar-xzf/dev/st0-C/tmp等/hosts**

## 3.杆菌

Bacula是一个备份程序，使您能够通过网络备份、恢复和验证数据。有针对Linux、Windows和Mac OS X的Bacula客户端，使其成为跨平台的网络范围解决方案。

#### 3.1. 概述

Bacula由几个组件和服务组成，用于管理要备份的文件和备份位置：

•Bacula控制器：控制所有备份、恢复、验证和归档操作的服务。

•Bacula控制台：允许与控制器通信的应用程序。控制台有三个版本：

•基于文本的命令行版本。

•基于Gnome的GTK+图形用户界面（GUI）界面。

•wxWidgets GUI界面。

•Bacula文件：也称为Bacula客户端程序。此应用程序安装在要备份的计算机上，并负责管理控制器请求的数据。

•Bacula存储：执行数据存储和恢复到物理介质的程序。

•Bacula Catalog：负责维护备份的所有文件的文件索引和卷数据库，实现归档文件的快速定位和恢复。该目录支持三种不同的数据库MySQL、PostgreSQL和SQLite。

•Bacula Monitor：允许监视控制器、文件守护程序和存储守护程序。目前，监视器仅作为GTK+GUI应用程序提供。

这些服务和应用程序可以在多台服务器和客户端上运行，如果备份单个磁盘或卷，也可以安装在一台计算机上。

#### 3.2. 安装

如果使用MySQL或PostgreSQL作为数据库，您应该已经有了可用的服务。

Bacula不会为您安装它们。

有多个包装包含不同的杆菌成分。要安装Bacula，请在终端提示符下输入：**sudo-apt-install-bacula**

默认情况下，安装bacula包将使用MySQL数据库作为目录。如果你想用

SQLite或PostgreSQL，对于目录，分别安装bacula-director-sqlite3或bacula director pgsql。

在安装过程中，将要求您提供数据库管理员和bacula数据库所有者的凭据。数据库管理员需要拥有创建数据库的相应权限，有关更多信息，请参阅第1节“MySQL”[p.233]。

#### 3.3. 配置

Bacula配置文件的格式基于由“{}”大括号包围的指令组成的资源。每个Bacula组件在/etc/Bacula目录中都有一个单独的文件。

各种细菌成分必须相互授权。这是使用password指令完成的。例如，/etc/bacula/bacula-dir.conf文件中的存储资源密码必须与/etc/bacula/bacula-sd.conf中的控制器资源密码匹配。

默认情况下，名为Client1的备份作业配置为归档Bacula目录。如果计划使用服务器备份多个客户端，则应将此作业的名称更改为更具描述性的名称。

要更改名称，请编辑/etc/bacula/bacula-dir.conf：

#

#定义主夜间保存备份作业#默认情况下，此作业将在中备份到磁盘

工作{

Name=“备份服务器”

JobDefs=“DefaultJob”Write Bootstrap=“/var/lib/bacula/Client1.bsr”

}

上面的示例将作业名称更改为与计算机主机名匹配的BackupServer。

用适当的主机名或其他描述性名称替换“BackupServer”。

控制台可用于向控制器查询有关作业的信息，但要与非root用户一起使用控制台，用户需要在bacula组中。要将用户添加到bacula组，请从终端输入以下内容：**sudo adduser$username bacula**

将$username替换为实际用户名。此外，如果要将当前用户添加到组中，则应注销并重新登录，以使新权限生效。

#### 3.4. 本地主机备份

本节介绍如何将单个主机上的指定目录备份到本地磁带机。

•首先，需要配置存储设备。编辑/etc/bacula/bacula-sd.conf添加：

装置{

Name=“磁带机”

设备类型=磁带

媒体类型=DDS-4

存档设备=/dev/st0

介质的硬件端=否；自动计数=是；#当设备打开时，读取它

AlwaysOpen=是；

RemovableMedia=是；

RandomAccess=no；Alert Command=“sh-c”tapeinfo-f%c | grep TapeAlert”

}

该示例适用于DDS-4磁带机。调整“媒体类型”和“存档设备”以匹配您的硬件。

您还可以取消对文件中其他示例之一的注释。

•编辑/etc/bacula/bacula-sd.conf后，需要重新启动存储守护程序：**sudo systemctl重新启动bacula-sd.service**

•现在在/etc/bacula/bacula-dir.conf中添加一个存储资源以使用新设备：

#“磁带机”存储设备的定义

储藏{

名称=磁带驱动器

#不要在此处使用“localhost”Address=backupserver#N.B.在此处使用完全限定的名称

SDPort=9103 Password=“CV70F6PF1T6PBOPT4VQONIGDR0V3LT3CGKIYJC”

设备=“磁带机”介质类型=磁带

}

Address指令必须是服务器的完全限定域名（FQDN）。将backupserver更改为实际主机名。

另外，确保Password指令与/etc/bacula/bacula-sd.conf中的密码字符串匹配。

•通过添加以下内容，创建一个新的文件集，该文件集将确定要备份的目录：

#LocalhostBacup文件集。

文件集{Name=“LocalhostFiles”

包括{Options{signature=MD5 compression=GZIP}

文件=/etc文件=/home

}

}

此文件集将备份/etc和/home目录。Options resource指令配置文件集，以便为每个备份的文件创建MD5签名，并使用GZIP压缩文件。

•接下来，为备份作业创建新计划：

#LocalhostBackup计划--每天。

时间表{

Name=“LocalhostDaily”在00:01运行=每天完整

}

作业将在每天上午00:01或12:01运行。还有许多其他可用的计划选项。

•最终创建作业：

#本地主机备份。

工作{

Name=“LocalhostBackup”

JobDefs=“DefaultJob”

启用=是

水平=满

FileSet=“LocalhostFiles”

Schedule=“LocalhostDaily”

Storage=TapeDrive Write Bootstrap=“/var/lib/bacula/LocalhostBackup.bsr”

}

该作业将每天对磁带机进行完整备份。

•使用的每条磁带都需要有标签。如果当前磁带没有标签，Bacula将发送电子邮件通知您。要使用控制台标记磁带，请从终端输入以下内容：**B控制台**

•在Bacula控制台提示下输入：**标签**

•然后会提示您输入存储资源：

自动选择的目录：MyCatalog

使用目录“MyCatalog”，定义的存储资源包括：

1：文件

2：磁带机

选择存储资源（1-2）：2

•输入新卷名：

输入新卷名：星期日定义的池：

1：默认

2:刮伤

用所需的标签替换Sunday。

•现在，选择池：

选择池（1-2）：1连接到备份服务器9103上的存储守护进程TapeDrive。。。

正在发送卷“星期日”插槽0的标签命令。。。

祝贺您，您现在已将Bacula配置为将本地主机备份到连接的磁带机。

#### 3.5. 资源

•有关更多Bacula配置选项，请参阅Bacula的文档[322][323]。

•Bacula主页11包含最新Bacula新闻和发展。

•另外，请参见Bacula Ubuntu Wiki[324]页面。

# 第20章。虚拟化

虚拟化正在许多不同的环境和情况下被采用。如果您是一名开发人员，虚拟化可以为您提供一个包含的环境，在这个环境中，您可以安全地进行几乎任何类型的开发，而不会弄乱您的主要工作环境。如果您是系统管理员，您可以使用虚拟化更轻松地分离服务，并根据需要移动它们。

Ubuntu中支持的默认虚拟化技术是KVM。对于Intel和AMD硬件，KVM需要虚拟化扩展。但KVM也可用于IBM Z和LinuxONE、IBM POWER以及ARM64。Xen在Ubuntu上也受支持，但并非适用于所有体系结构，例如不适用于IBMz和LinuxONE。Xen可以利用可用的虚拟化扩展，但也可以在没有虚拟化扩展的硬件上使用。Qemu是另一种不带虚拟化扩展的流行硬件解决方案。

## 1.利勃维特

libvirt库用于与不同的虚拟化技术进行接口。在开始使用libvirt之前，最好确保您的硬件支持KVM所需的虚拟化扩展。从终端提示中输入以下内容：**kvm正常**

将打印一条消息，通知您CPU是否支持硬件虚拟化。

在许多处理器支持硬件辅助虚拟化的计算机上，有必要激活BIOS中的选项以启用它。

#### 1.1. 虚拟网络

有几种不同的方式允许虚拟机访问外部网络。默认的虚拟网络配置包括桥接和iptables规则，这些规则实现了使用SLIRP协议的用户模式网络。流量通过主机接口传输到外部网络。

要使外部主机能够直接访问虚拟机上的服务，需要配置不同于默认类型的网桥。这允许虚拟接口通过物理接口连接到外部网络，使其在网络的其余部分显示为普通主机。

#### 1.2. 安装

要安装必要的软件包，请在终端提示符下输入：**sudo-apt安装qemu-kvm-libvirt-bin**

安装libvirt-bin后，需要将用于管理虚拟机的用户添加到libvirt组。

这样做将授予用户访问高级网络选项的权限。

在终端中输入：**sudo adduser$USER libvirt**

如果选择的用户是当前用户，则需要注销并重新登录才能使新的组成员资格生效。

现在可以安装来宾操作系统了。安装虚拟机的过程与直接在硬件上安装操作系统的过程相同。您需要一种自动化安装的方法，或者需要将键盘和监视器连接到物理机器。

在虚拟机的情况下，图形用户界面（GUI）类似于使用物理键盘和鼠标。virt viewer应用程序可以使用VNC连接到虚拟机的控制台，而不是安装GUI。有关更多信息，请参见第1.6节“虚拟机查看器”[p.342]。

有几种方法可以自动化Ubuntu的安装过程，例如使用preseeds、kickstart等。

有关详细信息，请参阅Ubuntu安装指南[325]。

另一种安装Ubuntu虚拟机的方法是使用uvtool。此应用程序从14.04开始提供，允许您设置特定的VM选项、执行自定义安装后脚本等。有关详细信息，请参阅第3节“云图像和uvtool”[p.346]。

Libvirt也可以配置为与Xen一起使用。有关详细信息，请参阅下面引用的Xen Ubuntu社区页面。

#### 1.3. 虚拟安装

virt安装是virtinst包的一部分。要安装它，请在终端提示符下输入：

**sudoapt安装virtinst**

使用virt安装时，有几个选项可用。例如：

**sudo virt install-n web\_devel-r 512 \--disk path=/var/lib/libvirt/images/web\_devel.img，bus=virtio，size=4-c\ubuntu-18.04-server-i386.iso--network-network=default，model=virtio \--图形vnc，listen=0.0.0--noautoconsole-v**

•在本例中，新虚拟机的名称为web\_devel。*-网络开发：*

•指定虚拟机将使用的内存量（MB）。*-r 512：*

•指示虚拟磁盘的路径，虚拟磁盘可以是文件、分区或逻辑卷。在本例中，/var/lib/libvirt/images/目录中的一个名为web\_devel.img的文件，大小为4G字节，使用virtio作为磁盘总线。*--磁盘路径=/var/lib/libvirt/images/web\_-devel.img，大小=4：*

•用作虚拟CDROM的文件。该文件可以是ISO文件，也可以是主机CDROM设备的路径。*-c ubuntu-18.04-server-i386.iso：*

•提供与虚拟机网络接口相关的详细信息。这里使用默认网络，并为virtio配置接口模型。*--网络*

•使用VNC和所有主机接口导出来宾的虚拟控制台。服务器通常没有GUI，因此局域网（LAN）上的另一台基于GUI的计算机可以通过VNC连接以完成安装。*--图形vnc，侦听=0.0.0.0：*

•不会自动连接到虚拟机的控制台。*--无自动控制台：*

•创建完全虚拟化的来宾。*-五:*

启动virt install后，您可以使用GUI（如果您的服务器有GUI）本地连接到虚拟机的控制台，或者通过基于GUI的计算机上的远程VNC客户端连接到虚拟机的控制台。

#### 1.4. 病毒克隆

virt clone应用程序可用于将一个虚拟机复制到另一个虚拟机。例如：**sudo virt clone-o web\_-devel-n database\_-devel-f/path/to/database\_-devel.img**

•原始虚拟机。*-o:*

•新虚拟机的名称。*-n:*

•新虚拟机要使用的文件、逻辑卷或分区的路径。*-f:*

另外，使用-d或--debug选项帮助解决virt clone的问题。

用适当的虚拟机名称替换web\_-devel和数据库\_-devel。

#### 1.5. 虚拟机管理

##### 1.5.1. 维尔什

有几种实用程序可用于管理虚拟机和libvirt。可以从命令行使用virsh实用程序。一些例子：

•要列出正在运行的虚拟机，请执行以下操作：**病毒列表**

•要启动虚拟机，请执行以下操作：**virsh启动web\u开发**

•类似地，要在启动时启动虚拟机：**virsh autostart web\_-devel**

•使用以下命令重新启动虚拟机：**virsh重新启动web\_-devel**

•虚拟机的状态可以保存到文件中，以便以后恢复。以下操作将虚拟机状态保存到根据日期命名的文件中：**virsh save web\_devel web\_devel-022708.state**

保存后，虚拟机将不再运行。

•保存的虚拟机可以通过以下方式还原：

**virsh还原web\_devel-022708.state**

•要关闭虚拟机，请执行以下操作：**virsh关闭web\_-devel**

•可通过输入以下命令将CDROM设备安装到虚拟机中：**virsh附加磁盘web\u devel/dev/cdrom/media/cdrom**

在上述示例中，使用适当的虚拟机名称替换web\_-devel，并使用描述性文件名替换web\_-devel-022708.state。

如果virsh（或其他vir\*工具）应连接到默认qemu kvm/system hipervisor以外的其他设备，则可以在man virsh或libvirt doc[326]中找到连接选项的替代方案

##### 1.5.2. 迁移

根据所使用的libvirt和hipervisor版本的不同，有不同类型的迁移可用。一般来说，这些类型是：

•离线迁移[327]

•实时迁移[328]

•复印后迁移[329]

这些方法有多种选择，但它们的入口点都是virsh migrate。有关更多详细信息，请阅读集成帮助。virsh迁移--帮助

一些关于实时迁移的约束和注意事项的有用文档可以在Ubuntu上找到

维基[330]

##### 1.5.3. 设备直通/热插拔

如果您希望始终通过设备，而不是此处所述的热插拔，请通过例如virsh edit<guestname>将设备的xml内容添加到静态来宾xml表示中。在这种情况下，不需要使用“附加/分离”。有不同种类的传递。可用的类型取决于硬件和软件设置。

•USB热插拔/直通

•VF热插拔/直通

但这两种类型都是以非常相似的方式处理的，虽然有各种各样的方法（例如，也通过qemu监视器），但建议通过libvirt驱动这样的更改。这样，libvirt可以尝试为您管理各种特殊情况，并在某种程度上掩盖版本差异。

通常，当通过libvirt驱动热插拔时，您会创建一个xml片段来描述设备，就像在静态来宾描述中一样。[331]usb设备通常由供应商/产品id标识：

<hostdev mode=&apos;subsystem&apos;type=&apos;usb&apos;managed=&apos;yes&apos;>

<source>

<vendor id=&apos;0x0b6d&apos;/><product id=&apos;0x3880&apos;/>

</source>

</hostdev>

虚拟功能通常通过其PCI-ID（域、总线、插槽、功能）分配。

<hostdev mode=&apos;subsystem&apos;type=&apos;pci&apos;managed=&apos;yes&apos;>

<source><address domain=&apos;0x0000&apos;总线=&apos;0x04&apos;插槽=&apos;0x10&apos;函数=&apos;0x0&apos;/>

</source>

</hostdev>

首先，获取虚拟功能是非常依赖于设备的，因此这里不能完全介绍。但一般来说，它包括建立一个iommu，通过VFIO[332]注册，有时还请求一些VFs。以下是ppc64el上的一个示例，用于在设备上获得4个VF：

$sudo modprobe vfio pci

#识别装置

$lspci-n-s 0005:01:01.3

0005:01:01.30200:10df:e228（版本10）

#注册并请求VFs

$echo 10df e228 | sudo-tee/sys/bus/pci/drivers/vfio-pci/new|id$echo 4 | sudo-tee/sys/bus/pci/devices/0005 \：01 \：00.0/sriov\_numvfs

然后通过libvirt将guest与xml片段关联，从而连接或分离设备。

**virsh附加设备<guestname><devicexml>**#在来宾中使用该设备

**virsh分离设备<guestname><devicexml>**

关于保护“过多”的装置保护，存在几个相关的已知问题。您可能需要调整apparmor配置文件中的异常，直到错误1552241[333]（用于USB）和https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1679704（用于VF分配）已解决。要检查您是否受到影响，请在使用USB/VF直通/热插拔功能时观看dmesg，并验证您是否看到apparmor拒绝[334]。

##### 1.5.4. 通过libvirt访问Qemu监视器

Qemu监视器[335]是在来宾运行时与Qemu/KVM交互的方式。对于有经验的用户，此界面具有许多非常强大的功能。在libvirt下运行时，出于管理目的，监视器接口由libvirt本身绑定，但用户仍然可以通过libvirt运行qemu监视器命令。一般语法为virsh qemu monitor command[options][guest]“command”

Libvirt涵盖了所需的大多数用例，但如果您希望/需要使用Libvirt，或者希望调整非常特殊的选项，您可以这样添加设备：

virsh qemu monitor命令--hmp zesty测试日志&apos;drive\u add 0 if=none，file=/var/libvirt/images/test.img，format=raw，id=disk1&apos;

但由于监视器功能强大，您可以做很多工作，特别是在调试时，例如显示来宾寄存器：

virsh qemu监视器命令--hmp y-ipns‘信息寄存器’RAX=00ffffc000000000 RBX=ffff8f0f5d5c7e48 RCX=00000000000000000RDX=FFFFFFA00007571C0 RSI=00000000000000000RDI=ffff8f0fdd5c7e48 RBP=ffff8f0f5d5c7e18 RSP=FFFFFF8F0F5D5C7DF8

[...]

##### 1.5.5. 虚拟机管理器

virt管理器包包含一个图形实用程序，用于管理本地和远程虚拟机。要安装virt manager，请输入：**sudoapt安装virt管理器**

由于virt manager需要图形用户界面（GUI）环境，建议将其安装在工作站或测试机上，而不是生产服务器上。要连接到本地libvirt服务，请输入：**virt经理-cqemu:///system**

通过在终端提示符中输入以下内容，可以连接到另一台主机上运行的libvirt服务：**virt经理-c qemu+ssh://virtnode1.mydomain.com/system**

上面的示例假设管理系统和virtnode1.mydomain.com之间的SSH连接已经配置，并使用SSH密钥进行身份验证。需要SSH密钥，因为libvirt会将密码提示发送到另一个进程。有关配置SSH的详细信息，请参阅第1节“OpenSSH服务器”[p.104]

#### 1.6. 虚拟机查看器

virt viewer应用程序允许您连接到虚拟机的控制台。VirtViewer确实需要图形用户界面（GUI）来与虚拟机交互。

要从终端安装virt viewer，请输入：**sudo-apt安装virt-viewer**

安装并运行虚拟机后，您可以通过以下方式连接到虚拟机的控制台：**虚拟查看器web\u-devel**

与virt manager类似，virt viewer也可以使用SSH和密钥身份验证连接到远程主机：确保用适当的虚拟机名称替换web\_-devel。**virt查看器-cqemu+ssh://virtnode1.mydomain.com/system 网络开发**

如果配置为使用桥接网络接口，还可以设置对虚拟机的SSH访问。

#### 1.7. 资源

•有关更多详细信息，请参阅KVM[336]主页。

•有关libvirt的更多信息，请参见libvirt主页[337]

•Virtual Machine Manager[338]网站提供了有关virt Manager开发的更多信息。

•另外，请访问freenode[339][340]上的#ubuntu virt IRC频道，讨论ubuntu中的虚拟化技术。

•另一个很好的资源是Ubuntu Wiki KVM16页面。

•有关Xen的信息，包括与libvirt一起使用Xen，请参见Ubuntu Wiki Xen[341]页面。

•有关如何将VT-d设备分配给qemu/KVM的基本信息，请参阅linux KVM[342]页。

## 2.Qemu

Qemu[343]是一种机器仿真器，可以在不同的机器上为一台机器运行操作系统和程序。大多数情况下，它不是用作仿真器，而是与KVM或XEN内核组件协作用作虚拟机。在这种情况下，它利用硬件的虚拟化技术来虚拟化来宾。

虽然qemu有一个命令行界面[344]和一个监视器[345]，用于与正在运行的客户机交互，但这种方式很少用于开发目的以外的其他方式。Libvirt提供了特定版本和虚拟机监控程序的抽象，并封装了一些变通方法和最佳实践。

#### 2.1. 升级机器类型

UbuntuWiki[346]上还记录了一些约束和注意事项

您可能希望将现有已定义来宾的计算机类型更新为：

•获取最新的安全修补程序和功能

•继续使用在现在不受支持的版本上创建的来宾

通常，建议在将qemu/kvm升级到新的主要版本时更新机器类型。但这可能永远不会是一项自动化任务，因为这种变化是可见的。来宾设备的外观可能会发生变化，新功能将向来宾宣布，等等。Linux通常非常善于容忍此类更改，但它在很大程度上取决于来宾的设置和工作负载，因此必须由系统的所有者/管理员进行评估。其他已知的操作系统通常会因更改硬件而产生严重影响。考虑一种类似于将物理设备的所有设备和固件替换到最新版本的机器类型的变化——所有适用于评估机器类型升级的考虑。

像往常一样，在进行重大配置更改时，最好备份来宾定义和磁盘状态，以便能够进行回滚，以防万一。没有通过virsh或类似工具更新机器类型的集成单一命令。这是机器定义的正常部分。因此，更新的方式与大多数其他方式相同。

首先关闭计算机并等待它达到该状态。

virsh关机<yourmachine>#等待

virsh list—非活动#现在应将您的计算机列为“关闭”

然后编辑机器定义并在“机器”属性的“类型”标记中查找类型。

virsh edit<yourmachine><type arch=&apos;x86\_64&apos;machine=&apos;pc-i440fx-xenial&apos;>hvm</type>

将其更改为所需的值。如果您需要通过“-M？”检查哪些类型可用，请注意，虽然提供上游类型作为方便，但只支持Ubuntu类型。在这里，您还可以看到当前的默认设置。通常，强烈建议您更改为较新的类型（如果可能），以利用较新的功能，但也可以利用仅适用于较新设备虚拟化的错误修复。

kvm-M？#列出机器类型，例如：。

pc-i440fx-xenial Ubuntu 16.04 pc（i440fx+PIIX，1996）（默认）。。。

在此之后，您可以再次启动您的客人。您可以根据需要从来宾和主机检查当前机器类型。

virsh start<yourmachine>#通过转储活动xml定义从主机检查

virsh dumpxml<yourmachine>|xmllint--xpath“string（//domain/os/type/@machine）”#或通过dmidecode（如果支持）从来宾处获得的sudo dmidecode | grep产品-A 1产品名称：标准PC（i440FX+PIIX，1996）版本：PC-i440FX-xenial

如果像xml文件一样保留非活动定义，请记住也要更新这些定义。

## 3.云图像和UV工具

#### 3.1. 介绍

由于Ubuntu是许多云平台上使用最多的操作系统之一，稳定安全的云映像的可用性变得非常重要。截至2004年12月12日，云基础设施外部的云映像利用率已得到提高。现在可以使用这些映像创建虚拟机，而无需完整安装。

#### 3.2. 使用uvtool创建虚拟机

从14.04 LTS开始，一个名为uvtool的工具极大地简化了使用云映像生成虚拟机（VM）的任务。uvtool提供了一种简单的机制，可以在本地同步云映像，并使用它们在几分钟内创建新的虚拟机。

##### 3.2.1. UV工具包

要使用uvtool，需要以下软件包及其依赖项：

•uvtool

•uvtool-libvirt

要安装uvtool，请运行：

$sudo apt-y安装工具

这将安装uvtool的主要命令：

•uvt simplestreams libvirt

•uvt kvm

##### 3.2.2. 使用uvt simplestreams libvirt获取Ubuntu云映像

这是uvtool带来的主要简化之一。它知道在哪里可以找到云图像，因此只需要一个命令就可以获得新的云图像。例如，如果要同步amd64体系结构的所有云图像，则uvtool命令应为：

$uvt simplestreams libvirt sync arch=amd64

从互联网下载所有图像需要一段时间后，您将在本地存储一整套云图像。要查看已下载的内容，请使用以下命令：

$uvt simplestreams libvirt查询

release=oneiric arch=amd64 label=release（20130509）release=precise arch=amd64 label=release（20160315）release=quantal arch=amd64 label=release（20140409）release=raring arch=amd64 label=release（20140111）release=saucy arch=release（20140709）release=trusty arch=amd64 label=release（20160314）release=utopic arch=amd64 label=release（20150723）发布=生动arch=amd64标签=发布（20160203）发布=狡猾arch=amd64标签=发布（20160315）发布=xenial arch=amd64标签=beta1（20160223.1）

如果只想同步一个特定的云映像，则需要使用release=和arch=过滤器来确定需要同步的映像。

$uvt simplestreams libvirt同步发布=仿生拱门=amd64

##### 3.2.3.使用uvt kvm创建虚拟机

为了在创建虚拟机后连接到该虚拟机，您必须为Ubuntu用户提供有效的SSH密钥。如果您的环境没有SSH密钥，您可以使用以下命令轻松创建一个SSH密钥：

$ssh keygen生成公共/私有rsa密钥对。

输入保存密钥的文件（/home/ubuntu/.ssh/id\u rsa）：

输入密码短语（无密码短语为空）：

再次输入相同的密码短语：

您的身份已保存在/home/ubuntu/.ssh/id\u rsa中。

您的公钥已保存在/home/ubuntu/.ssh/id\_rsa.pub中。

关键指纹是：4d:ba:5d:57:c9:49:ef:b5:ab:71:14:56:6e:2b:ad:9bubuntu@bionicS密钥的随机艺术图像为：

+--[RSA 2048]----+

| ..|

|o=|

| . \*\*|

|+o+=|

|S….=|

|o.+|

|……哦|

| \* |

|E|

+-----------------+

要使用uvtool创建一个新的虚拟机，请在终端中运行以下操作：

$uvt kvm创建第一个测试

这将使用本地可用的当前LTS云映像创建名为firsttest的VM。如果要指定用于创建VM的版本，需要使用release=filter：

$uvt kvm create secondtest release=仿生uvt kvm wait可用于等待VM创建完成：

$uvt kvm等待第二次测试--不安全

警告：尚未实现安全等待引导完成；请使用--unsecure。

##### 3.2.4.连接到正在运行的VM

虚拟机创建完成后，您可以使用SSH连接到虚拟机：

$uvt kvm ssh secondtest--不安全

目前，需要--unsecure，因此只有在完全信任网络基础设施的情况下，才可以使用此机制连接到VM。

您还可以使用VM的IP地址使用常规SSH会话连接到VM。可以使用以下命令查询地址：

$uvt kvm ip第二次测试

192.168.122.199

$ssh-i~/.ssh/id\u rsaubuntu@192.168.122.199无法确定主机“192.168.122.199（192.168.122.199）”的真实性。

ECDSA密钥指纹为SHA256:8OXAZTRWZTMTv8SC9LYYJUQBU79Z9JP8BUH6G8R8CW。

是否确实要继续连接（是/否）？是警告：已将“192.168.122.199”（ECDSA）永久添加到已知主机列表中。欢迎使用Ubuntu Bionic Beaver（开发分支）（GNU/Linux 4.14.0-X-generic ARCH）

\*文件：https://help.ubuntu.com/

使用Ubuntu Advantage cloud Guest获得云支持：http://www.ubuntu.com/business/services/cloud

可以更新0个包。

0更新是安全更新。

Ubuntu系统附带的程序是自由软件；每个程序的确切分发条款在/usr/share/doc/\*/copyright中的各个文件中进行了描述。

在适用法律允许的范围内，Ubuntu绝对不提供任何担保。

要以管理员（用户“root”）身份运行命令，请使用“sudo<command>”。有关详细信息，请参阅“man sudo\_root”。ubuntu@secondtest:~$

##### 3.2.5.获取正在运行的虚拟机列表

您可以使用以下命令获取系统上运行的虚拟机列表：

$uvt kvm列表第二次测试

##### 3.2.6.销毁您的虚拟机

完成VM后，您可以使用以下方法销毁它：

$uvt kvm销毁第二次测试3.2.7.更多uvt kvm选项

以下选项可用于更改正在创建的VM的某些特征：

•--内存：以兆字节为单位的RAM量。默认值：512。

•--磁盘：操作系统磁盘的大小（GB）。默认值：8。

•--cpu：cpu核心数。默认值：1。

其他一些参数将对cloud init配置产生影响：

•--密码：允许使用Ubuntu帐户和提供的密码登录VM。

•--run script once script\_file：第一次启动时以root用户身份在VM上运行script\_file，但不再运行。

•--软件包列表：在第一次启动时安装软件包列表中指定的逗号分隔的软件包。

uvt kvm手册页中提供了所有可用修改器的完整说明。

#### 3.3.资源

如果您有兴趣了解更多信息，如有疑问或建议，请联系Ubuntu服务器团队：

•IRC:#免费节点上的ubuntu服务器

•邮件列表：位于lists.ubuntu.com[347]的ubuntu服务器

## 4.Ubuntu云

云计算是一种允许按需分配大量资源的计算模型。这些资源（如存储、计算能力、网络和软件）在互联网上随时随地作为服务进行抽象和交付。这些服务的计费方式与公共服务（如ele）使用的服务类似Ubuntu云基础设施使用OpenStack开源软件为公共和私有云构建高度可扩展的云计算。

#### 4.1.安装和配置

由于目前这项复杂技术的发展速度很快，我们请读者查阅上游文档[348]，了解有关安装和配置的所有事项。

#### 4.2.支持和故障排除

社区支持

•OpenStack邮件列表[349]

•OpenStack Wiki搜索[350]

•启动板bug区域[351]

•加入freenode上的IRC频道#openstack。

#### 4.3.资源

•云计算-服务模式[352]

•OpenStack计算[353]

•OpenStack图像服务[354]

•OpenStack对象存储管理指南[355]

•在Ubuntu上安装OpenStack对象存储[356]

• http://cloudglossary.com/

## 5.LXD

LXD（发音为lex dee）是lightervisor，或轻量级容器管理程序。虽然这一说法一直存在争议，但基于最初的学术论文，它已经得到了充分的证明[357]。它还很好地将LXD与LXC区分开来[358]。

LXC（lex-see）是一个在本地系统上创建和管理“容器”的程序

API允许更高级别的管理者（如LXD）管理容器。在某种意义上，可以将LXC与QEMU进行比较，同时将LXD与libvirt进行比较。

LXC API处理“容器”。LXD API处理“远程”，为图像和容器提供服务。这在网络上扩展了LXC功能，并允许简洁地管理容器迁移和容器图像发布等任务。

LXD在某些容器管理任务中使用LXC。但是，它保留自己的容器配置信息并有自己的约定，因此最好不要在LXD容器中手动使用经典的LXC命令。本文档将重点介绍如何在Ubuntu系统上配置和管理LXD。

#### 5.1.在线资源

在线LXD自述中有关于LXD[359]入门的优秀文档。还有一个在线服务器，允许您远程试用LXD[360]。Stephane Graber在LXD 2.0上也有一个优秀的博客系列[361]。最后，还有关于如何使用juju[362]驱动LXD的优秀文档。

本文档将提供一个特定于Ubuntu服务器的LXD视图，重点介绍管理。

#### 5.2.安装

LXD预安装在Ubuntu服务器云映像上。在其他系统上，LXD包可以通过以下方式安装：**sudoapt安装lxd**

这将安装LXD以及推荐的依赖项，包括LXC库和lxcfs。

#### 5.3.内核准备

一般来说，Ubuntu 16.04在默认情况下应该启用所有需要的功能。例外情况是，为了启用交换记帐，必须设置启动参数swapaccount=1。这可以通过将其附加到/etc/default/GRUB中的GRUB\_CMDLINE\_LINUX\_default=变量，然后以root用户身份运行“update GRUB”并重新启动来完成。

#### 5.4.配置

默认情况下，LXD安装在本地UNIX套接字上，组LXD的成员可以与之对话。它没有信任密码设置。它使用位于/var/lib/LXD的文件系统来存储容器。要使用不同的设置配置LXD，请使用LXD init。这将允许您选择：

•目录或ZFS[363]容器后端。如果选择ZFS，则可以选择要使用的块设备，或要用作备份存储的文件大小。

•网络可用性

•远程客户端用于证明其客户端证书的“信任密码”

您必须以root用户身份运行“lxd init”。lxc命令可以作为组lxd成员的任何用户运行。如果用户joe不是组“lxd”的成员，您可以运行：**adduser joe lxd**

新成员资格将在下次登录时生效，或在从现有登录运行“newgrp lxd”后生效。

有关服务器、容器、配置文件和设备配置的更多信息，请参阅源代码附带的最终配置，可在线找到[364]

#### 5.5.创建第一个容器

本节将描述最简单的容器任务。

##### 5.5.1.创建容器

每个新容器都是基于映像、现有容器或容器快照创建的。在安装时，LXD配置有以下映像服务器：

•ubuntu：这为官方ubuntu服务器云图像发布服务。

•ubuntu daily：提供每日开发版本的官方ubuntu服务器云图像。

•图像：这是images.linuxcontainers.org的默认安装别名。这是使用lxc“下载”模板使用的相同图像构建的经典lxc图像。这包括各种发行版和最小的自定义Ubuntu图像。这不是Ubuntu图像的推荐服务器。创建和启动集装箱是

**lxc启动远程：图像容器名称**

图像通过其散列进行标识，但也有别名。“ubuntu”服务器知道许多别名，如“16.04”和“xenial”。可以通过以下方式查看ubuntu服务器上可用的所有图像的列表：**lxc图像列表：**

要查看有关特定图像的更多信息，包括已知的所有别名，可以使用：**lxc图像信息ubuntu:xenial**

您通常可以使用发行名（“xenial”）或发行号（16.04）来引用Ubuntu映像。此外，“lts”是最新受支持的lts发行版的别名。要选择不同的体系结构，您可以指定所需的体系结构：**lxc图像信息ubuntu:lts/arm64**

现在，让我们开始我们的第一个容器：

**lxc发布ubuntu:xenial x1**

这将下载当前架构的官方Xenial cloud映像，然后使用该映像创建一个容器，并最终启动它。命令返回后，您可以使用以下命令查看它：

**lxc列表lxc信息x1**

并使用以下命令在其中打开外壳：

**lxc exec x1 bash**

“试用”页面提供了可用于管理容器的命令的完整概要。

现在已经下载了“xenial”映像，它将保持同步，直到（默认情况下）10天内没有基于它创建新容器。之后，它将被删除。

#### 5.6.LXD服务器配置

默认情况下，LXD是套接字激活的，并且配置为仅在本地UNIX套接字上侦听。当您第一次查看进程列表时，LXD可能没有运行，但任何LXC命令都会启动它。例如：**lxc列表**

这将创建您的客户端证书，并与LXD服务器联系以获取容器列表。要通过网络访问服务器，您可以使用以下命令设置http端口：**lxc config set core.https\_地址：8443**

这将告诉LXD侦听所有地址上的端口8843。

##### 5.6.1.认证

默认情况下，LXD将允许组“LXD”的所有成员（默认情况下包括组管理员的所有成员）通过UNIX套接字与它进行通信。通过网络进行通信是使用服务器和客户端证书进行授权的。

在客户端c1希望使用远程r1之前，必须使用以下方式注册r1：**lxc remote add r1 r1.example.com:8443**

将显示r1证书的指纹，以允许c1处的用户拒绝假证书。服务器将依次通过以下两种方式之一验证c1是否受信任。第一种方式是使用以下方式提前从任何已注册的客户端注册该证书：

**lxc配置信任添加r1 certfile.crt**

现在，当客户端将r1添加为已知的远程服务器时，它将不需要提供密码，因为服务器已经信任它。

另一种方法是在初始配置时使用“lxd init”，或者在实际配置之后使用r1配置“信任密码”

**lxc config set core.trust\u密码**

然后，当客户端将r1注册为已知远程服务器时，可以提供密码。

##### 5.6.2.后备仓库

LXD支持多个备份存储。建议的备份存储是ZFS，但并非在所有平台上都可用。支持的备份存储包括：

•ext4：这是默认设置，并且最容易使用。使用ext4备份存储，容器和图像仅作为目录存储在主机文件系统上。启动新容器需要复制整个文件系统，10个容器将占用一个容器10倍的空间。

•ZFS：如果您的体系结构（amd64、arm64或ppc64le）支持ZFS，则可以使用“LXD init”将LXD设置为使用它。如果您已经配置了ZFS池，则可以通过设置ZFS\_pool\_name配置键告知LXD使用它：**lxc config set storage.zfs\_pool\_name lxd**

使用ZFS，启动新容器的速度很快，因为文件系统是作为映像文件系统的一个写拷贝克隆启动的。请注意，除非容器具有特权（见下文），否则LXD需要在容器启动之前更改所有文件的所有权，但这速度很快，并且只更改很少的实际文件系统数据。

•Btrfs:Btrfs与ZFS具有许多相同的优点。要将Btrfs用作LXD备份存储，只需在/var/lib/LXD下安装一个Btrfs文件系统。LXD将检测到这一点，并在启动新容器或快照容器时利用Btrfs子卷功能。

•LVM：要使用名为“lxd”的LVM卷组，您可以使用命令告诉lxd将其用于容器和图像

**lxc config set storage.lvm\_vg\_name lxd**

启动新容器时，其rootfs将作为lv克隆启动。它将立即装载，以便可以移动文件UID，然后卸载。容器快照也将作为lv快照创建。

#### 5.7.容器配置

容器是根据一组配置文件（将在下一节中介绍）和一组特定于容器的配置文件进行配置的。首先应用配置文件，以便特定于容器的配置可以覆盖配置文件配置。

容器配置包括架构等属性、CPU和RAM等资源限制、包括apparmor限制覆盖在内的安全详细信息以及应用于容器的设备。

设备可以有多种类型，包括UNIX字符、UNIX块、网络接口或“磁盘”。要将主机装载插入容器，将使用“磁盘”设备类型。例如，要在容器c1的/opt处装载/opt，可以使用：请参阅：**lxc配置设备添加c1 opt磁盘源=/opt路径=opt lxc帮助配置**

有关编辑容器配置的详细信息。您也可以使用：**配置编辑c1**

在指定的$EDITOR中编辑整个c1配置。配置顶部的注释将显示正确语法的示例，以帮助管理员开始运行。如果退出$EDITOR时编辑的配置无效，则$EDITOR将重新启动。

#### 5.8. 轮廓

配置文件是可应用于多个容器的命名配置集合。例如，默认情况下，使用“lxc-launch”创建的所有容器都包含“default”配置文件，该配置文件提供网络接口“eth0”。

要屏蔽将从配置文件继承但不应位于最终容器中的设备，请定义一个名称相同但类型为“无”的设备：

**lxc配置设备添加c1 eth1无**

#### 5.9. 筑巢

所有容器都共享相同的主机内核。这意味着暴露于容器的功能和恶意容器的主机安全性之间总是存在固有的权衡。因此，默认情况下，容器受到嵌套子容器所需功能的限制。为了在lxd容器下运行lxc或lxd容器，“security.nesting”功能必须设置为true：

**lxc配置集container1 security.nesting true**

完成后，container1将能够启动子容器。

为了运行嵌套在非特权容器下的非特权（LXD中的默认值）容器，您需要确保足够宽的UID映射。请参阅下面的“UID映射”部分。

##### 5.9.1. 码头工人

为了便于在LXD容器中运行docker容器，提供了“docker”配置文件。要使用docker配置文件启动新容器，可以运行：**lxc启动xenial container1-p默认值-p docker**

请注意，目前Ubuntu 16.04中的docker包已经过修补，以便于在容器中运行。预计这一支持很快就会到达上游。

请注意，还需要“cgroup namespace”支持。这在16.04内核和4.6上游源代码中都有。

#### 5.10. 限制

LXD支持对容器可以使用的资源的灵活约束。限制分为以下几类：

•CPU：以多种方式限制容器可用的CPU。

•磁盘：配置负载下I/O请求的优先级

•RAM：配置内存和交换可用性

•网络：配置负载下的网络优先级

•进程：限制容器中并发进程的数量。

有关LXD已知限制的完整列表，请参阅配置文档[365]。

#### 5.11. UID映射和特权容器

默认情况下，LXD创建非特权容器。这意味着容器中的root是主机上的非root UID。它对容器拥有的资源有特权，但对主机没有特权，这使得容器中的root用户大致相当于主机上的一个没有特权的用户。（主要的例外是通过系统调用接口暴露的攻击面增加）

简单地说，在一个非特权容器中，65536个UID被“转移”到容器中。例如，主机上容器中的UID 0可能是100000，容器中的UID 1可能是100001，等等，直到165535。UID和GID的起始值分别由/etc/subuid和/etc/subgid文件中的“根”条目确定。（参见subuid（5）手册第[366]页）。

通过将security.privileged标志设置为true，可以请求容器在没有UID映射的情况下运行：

**lxc配置集c1 security.privileged true**

但是请注意，在这种情况下，容器中的root用户是主机上的root用户。

#### 5.12.公寓

默认情况下，LXD使用apparmor配置文件限制容器，该配置文件保护容器彼此不受影响，并保护主机不受容器影响。例如，这将防止一个容器中的root向另一个容器中的root发送信号，即使它们具有相同的uid映射。它还防止写入危险的、未命名空间的文件，如许多sysctls和/proc/sysrq触发器。

如果需要为容器c1修改容器的apparmor策略，则可以在“raw.apparmor”配置密钥中添加特定的apparmor策略行。

#### 5.13.Seccomp

所有容器都受默认的seccomp策略限制。此策略可防止某些危险操作，如强制umounts、内核模块加载和卸载、kexec和系统调用时的open\_by\_handle\_。无法修改seccomp配置，但可以使用raw.lxc请求完全不同的seccomp策略（或无）（见下文）。

#### 5.14.原始LXC配置

LXD配置容器以实现主机安全性和容器可用性的最佳平衡。强烈建议尽可能使用默认值，并根据需要使用LXD配置键请求LXD进行修改。但是，有时可能需要与底层lxc驱动程序本身对话。这可以通过指定lxc configu来完成“raw.lxc”LXD配置键中的定量项目。这些项目必须是lxc.container.conf（5）手册页[367]中记录的有效项目。

#### 5.15.图像和容器

LXD是基于图像的。当您创建第一个容器时，通常会使用现有图像来创建。

LXD预先配置了三个默认图像遥控器：

•ubuntu：这是一个基于simplestreams的[368]远程服务发布的ubuntu云图像。

•ubuntu daily：这是另一款基于simplestreams的远程设备，提供“每日”ubuntu云图像。这些图像速度更快，但稳定性可能较差。

•图像：这是一个远程发布许多发行版的尽力而为的容器图像，使用社区提供的构建脚本创建。

要查看其中一台服务器上的可用图像，您可以使用：**lxc图像列表：**

为了便于参考，大多数图像都有几个别名。要查看别名的完整列表，可以使用

**lxc图像别名列表图像：**

可以使用任何别名或图像指纹来指定如何创建新容器。例如，要创建amd64 Ubuntu 14.04容器，一些选项包括：

**lxc启动ubuntu:14.04 trusty1 lxc启动ubuntu:trusty trusty1 lxc启动ubuntu:trusty/amd64 trusty1 lxc启动ubuntu:lts trusty1**

“lts”别名总是指最新发布的lts映像。

##### 5.15.1.快照

可以使用“lxc move”命令重命名和实时迁移容器：

**lxc移动c1最终测试版**

也可以对其进行快照：**lxc快照c1 YYYY-MM-DD**

随后可以通过恢复快照恢复对c1的更改：**lxc恢复u1 YYYY-MM-DD**

还可以通过复制容器或快照来创建新容器：**lxc副本u1/YYYY-MM-DD测试容器**

##### 5.15.2.发布图像

当容器或容器快照准备好供其他人使用时，可以使用将其发布为新图像；

**lxc发布u1/YYYY-MM-DD——别名foo-2.0**

默认情况下，发布的映像将是私有的，这意味着LXD将不允许没有受信任证书的客户端查看它们。如果映像可以安全地供公众查看（即不包含私有信息），则

“public”标志可以在发布时使用

**lxc publish u1/YYYY-MM-DD--别名foo-2.0 public=true**

或事后使用

**lxc图像编辑foo-2.0**

改变公共领域的价值。

##### 5.15.3.图像导出和导入

图像可以导出为tarballs，也可以从tarballs导入：

**lxc图像导出foo-2.0 foo-2.0.tar.gz**

**lxc图像导入foo-2.0.tar.gz--别名foo-2.0--公共**

#### 5.16.故障排除

要查看关于LXD本身的调试信息，请在基于systemd的主机上使用

**journalctl-u lxd**

在基于Upstart的系统上，您可以在/var/log/Upstart/lxd.log中找到日志。要使lxd提供更多关于它所服务的请求的信息，请在lxd的参数中添加“-debug”。在systemd中，将“-debug”附加到/lib/systemd/system/lxd.service中的“ExecStart=”行。在Upstart中，将其附加到/etc/init/lxd.conf中的exec/usr/bin/lxd行。

容器c1的容器日志文件可通过以下方式查看：**lxc信息c1——显示日志**

使用的配置文件可以在/var/log/lxd/c1/lxc.conf下找到，而apparmor配置文件可以在/var/lib/lxd/security/apparmor/profiles/c1和/var/lib/lxd/security/seccomp/c1中找到。

## 6.LXC

容器是一种轻量级虚拟化技术。与Qemu或VMware等完全虚拟化相比，它们更类似于增强型chroot，因为它们不模拟硬件，而且容器与主机共享相同的操作系统。容器类似于Solaris区域或BSD监狱。Linuxvserver和OpenVZ是两种预存在的虚拟化sting是独立开发的容器实现，比如Linux的功能。事实上，容器是在vserver和OpenVZ功能上游工作的结果。

有两个容器的用户空间实现，每个实现都利用相同的内核功能。Libvirt通过连接到“LXC://”允许通过LXC驱动程序使用容器。这非常方便，因为它支持与其他驱动程序相同的用法。另一个实现，简称为“LXC”，与Libvirt不兼容，但使用更多的用户空间工具更灵活。可以在两者之间切换，尽管存在可能导致混淆的特性。

在本文档中，我们将主要介绍lxc软件包。由于libvirt lxc容器缺乏Apparmor保护，因此通常不建议使用libvirt lxc。

在本文档中，容器名称将显示为CN、C1或C2。

#### 6.1.安装

lxc软件包可以使用

**sudoapt安装lxc**

这将引入所需的和推荐的依赖项，并为容器使用设置一个网桥。如果您希望使用非特权容器，则需要确保用户有足够的已分配子UID和子GID，并且可能希望允许用户将容器连接到网桥（见第6.2.3节，“基本非特权用法”[p.364]）。

#### 6.2.基本用法

LXC可以以两种不同的方式使用—特权，以root用户身份运行LXC命令；非特权，以非root用户身份运行LXC命令。（根用户启动非特权容器是可能的，但这里没有描述。）非特权容器的限制更大，例如无法创建设备节点或装载块备份的文件系统。但是，由于容器中的根用户标识映射到主机上的非根用户标识，因此它们对主机的危险性较小。

##### 6.2.1.基本特权使用

要创建特权容器，只需执行以下操作：

**sudo lxc create--模板下载--名称u1**

或者，缩写

**sudo lxc create-t下载-n u1**

这将以交互方式要求下载容器根文件系统类型，特别是发行版、发行版和体系结构。要以非交互方式创建容器，可以在命令行上指定以下值：

**sudolxc create-t download-nu1--distubuntu--release bionic--arch amd64**

或

**sudolxc create-t下载-nu1--d ubuntu-r仿生-a amd64**

现在，您可以使用lxc ls列出容器，使用lxc info获取详细的容器信息，使用lxc start启动和lxc stop停止容器。如果ssh不是选项，则使用lxc attach和lxc控制台可以输入容器。lxc destroy将删除容器，包括其rootfs。有关每个命令的详细信息，请参阅手册页面。示例会话可能如下所示：

**苏多lxc ls——别致**

**sudo lxc start--name u1--守护进程sudo lxc info--name u1 sudo lxc stop--name u1 sudo lxc destroy--name u1**

##### 6.2.2.用户名称空间

非特权容器允许用户在没有任何根权限的情况下创建和管理容器。支持此功能的功能称为用户命名空间。用户命名空间是分层的，父命名空间中的特权任务能够将其ID映射到子命名空间。默认情况下，主机上的每个任务都在初始用户命名空间中运行命名空间，其中完整范围的ID映射到完整范围。这可以通过查看/proc/self/uid\_map和/proc/self/gid\_map看到，这两个映射都将显示“0 0 4294967295”当从初始用户名称空间读取时。从Ubuntu 14.04开始，当创建新用户时，默认情况下会向他们提供一系列用户id。分配id的列表可以在文件/etc/subuid和/etc/subgid中看到。有关详细信息，请参阅各自的手册页。按照惯例，subuid和subgid从id 100000开始，以避免冲突与系统用户联系。

如果用户是在早期版本中创建的，则可以使用usermod为其授予一系列ID，如下所示：

**sudo用户模式-v 100000-200000-w 100000-200000用户1**

程序newuidmap和newgidmap是uidmap包中的setuid根程序，lxc在内部使用这些程序将子UID和子GID从主机映射到非特权容器中。它们确保用户仅映射由主机配置授权的ID。

##### 6.2.3.基本非特权用途

要创建非特权容器，首先需要几个步骤。您需要创建默认容器配置文件，指定所需的id映射和网络设置，并配置主机以允许非特权用户连接到主机网络。下面的示例假定您的映射用户和组id范围为100000-165536。检查您的实际用户和组id范围，并相应修改示例：

**grep$USER/etc/subuid grep$USER/etc/subgid**

**mkdir-p~/.config/lxc**

**echo“lxc.id\_map=u 0 100000 65536”>~/.config/lxc/default.conf echo“lxc.id\_map=g 0 100000 65536”>>~/.config/lxc/default.conf echo“lxc.network.type=veth”>~/.config/lxc/default.conf echo“lxc.network.link=lxcbr0”>>~/.config/lxc/default.conf echo“$USER-veth lx0 2”| sudo tee-a/etc/lxc/lxc/lxc/lxc/lxc-usernet**

在此之后，您可以使用与特权容器相同的方法创建非特权容器，而无需使用sudo。

**lxc create-t download-n u1--d ubuntu-r bionic-a amd64 lxc start-n u1-d lxc attach-n u1 lxc stop-n u1 lxc destroy-n u1**

##### 6.2.4.嵌套

为了在容器内运行容器（称为嵌套容器），父容器配置文件中必须有两行：

lxc.mount.auto=cgroup

lxc.aa\_profile=lxc容器默认值，带嵌套

第一个将使cgroup manager套接字绑定到容器中，以便容器内的lxc能够管理其嵌套容器的cgroup。第二个将使容器在更宽松的Apparmor策略中运行，该策略允许容器执行启动容器所需的装载。请注意，使用此策略时与常规策略或非特权容器相比，使用特权容器的安全性要低得多。有关更多信息，请参阅第6.9节“Apparmor”[p.368]。

#### 6.3.全局配置

LXC查阅了以下配置文件。对于特权使用，它们位于/etc/LXC下，而对于非特权使用，它们位于~/.config/LXC下。

•lxc.conf可以选择为几个lxc设置指定备用值，包括lxcpath、默认配置、要使用的cgroup、cgroup创建模式以及lvm和zfs的存储后端设置。

•default.conf指定每个新创建的容器应包含的配置。这通常至少包含一个网络部分，对于非特权用户，还包含一个id映射部分

•lxc-usernet.conf指定非特权用户如何将其容器连接到主机拥有的网络。

lxc.conf和default.conf都位于/etc/lxc和$HOME/.config/lxc下，而lxc-usernet.conf仅位于主机范围内。

默认情况下，对于根用户，容器位于/var/lib/lxc下，否则位于$HOME/.local/share/lxc下。

可以使用“-P |--lxcpath”参数为所有lxc命令指定位置。

#### 6.4.联网

默认情况下，LXC为每个容器创建一个专用网络命名空间，其中包括一个第2层网络堆栈。容器通常通过将物理NIC或veth隧道端点传递到容器中来连接到外部世界。LXC在主机启动时创建一个网桥lxcbr0。容器使用默认配置创建n将有一个远程端插入lxcbr0网桥的veth NIC。NIC一次只能存在于一个命名空间中，因此传递到容器中的物理NIC在主机上不可用。

可以在没有专用网络命名空间的情况下创建容器。在这种情况下，容器将可以像其他任何应用程序一样访问主机网络。请注意，如果容器运行的是upstart（如Ubuntu）发行版，这尤其危险，因为与init（如shutdown）通信的程序将通过网络进行通信将Unix域套接字抽象到主机的upstart，并关闭主机。

要根据域名为lxcbr0上的容器提供持久ip地址，可以将条目写入/etc/lxc/dnsmasq.conf，如下所示：

dhcp主机=lxcmail，10.0.3.100 dhcp主机=ttrss，10.0.3.101

如果希望容器可以公开访问，有几种方法可以实现。例如，使用iptables将主机端口转发到容器

iptables-t nat-A预路由-p tcp-i eth0-dport 587-j DNAT \-到目标10.0.3.100:587

另一种方法是桥接主机的网络接口（请参阅《Ubuntu服务器指南》的网络配置章节，第1.4节，“桥接”[p.46]）。然后，在容器配置文件中指定主机的桥接，以代替lxcbr0

lxc.network.type=veth lxc.network.link=br0

最后，您可以要求LXC将macvlan用于容器的NIC。请注意，这有局限性，并且根据配置，可能不允许容器与主机本身通信。因此，其他两个选项是首选的，并且更常用。

有几种方法可以确定容器的ip地址。首先，可以使用lxc ls--fancy打印所有正在运行的容器的ip地址，或者使用lxc info-i-H-n C1打印C1的ip地址。如果主机上安装了dnsmasq，还可以在/etc/dnsmasq.conf中添加一个条目，如下所示server=/lxc/10.0.3.1dnsmasq将在本地解析C1.lxc，以便您可以执行以下操作：

ping C1 ssh C1

有关更多信息，请参阅lxc.conf手册页以及/usr/share/doc/lxc/examples/下的示例网络配置。

#### 6.5.LXC启动

LXC没有长时间运行的守护进程。但是它有三个upstart作业。

•/etc/init/lxc-net.conf：是一个可选作业，仅当/etc/default/lxc-net指定USE\_lxc\_BRIDGE（默认情况下为true）时才会运行。它为容器设置一个可使用的网桥。

•/etc/init/lxc.conf加载lxc apparmor配置文件并可选择启动任何autostart容器。如果在/etc/default/lxc中将lxc\_AUTO（默认为true）设置为true，则将忽略autostart容器。有关autostart容器的更多信息，请参阅lxc autostart手册页面。

•/etc/init/lxc-instance.conf被/etc/init/lxc.conf用来自动启动容器。

#### 6.6.后备仓库

LXC支持多个容器根文件系统的备份存储。默认情况下是一个简单的目录备份存储，因为只要底层文件系统足够大，它就不需要预先定制主机。它也不需要根权限来创建备份存储，因此它可以无缝地用于非特权使用。rootfs用于privileged目录支持的容器（默认情况下）位于/var/lib/lxc/C1/rootfs下，而非特权容器的rootfs位于~/.local/share/lxc/C1/rootfs下。如果在lxc.system.com中指定了自定义lxcpath，则容器rootfs将位于$lxcpath/C1/rootfs下。

目录支持的容器C1的快照克隆C2变为覆盖的容器，其rootfs称为overlayfs:/var/lib/lxc/C1/rootfs:/var/lib/lxc/C2/delta0。其他后备存储类型包括loop、btrfs、LVM和zfs。

btrfs支持的容器看起来很像目录支持的容器，其根文件系统位于同一位置。但是，根文件系统包含一个子卷，因此使用子卷快照创建快照克隆。

支持LVM的容器的根文件系统可以是任何单独的LV。可以在lxc.conf中指定默认VG名称。文件系统类型和大小可以使用lxcreate对每个容器进行配置。

zfs支持的容器的rootfs是一个单独的zfs文件系统，安装在传统的/var/lib/lxc/C1/rootfs位置下。zfsroot可以在lxc create中指定，默认值可以在lxc.system.conf中指定。

有关使用各种备份存储创建容器的更多信息，请参见lxc创建手册页面。

#### 6.7. 模板

创建容器通常涉及为容器创建根文件系统。lxc create将这项工作委托给模板，通常每个发行版都有模板。lxc附带的lxc模板可以在/usr/share/lxc/templates下找到，其中包括创建Ubuntu、Debian、Fedora、Oracle、centos和gentoo容器的模板。

在大多数情况下，创建分发映像需要能够创建设备节点，通常需要在其他分发中无法使用的工具，并且通常非常耗时。因此，lxc附带了一个特殊的下载模板，可以从中央lxc服务器下载预构建的容器映像。最重要的用例是允许非root用户简单地创建非特权容器，例如，他们不能轻松地运行debootstrap命令。

运行lxc create时，后面的所有选项都传递给模板。在以下命令中，-name，-template和--bdev传递给lxc create，而--release传递给模板：

**lxc创建--模板ubuntu--名称c1--bdev循环--发布仿生**

通过将--help和模板名传递给lxcreate，可以获得任何特定容器支持的选项的帮助。例如，有关下载模板的帮助，

**lxc创建--模板下载--帮助**

#### 6.8. 自动启动

LXC支持在系统启动时标记要启动的容器。在Ubuntu 14.04之前，这是通过/etc/lxc/auto目录下的符号链接完成的。从Ubuntu 14.04开始，它是通过容器配置文件完成的。条目

**lxc.start.auto=1 lxc.start.delay=5**

这意味着容器应该在引导时启动，系统应该在启动下一个容器之前等待5秒钟。LXC还支持容器的排序和分组，以及通过autostart组重新启动和关闭。有关更多信息，请参阅lxc autostart和lxc.container.conf的手册页面。

#### 6.9. 公寓

LXC附带了一个默认的Apparmor配置文件，旨在保护主机免受容器内权限的意外滥用。例如，容器将无法写入/proc/sysrq触发器或大多数/sys文件。

通过运行lxc start输入usr.bin.lxc-start配置文件。此配置文件主要防止lxc start在容器的根文件系统之外安装新的文件系统。在执行容器的init之前，LXC请求切换到容器的概要文件。默认情况下，此配置文件是在/etc/apparmor.d/lxc/lxc-default中定义的lxc容器默认策略。此配置文件防止容器访问许多危险的路径，也防止容器装载大多数文件系统。

容器中的程序不能被进一步限制——例如，MySQL在容器配置文件下运行（保护主机），但不能进入MySQL配置文件（保护容器）。lxc execute不会输入Apparmor配置文件，但它生成的容器将受到限制。

##### 6.9.1. 自定义容器策略

如果您发现lxc启动失败是由于合法访问被其Apparmor策略拒绝，您可以通过执行以下操作禁用lxc启动配置文件：

sudo apparmor\_解析器-R/etc/apparmor.d/usr.bin.lxc-start sudo ln-s/etc/apparmor.d/usr.bin.lxc-start/etc/apparmor.d/disabled/

这将使lxc开始运行时不受限制，但会继续限制容器本身。如果您还希望禁用容器限制，那么除了禁用usr.bin.lxc-start配置文件外，还必须添加：lxc.aa\_profile=unconfined

到容器的配置文件。

LXC附带了一些容器的备用策略。如果希望在容器中运行容器（嵌套），那么可以通过向容器配置文件添加以下行，使用lxc容器默认值和嵌套配置文件

lxc.aa\_profile=lxc容器默认值，带嵌套

如果希望在容器中使用libvirt，则需要通过取消注释以下行来编辑该策略（在/etc/apparmor.d/lxc/lxc default with nesting中定义）：

mount fstype=cgroup->/sys/fs/cgroup/\*\*，

并重新加载策略。

请注意，具有特权容器的嵌套策略远不如默认策略安全，因为它允许容器在非标准位置重新装载/sys和/proc，从而绕过apparmor保护。

非特权容器没有这个缺点，因为容器根不能写入根拥有的proc和sys文件。

lxc附带的另一个概要文件允许容器装载块文件系统类型，如ext4。这在某些情况下很有用，比如maas配置，但通常被认为是不安全的，因为内核中的超级块处理程序没有被审计以安全处理不受信任的输入。

如果需要在自定义概要文件中运行容器，可以在/etc/apparmor.d/lxc/下创建新概要文件。它的名称必须以lxc开头-以便允许lxc start转换到该概要文件。lxcdefault概要文件包括可重用的抽象文件/etc/apparmor.d/abstractions/lxc/containerbase。因此，启动新配置文件的一种简单方法是执行相同的操作，然后在策略底部添加额外的权限。

创建策略后，使用以下方法加载策略：

sudo apparmor\_解析器-r/etc/apparmor.d/lxc-containers

重新启动后将自动加载配置文件，因为它是由文件/etc/apparmor.d/lxc容器提供的。最后，要使容器CN使用这个新的lxc CN配置文件，请在其配置文件中添加以下行：

lxc.aa\_profile=lxc CN profile

#### 6.10. 对照组

控制组（cgroups）是一个核心功能，提供分层任务分组和每个cgroups资源的计算和限制。它们在容器中用于限制块和字符设备访问以及冻结（挂起）容器。它们还可以进一步用于限制内存使用和阻塞i/o、保证最小cpu共享以及将容器锁定到特定cpu。

默认情况下，特权容器CN将分配给名为/lxc/CN的cgroup。在名称冲突的情况下（使用自定义LXCPath时可能会发生），将在cgroup名称后追加后缀“-n”，其中n是从0开始的整数。

默认情况下，特权容器CN将分配给启动容器的任务的cgroup下名为CN的cgroup，例如/usr/1000.user/1.session/CN。容器根目录将被赋予目录（但不是所有文件）的组所有权，以便允许它创建新的子cgroup。

从Ubuntu14.04开始，LXC使用cgroup管理器（cgmanager）来管理cgroup。cgroup管理器通过Unix套接字/sys/fs/cgroup/cgmanager/sock接收D-Bus请求。为方便安全嵌套容器，该行

**lxc.mount.auto=cgroup**

可以添加到容器配置，从而将/sys/fs/cgroup/cgmanager目录装入容器。容器应依次启动cgroup管理代理（如果容器中安装了cgmanager包，则默认情况下会启动），该代理将/sys/fs/cgroup/cgmanager目录移动到/sys/fs/cgroup/cgmanager.lower，然后在其自己的套接字/sys/fs/cgroup/cgmanager/sock上开始侦听对代理的请求。宿主cgmanager将确保嵌套容器不能逃逸其分配的cgroup或发出未经授权的请求。

#### 6.11. 克隆

对于快速资源调配，您可能希望根据需要自定义规范容器，然后制作多个副本。这可以通过lxc克隆程序完成。

克隆是另一个容器的快照或副本。副本是从原始容器复制的新容器，在主机上占用的空间与原始容器相同。快照利用底层备份存储的快照功能创建引用第一个备份的写时拷贝容器。可以从btrfs、LVM、zfs和目录备份容器创建快照。每个备份存储都有自己的特性—例如，未配置thinpool的LVM容器不能支持快照的快照；在释放所有快照之前，无法删除带有快照的zfs容器；必须更仔细地规划LVM容器，因为底层文件系统可能不支持增长；btrfs没有任何这些缺点，但fsync性能降低，导致dpkg速度变慢。

目录打包容器的快照是使用覆盖文件系统创建的。例如，特权目录支持的容器C1的根文件系统位于/var/lib/lxc/C1/rootfs下。将启动名为C2的C1快照克隆，并将C1的rootfs以只读方式安装在/var/lib/lxc/C2/delta0下。重要的是，在这种情况下，不允许运行C1或在C2运行时拆除C1。建议将C1视为规范的基本容器，而只使用它的快照。

给定一个名为C1的现有容器，可以使用创建副本：快照可以使用：**sudo lxc克隆-o C1-n C2 sudo lxc克隆-s-o C1-n C2**

有关更多信息，请参阅lxc克隆手册页。

##### 6.11.1. 快照

为了更容易地支持使用快照克隆进行迭代容器开发，LXC支持快照。在容器C1上工作时，在进行潜在危险或难以恢复的更改之前，可以创建快照

**sudo lxc快照-n C1**

它是/var/lib/lxcsnaps或$HOME/.local/share/lxcsnaps下名为“snap0”的快照克隆。下一个快照将被称为“snap1”，等等。可以使用lxc snapshot-L-n C1列出现有快照，并且可以使用lxc snapshot-r snap1-n C1恢复快照-擦除当前C1容器。执行restore命令后，snap1快照将继续存在，先前的C1将被擦除并替换为snap1快照。

btrfs、lvm、zfs和overlayfs容器支持快照。如果在directorybacked容器上调用lxc快照，则会记录一个错误，并将快照创建为副本克隆。原因是，如果用户创建目录备份容器的overlayfs快照，然后对目录备份容器进行更改，则原始容器更改将部分反映在快照中。如果需要目录备份容器C1的快照，则应创建C1的overlayfs克隆，不应再次触摸C1，并且可以随意编辑和快照overlayfs克隆

**lxc克隆-s-o C1-n C2**

**lxc start-n C2-d#进行一些更改**

**lxc停止-n C2 lxc快照-n C2 lxc启动-n C2#等**

##### 6.11.2. 临时容器

虽然快照对于图像的长期增量开发很有用，但临时容器将快照用于快速的一次性容器。给定一个基本容器C1，您可以使用

**lxc启动瞬时-o C1**

容器以C1的快照开始。登录容器的说明将打印到控制台。关闭后，临时容器将被销毁。有关更多选项，请参阅lxc开始临时手册页面。

#### 6.12. 生命周期管理挂钩

从Ubuntu 12.10开始，可以定义在容器生命周期的特定点执行的钩子：

•在容器TTY、控制台或装载启动之前，在主机名称空间中运行预启动挂钩。如果在此挂钩中安装了任何支架，则应在后限位挂钩中清理。

•预装载挂钩在容器的名称空间中运行，但在根文件系统被装载之前运行。

当容器关闭时，在此挂钩中完成的安装将自动清理。

•挂载钩子在容器文件系统挂载之后，但在容器调用pivot\_root以更改其根文件系统之前运行。

•在执行容器的初始化之前，立即运行启动挂钩。由于这些命令是在旋转到容器的文件系统后执行的，因此必须将要执行的命令复制到容器的文件系统中。

•停止后挂钩在集装箱关闭后执行。

如果任何钩子返回错误，容器的运行将中止。任何停止后挂钩仍将执行。脚本生成的任何输出都将以调试优先级记录。

请参阅lxc.container.conf手册页面，了解用于指定挂钩的配置文件格式。lxc包附带了一些示例钩子，作为如何编写和使用此类钩子的示例。

#### 6.13. 安慰

容器具有可配置数量的控制台。一个始终存在于容器的/dev/console上。除非指定了-d选项，否则这将显示在运行lxc start的终端上。可以使用-c console file选项将/dev/console上的输出重定向到lxc start文件。额外控制台的数量由lxc.tty变量指定，通常设置为4。这些控制台显示在/dev/ttyN上（对于1<=N<=4）。要从主机登录控制台3，请使用：**sudo lxc控制台-n容器-t 3**

或者，如果未指定-tn选项，将自动选择未使用的控制台。要退出控制台，请使用转义序列Ctrl-a q。请注意，由于lxcstart没有-d选项，因此转义序列在控制台中不起作用。

每个容器控制台实际上是主机（不是来宾）pty挂载中的一个Unix98 pty，绑定挂载在来宾的/dev/ttyN和/dev/console上。因此，如果来宾卸载这些设备或试图访问实际的字符设备4:N，那么它将不会向LXC控制台提供getty服务。（使用默认设置，容器将无法访问该字符设备，因此getty将失败。）当引导脚本盲目地挂载新的/dev时，很容易发生这种情况。

#### 6.14. 故障排除

##### 6.14.1. 登录中

如果启动容器时出现问题，第一步应该是从LXC获取完整日志：**sudo lxc start-n C1-l trace-o debug.out**

这将导致lxc以最详细的级别进行日志记录、跟踪，并将日志信息输出到名为“debug.out”的文件中。如果文件debug.out已经存在，将附加新的日志信息。

##### 6.14.2. 监控集装箱状态

有两个命令可用于监视容器状态的更改。lxc监视器监视一个或多个容器的任何状态更改。它像使用-n选项一样使用容器名称，但在本例中，容器名称可以是posix正则表达式，以允许监视所需的容器集。lxcmonitor在打印容器更改时继续运行。lxc wait等待特定状态更改，然后退出。例如，

**sudo lxc监视器-n cont[0-5]\***

将所有状态更改打印到与列出的正则表达式匹配的任何容器，而

**sudo lxc wait-n cont1-s“停止|冻结”**

将等待容器cont1进入停止或冻结状态，然后退出。

##### 6.14.3. 贴上

从Ubuntu 14.04开始，可以附加到容器的名称空间。最简单的情况就是简单地做

**sudo lxc连接-n C1**

它将启动一个附加到C1名称空间的shell，或者，实际上是在容器内部。附加功能非常灵活，允许附加到容器名称空间和安全上下文的子集。有关更多信息，请参阅手册页。

##### 6.14.4. 容器初始化详细性

如果LXC完成了容器启动，但容器初始化未能完成（例如，没有显示登录提示），则从初始化进程请求额外的详细信息可能会很有用。对于upstart容器，这可能是：**sudo lxc start-n C1/sbin/init loglevel=debug**

例如，您也可以启动一个完全不同的程序来代替init

**sudo lxc启动-n C1/bin/bash sudo lxc启动-n C1/bin/sleep 100 sudo lxc启动-n C1/bin/cat/proc/1/status**

#### 6.15. LXC API

现在可以通过liblxc导出的API访问大部分LXC功能，该API的绑定有多种语言，包括Python、lua、ruby和go。

下面是一个使用python绑定（python3 lxc包中提供）的示例，该绑定创建并启动容器，然后等待容器关闭：

#苏多蟒蛇3

Python 3.2.3（默认值，2012年8月28日，08:26:03）

[GCC 4.7.1 20120814（预发布）]在linux2上键入“帮助”、“版权”、“信用证”或“许可证”以获取更多信息。>>导入lxc\uuuuu main\uuuuuuuu:1：警告：python lxc API还不稳定，将来可能在任何时候发生更改。>>>c=lxc.Container（“C1”）>>c.create（“ubuntu”）

符合事实的

>>>c.开始（）

正确>>>c.等待（“已停止”）

符合事实的

#### 6.16. 安全

命名空间将ID映射到资源。通过不向容器提供引用资源的任何id，可以保护资源。这是提供给容器用户的一些安全性的基础。例如，IPC名称空间是完全隔离的。但是，其他名称空间存在各种漏洞，这些漏洞允许不适当地将特权从一个容器应用到另一个容器或主机。

默认情况下，LXC容器在Apparmor策略下启动，以限制某些操作。有关AppArmor与lxc集成的详细信息，请参见第6.9节“AppArmor”[p.368]。非特权容器通过将容器中的根映射到一个非特权主机用户ID而更进一步。这将阻止访问代表主机资源的/proc和/sys文件，以及主机上root用户拥有的任何其他文件。

##### 6.16.1. 可利用的系统调用

容器与主机共享内核是一个核心容器特性。因此，如果内核包含任何可利用的系统调用，容器也可以利用这些调用。一旦容器控制了内核，它就可以完全控制主机已知的任何资源。

由于Ubuntu 12.10（Quantal），容器也可以受到seccomp过滤器的约束。Seccomp是一个新的内核特性，它过滤任务及其子任务可能使用的系统调用。虽然预计在不久的将来将改进和简化策略管理，但当前的策略包含一个简单的系统呼叫号码白名单。策略文件的第一行以版本号（必须为1）开头，第二行以策略类型（必须为“白名单”）开头。它后面是一个数字列表，每行一个。

通常，要运行完整的分发容器，需要大量的系统调用。但是，对于应用程序容器，可以将可用系统调用的数量减少到几个。即使对于运行完整分发的系统容器，也可能获得安全性收益，例如，通过删除64位容器中的32位兼容系统调用。有关如何配置容器以使用seccomp的详细信息，请参阅lxc.container.conf手册页面。默认情况下，不加载任何seccomp策略。

#### 6.17. 资源

•DeveloperWorks文章LXC:Linux容器工具[369]是容器使用的早期介绍。

•安全容器食谱[370]展示了使用安全模块使容器更加安全。

•上述手册页面可在以下网址找到：

能力[371]lxc.conf[372]

•上游LXC项目位于linuxcontainers.org[373]。

•LXC安全问题在LXC安全维基页面[374]中列出并讨论

•有关Linux中名称空间的更多信息，请参阅：S.Bhattiprolu、E.W.Biederman、S.E.Hallyn和D.Lezcano。主流Linux中的虚拟服务器和检查点/重启。SIGOPS操作系统评论，42（5），2008年。

# 第二十一章。群集

## 1.DRBD

分布式复制块设备（DRBD）在多个主机之间镜像块设备。复制对主机系统上的其他应用程序是透明的。任何块设备硬盘、分区、RAID设备、逻辑卷等都可以镜像。

要开始使用drbd，首先安装必要的软件包。从终端输入：**sudo apt安装drbd8 UTIL**

如果将虚拟内核用作虚拟机的一部分，则需要手动编译drbd模块。在虚拟机中安装linux服务器包可能更容易。

本节介绍如何设置一个drbd来复制一个单独的/srv分区，两台主机之间有一个ext3文件系统。分区大小不是特别相关，但两个分区的大小必须相同。

#### 1.1. 配置

本例中的两台主机分别称为drbd01和drbd02。他们需要通过DNS或/etc/hosts文件配置名称解析。详见第8章域名服务（DNS）[166页]。

•要配置drbd，请在第一台主机上编辑/etc/drbd.conf：

全局{使用计数编号；}公共{同步器{速率100M；}}资源r0{协议C；启动{

wfc超时15；degr wfc超时60；}net{

cram hmac alg sha1；drbd01上的共享机密“机密”}{

device/dev/drbd0；disk/dev/sdb1；地址192.168.0.1:7788；元磁盘内部；}位于drbd02上{

device/dev/drbd0；disk/dev/sdb1；地址192.168.0.2:7788；元磁盘内部；}

}

在/etc/drbd.conf中还有许多其他选项，但对于本例，它们的默认值很好。

•现在将/etc/drbd.conf复制到第二台主机：**scp/etc/drbd.conf drbd02：~**

•在drbd02上，将文件移动到/etc：**sudo mv drbd.conf/etc/**

•现在使用drbdadm实用程序初始化元数据存储。在每台服务器上执行：**sudo drbdadm创建md r0**

•接下来，在两台主机上启动drbd守护程序：**sudo systemctl启动drbd.service**

•在drbd01或您希望成为主要主机的任何主机上，输入以下内容：**sudo drbdadm--覆盖对等主all的数据**

•执行上述命令后，数据将开始与辅助主机同步。要查看进度，请在drbd02上输入以下内容：**手表-n1 cat/proc/drbd**

要停止观看输出，请按Ctrl+c。

•最后，将文件系统添加到/dev/drbd0并装载它：

**sudo mkfs.ext3/dev/drbd0 sudo mount/dev/drbd0/srv**

#### 1.2. 测试

要测试数据是否在主机之间实际同步，请将drbd01（主服务器）上的一些文件复制到/srv:Next，unmount/srv:**sudo cp-r/etc/default/srv sudo umount/srv**

*使降级*将主服务器添加到辅助角色：

**sudo drbdadm辅助r0**

现在在辅助服务器上，将其升级为主要角色：最后，装载分区：**sudo drbdadm主r0 sudo mount/dev/drbd0/srv**

使用ls，您应该可以看到从以前的主主机drbd01复制的/srv/default。

#### 1.3. 工具书类

•有关DRBD的更多信息，请参见DRBD网站[375]。

•drbd.conf手册页[376]包含本指南未涵盖的选项的详细信息。

•此外，请参见drbdadm手册页[377]。

•DRBD Ubuntu Wiki[378]页面也有更多信息。

# 第二十二章。虚拟专用网

OpenVPN是Ubuntu存储库中提供的虚拟专用网络（VPN）解决方案。它灵活、可靠、安全。它属于SSL/TLS VPN堆栈系列（不同于IPSec VPN）。本章将介绍如何安装和配置OpenVPN以创建VPN。

## 1.OpenVPN

如果您想要的不仅仅是预共享密钥，那么OpenVPN可以轻松地设置和使用公钥

使用SSL/TLS证书在VPN服务器和客户端之间进行身份验证和密钥交换的基础架构（PKI）。OpenVPN可以在路由或桥接VPN模式下使用，并且可以配置为使用UDP或TCP。端口号也可以配置，但端口1194是正式的。它只使用单一端口进行所有通信。VPN客户端实现几乎可用于任何东西，包括所有Linux发行版、OS X、Windows和基于OpenWRT的WLAN路由器。

#### 1.1. 服务器安装

要在终端中安装openvpn，请输入：**sudo apt安装openvpn easy rsa**

#### 1.2. 公钥基础设施设置

构建OpenVPN配置的第一步是建立PKI（公钥基础设施）。公钥基础设施包括：

•服务器和每个客户端的单独证书（也称为公钥）和私钥，以及

•主证书颁发机构（CA）证书和密钥，用于签署每个服务器和客户端证书。

OpenVPN支持基于证书的双向身份验证，这意味着在建立互信之前，客户端必须验证服务器证书，服务器必须验证客户端证书。

服务器和客户端都将通过首先验证所提供的证书是否由主证书颁发机构（CA）签名，然后测试现在已验证的证书头中的信息，例如证书公用名或证书类型（客户端或服务器），来验证另一方。

##### 1.2.1. 证书颁发机构设置

要设置您自己的证书颁发机构（CA）并为OpenVPN服务器和多个客户端生成证书和密钥，请首先将easy rsa目录复制到/etc/OpenVPN。这将确保在更新包时不会丢失对脚本的任何更改。从终端更改为用户根目录，并：

**mkdir/etc/openvpn/easy rsa/**

**cp-r/usr/share/easy rsa/\*/etc/openvpn/easy rsa/**

接下来，编辑/etc/openvpn/easy rsa/vars，根据您的环境调整以下内容：

export KEY\u COUNTRY=“US”export KEY\u PROVINCE=“NC”export KEY\u CITY=“Winston Salem”export KEY\u ORG=“示例公司”export KEY\u EMAIL=”steve@example.com“导出密钥\u CN=MyVPN导出密钥\u ALTNAMES=AltMyVPN导出密钥\u NAME=MyVPN导出密钥\u OU=MyVPN

输入以下内容以生成主证书颁发机构（CA）证书和密钥：

**cd/etc/openvpn/easy rsa/source vars./clean all**

**/建造ca**

##### 1.2.2. 服务器证书

接下来，我们将为服务器生成证书和私钥：

**./build key server myserver name**

与上一步一样，大多数参数都可以设置为默认值。另外两个查询需要肯定的响应，“签署证书？[y/n]”和“1/1证书请求已认证，提交？[y/n]”。

必须为OpenVPN服务器生成Diffie Hellman参数：

**/建造卫生署**

所有证书和密钥都已在子目录keys/中生成。通常的做法是将它们复制到/etc/openvpn/：

**cd键/**

**cp myservername.crt myservername.key ca.crt dh2048.pem/etc/openvpn/**

##### 1.2.3. 客户端证书

VPN客户端还需要一个证书来向服务器验证自身。通常，为每个客户端创建不同的证书。要创建证书，请在作为root用户时在终端中输入以下内容：

**cd/etc/openvpn/easy rsa/source vars./build key client1**

使用安全方法将以下文件复制到客户端：

•/etc/openvpn/ca.crt

•/etc/openvpn/easy rsa/keys/client1.crt

•/etc/openvpn/easy rsa/keys/client1.key

由于客户端证书和密钥仅在客户端计算机上是必需的，因此应将它们从服务器中删除。

#### 1.3. 简单服务器配置

在安装OpenVPN的同时，您还获得了以下示例配置文件（如果您进行检查，还可以获得更多）：

root@server：/#ls-l/usr/share/doc/openvpn/examples/sample config files/total 68-rw-r--r--1根根目录3427 2011-07-04 15:09 client.conf

-rw-r--r--1根根4141412011-07-04 15:09 server.conf.gz

首先将server.conf.gz复制并解包到/etc/openvpn/server.conf。

**sudo cp/usr/share/doc/openvpn/examples/sample config files/server.conf.gz/etc/openvpn/sudo gzip-d/etc/openvpn/server.conf.gz**

编辑/etc/openvpn/server.conf以确保以下行指向您在上一节中创建的证书和密钥。

ca ca.crt cert myserver name.crt key myserver name.key dh dh2048.pem

编辑/etc/sysctl.conf并取消注释以下行以启用IP转发。

#net.ipv4.ip\_forward=1，然后重新加载sysctl。**sudo sysctl-p/etc/sysctl.conf**

这是获得可工作的OpenVPN服务器所需的最低配置。您可以使用sample server.conf文件中的所有默认设置。现在启动服务器。您将在via日志中找到日志记录和错误消息。取决于你所寻找的：**sudo journalctl-xe**

如果您启动了模板化服务openvpn@server您可以使用以下选项筛选此特定消息源：

**sudo journalctl--标识符ovpn服务器**

请注意，“systemctl启动openvpn”并不是启动您刚才定义的openvpn。Openvpn使用模板化的systemd作业，openvpn@CONFIGFILENAME. 例如，如果您的配置文件是“server.conf”，则会调用您的服务openvpn@server. 您可以针对模板化服务运行所有类型的服务和systemctl命令，如start/stop/enable/disable/preset，如openvpn@server.

ubuntu@testopenvpn-服务器：~$sudo systemctl startopenvpn@server

ubuntu@testopenvpn-服务器：~$sudo systemctl状态openvpn@server . openvpn@server.service-已加载到服务器的OpenVPN连接：已加载（/lib/systemd/system/openvpn@.service；已启用；供应商预设：已启用）激活：自2016年4月12日星期二08:51:14 UTC起激活（运行）；1s前文档：man:openvpn（8）

https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage https://community.openvpn.net/openvpn/wiki/HOWTO 进程：1573 ExecStart=/usr/sbin/openvpn--daemon ovpn-%i--status/run/openvpn/%i.status 10--cd/etc/openvpn--script security 2--config/etc/openvpn/%i.conf--writep

主PID:1575（openvpn）

任务：1（限制：512）

CGroup:/system.slice/system-openvpn.slice/openvpn@server.service|-1575/usr/sbin/openvpn--daemon ovpn server--status/run/openvpn/server.status 10--cd/etc/openvpn--script security 2--config/etc/openvpn/server.conf-wr

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：/sbin/ip路由添加10.8.0.0/24 via

 10.8.0.2

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：UDPv4链路本地（绑定）：[undef]

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：UDPv4链接远程：[undef]

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：调用MULTI:MULTI\_init，r=256 v=256 Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：IFCONFIG POOL:base=10.8.0.4 size=62，ipv6=0 Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：IFCONFIG\_POOL\_read（），in=&apos;client1,10.8.0.4&apos;，TODO:ipv6 Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：成功->ifconfig\u pool\u set（）

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：IFCONFIG池列表

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：客户端1,10.8.0.4

Apr 12 08:51:14 testopenvpn服务器ovpn服务器[1575]：初始化序列已完成

您可以在一个系统上启用/禁用各种openvpn服务，但也可以让Ubuntu来完成繁重的工作。在/etc/default/openvpn中有AUTOSTART的配置。允许的值是“全部”、“无”或以空格分隔的VPN名称列表。如果为空，则假定为“全部”。VPN名称指的是VPN配置文件名。即“主页”如果您正在运行systemd，则将是/etc/openvpn/home.conf，更改此变量将需要运行“systemctl daemon reload”，然后在“systemctl daemon reload”之后重新启动openvpn服务（如果您删除了条目，则可能需要手动停止这些条目）“generic”调用daemon reload时，openvon将重新启动/lib/systemd/system generators/openvpn generator中的生成器为您的conf文件创建的所有依赖服务。

这是获得正常工作的OpenVPN服务器所需的最低配置。您可以使用sample server.conf文件中的所有默认设置。现在启动服务器。您将在日志中找到日志记录和错误消息。

现在检查OpenVPN是否创建了tun0接口：

root@server：/etc/openvpn#ifconfig tun0

tun0链路营地：UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 inet地址：10.8.0.1 P-t-P:10.8.0.2掩码：255.255.255运行NOARP多播MTU的上行点：1500公制：1

[...]

#### 1.4.简单的客户端配置

有各种不同的OpenVPN客户端实现，有GUI的也有GUI的。您可以在后面的章节中阅读有关客户端的更多信息。现在我们使用OpenVPN客户端For Ubuntu，它与服务器的可执行文件相同。因此，您必须在客户端计算机上再次安装OpenVPN包：**sudoapt安装openvpn**

这次将client.conf示例配置文件复制到/etc/openvpn/。**sudo cp/usr/share/doc/openvpn/examples/sample config files/client.conf/etc/openvpn/**

将您在上述部分中创建的CA的客户端密钥和证书复制到/etc/openvpn/并编辑/etc/openvpn/client.conf，以确保以下行指向这些文件。如果您在/etc/openvpn/中有这些文件，则可以省略路径。

ca ca.crt证书客户端1.crt密钥客户端1.密钥

您必须至少指定OpenVPN服务器名称或地址。确保配置中包含关键字client。这就是启用客户端模式的原因。

客户

远程vpnserver.example.com 1194

另外，请确保指定从服务器复制的密钥文件名

ca ca.crt证书客户端1.crt密钥客户端1.密钥

现在启动OpenVPN客户端：

ubuntu@testopenvpn-客户端：~$sudo systemctl startopenvpn@client ubuntu@testopenvpn-客户端：~$sudo systemctl状态openvpn@client . openvpn@client.service-与客户端的OpenVPN连接

已加载：已加载（/lib/systemd/system/openvpn@.service；已禁用；供应商预设：已启用）活动：自2016年4月12日星期二08:50:50 UTC起活动（运行）；3年前文档：man:openvpn（8）

https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage https://community.openvpn.net/openvpn/wiki/HOWTO 进程：1677 ExecStart=/usr/sbin/openvpn--daemon ovpn-%i--status/run/openvpn/%i.status 10--cd/etc/openvpn--script security 2--config/etc/openvpn/%i.conf--writep

主PID:1679（openvpn）

任务：1（限制：512）

CGroup:/system.slice/system-openvpn.slice/openvpn@client.service

|-1679/usr/sbin/openvpn--daemon ovpn client--status/run/openvpn/client.status

10--cd/etc/openvpn--scriptsecurity 2--config/etc/openvpn/client.conf--wr

Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：选项导入：--ifconfig/up选项已修改Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：选项导入：路由选项已修改

Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：路由\u网关

192.168.122.1/255.255.255.0 IFACE=eth0 HWADDR=52:54:00:89:ca:89

4月12日08:50:52 testopenvpn客户端ovpn客户端[1679]：TUN/TAP设备tun0已打开

Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：TUN/TAP TX队列长度设置为100 Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：do\_ifconfig，tt->ipv6=0，tt-

>\u ifconfig\u ipv6\u设置是否为0

4月12日08:50:52 testopenvpn客户端ovpn客户端[1679]：/sbin/ip链路设置dev tun0向上mtu 1500 4月12日08:50:52 testopenvpn客户端ovpn客户端[1679]：/sbin/ip地址添加dev tun0本地

10.8.0.6同行10.8.0.5

Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：/sbin/ip路由添加10.8.0.1/32 via

 10.8.0.5

Apr 12 08:50:52 testopenvpn客户端ovpn客户端[1679]：初始化序列已完成

检查是否创建了tun0接口：

root@client：/etc/openvpn#ifconfig tun0

tun0链接营地：UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 inet地址：10.8.0.6 P-t-P:10.8.0.5掩码：255.255.255上行点运行NOARP多播MTU:1500度量：1检查是否可以ping OpenVPN服务器：

root@client：/etc/openvpn#ping 10.8.0.1 ping 10.8.0.1（10.8.0.1）56（84）字节的数据。

10.8.0.1中的64字节：icmp\_req=1 ttl=64时间=0.920毫秒

OpenVPN服务器始终使用客户端网络中的第一个可用IP地址，并且只有该IP是可ping的。例如，如果您为客户端网络掩码配置了a/24，则将使用.1地址。您在上面的ifconfig输出中看到的Pt-P地址通常不响应ping请求。

查看您的路线：

root@client：/etc/openvpn#netstat-rn内核IP路由表

目标网关Genmask标志MSS窗口irtt Iface

10.8.0.5 0.0.0.0 255.255.255.255 UH 0 0 0 tun0

10.8.0.1 10.8.0.5 255.255.255.255 UGH 0 0 tun0

192.168.42.0 0.0.0.0 255.255.0 U 0 0 0 0 eth0 0.0.0 192.168.42.1 0.0.0.0.0 UG 0 0 0 eth0

#### 1.5.首次故障排除

如果上述操作不适用于您，请检查以下内容：

•检查日志，例如journalctl——标识符ovpn服务器（用于server.conf）

•检查您是否在client.conf和server.conf中正确指定了密钥文件名。

•客户端能否连接到服务器机器？可能防火墙正在阻止访问？检查服务器上的日志。

•客户端和服务器必须使用相同的协议和端口，例如UDP端口1194，请参阅端口和协议配置选项

•客户端和服务器必须使用相同的压缩配置，请参阅comp lzo config选项

•关于桥接与路由模式，客户端和服务器必须使用相同的配置，请参阅服务器与服务器桥接配置选项

#### 1.6.高级配置

##### 1.6.1.服务器上的高级路由VPN配置

以上是一个非常简单的工作VPN。客户端可以通过加密隧道访问VPN服务器机器上的服务。如果您想访问更多服务器或其他网络中的任何内容，请将一些路由推送到客户端。例如，如果您公司的网络可以汇总到网络192.168.0.0/16，则可以将此路由推送到客户端。但是您还必须更改返回路径的路由-您的服务器需要知道到VPN客户端网络的路由。

或者，您可以将默认网关推送到所有客户端，首先将其所有internet流量发送到VPN网关，然后通过公司防火墙从该网关发送到internet。本节介绍了一些可能的选项。

将路由推送到客户端，使其能够到达服务器后面的其他私有子网。请记住，这些私有子网还需要知道如何将OpenVPN客户端地址池（10.8.0.0/24）路由回OpenVPN服务器。推送“路由10.0.0.0 255.0.0.0”

如果启用，此指令将配置所有客户端通过VPN重定向其默认网络网关，导致所有IP流量（如web浏览和DNS查找）通过VPN（OpenVPN服务器计算机或您的中央防火墙可能需要NAT TUN/TAP接口到internet，以使其正常工作）。推送“重定向网关def1绕过dhcp”

配置服务器模式并为OpenVPN提供一个VPN子网，以便从中提取客户端地址。服务器本身将使用10.8.0.1，其余部分将提供给客户端。每个客户端将能够在

10.8.0.1.如果您正在进行以太网桥接，请将此行注释掉。

服务器10.8.0.0 255.255.255.0

在此文件中维护客户端到虚拟IP地址关联的记录。如果OpenVPN关闭或重新启动，则可以从先前分配的池中为重新连接的客户端分配相同的虚拟IP地址。ifconfig pool persist ipp.txt将DNS服务器推送到客户端。

推送“dhcp选项DNS 10.0.0.2”推送“dhcp选项DNS 10.1.0.2”允许客户端到客户端通信。客户对客户

在VPN链路上启用压缩。复合lzo

keepalive指令使类似ping的消息在链路上来回发送，以便每一方都知道另一方何时宕机。每1秒Ping一次，如果在3秒的时间段内没有收到Ping，则假定远程对等机已关闭。保持1 3

在初始化之后减少OpenVPN守护进程的权限是一个好主意。

用户nobody组nogroup

OpenVPN 2.0包含一项功能，允许OpenVPN服务器从连接的客户端安全地获取用户名和密码，并将该信息用作验证客户端的基础。要使用此身份验证方法，首先将auth user pass指令添加到客户端配置中。它将指示OpenVPN客户端向用户查询用户名/密码，并通过安全TLS通道将其传递给服务器。

#客户端配置！验证用户通行证

这将告诉OpenVPN服务器验证客户端使用登录PAM模块输入的用户名/密码。如果使用Kerberos等集中式身份验证，则此功能非常有用。

plugin/usr/lib/openvpn/openvpn-plugin-auth-pam.so登录

请阅读OpenVPN强化安全指南[379]以获取进一步的安全建议。

##### 1.6.2. 服务器上的高级桥接VPN配置

可以为路由或桥接VPN模式设置OpenVPN。有时这也被称为OSI第二层与第三层VPN。在桥接VPN中，所有第2层帧（例如所有以太网帧）都发送到VPN合作伙伴，而在路由VPN中，只有第3层数据包发送到VPN合作伙伴。在桥接模式下，所有通信量（包括传统的局域网本地通信量，如本地网络广播、DHCP请求、ARP请求等）都被发送到VPN合作伙伴，而在路由模式下，这将被过滤。

*1.6.2.1. 为服务器上的桥接准备接口配置*

首先，使用netplan使用所需的以太网设备配置网桥设备。

$cat/etc/netplan/01-netcfg.yaml#此文件描述了系统上可用的网络接口#有关更多信息，请参阅netplan（5）。

网络：

版本：2渲染器：networkd以太网：enp0s31f6:dhcp4:无网桥：br0:

接口：[enp0s31f6]dhcp4:否

地址：[10.0.1.100/24]网关4:10.0.1.1名称服务器：地址：[10.0.1.1]

强烈建议使用静态IP地址。DHCP寻址也可以工作，但是您仍然需要在OpenVPN配置文件中对静态地址进行编码。

服务器上的下一步是在引导时将以太网设备配置为混杂模式。为此，请确保已安装networkd dispatcher包，并创建以下配置脚本。

**sudoapt更新**

**sudo apt安装网络调度器**

**sudo touch/usr/lib/networkd dispatcher/dorment.d/promisc\_桥sudo chmod+x/usr/lib/networkd dispatcher/dorment.d/promisc\_桥**

然后添加以下内容。

#!/垃圾箱/垃圾箱集-e

如果[“$IFACE”=br0]；然后#物理接口ip链路上的“carrier”没有网络调度程序事件在fi上设置eth0 up promisc

*1.6.2.2. 准备用于桥接的服务器配置*

编辑/etc/openvpn/server.conf以使用tap而不是tun，并将服务器设置为使用服务器网桥指令：

;德夫屯德夫塔普；服务器10.8.0.0 255.255.255.0

服务器网桥10.0.0.4 255.255.255.0 10.0.0.128 10.0.0.254配置服务器后，通过输入以下命令重新启动openvpn：**sudo systemctl重启openvpn@server**

*1.6.2.3. 客户端配置*

首先，在客户端上安装openvpn：

**sudoapt安装openvpn**

然后配置服务器并将客户端证书复制到/etc/openvpn/目录，通过复制示例创建客户端配置文件。在客户端计算机上的终端中，输入：Now edit/etc/openvpn/client.conf更改以下选项：**sudo cp/usr/share/doc/openvpn/examples/sample config files/client.conf/etc/openvpn**

开发tap；dev tun ca.crt证书客户端1.crt密钥客户端1.key

最后，重新启动openvpn：**sudo systemctl重启openvpn@client**

您现在应该能够通过VPN连接到远程LAN。

#### 1.7. 客户端软件实现

##### 1.7.1. 用于OpenVPN的Linux网络管理器GUI

许多Linux发行版，包括Ubuntu桌面版本，都附带了网络管理器，这是一个很好的配置网络设置的GUI。它还可以管理您的VPN连接。确保已安装package network manager openvpn。在这里，您可以看到安装还安装了所有其他必需的软件包：

root@client：~#apt安装网络管理器openvpn读取软件包列表。。。多恩

构建依赖树

正在读取状态信息。。。完成后，将安装以下额外软件包：liblzo2-2 libpkcs11-helper1网络管理器openvpn gnome openvpn建议软件包：

resolvconf将安装以下新软件包：

liblzo2-2 libpkcs11-helper1网络管理器openvpn网络管理器openvpn gnome openvpn 0已升级，5已新安装，0已删除，631未升级。

需要获得700 kB的档案。

执行此操作后，将使用3031 kB的额外磁盘空间。

是否要继续[Y/n]？

要向network manager通知新安装的软件包，您必须重新启动它：

root@client：~#重新启动网络管理器网络管理器启动/运行，进程3078

打开Network Manager GUI，选择VPN选项卡，然后选择“添加”按钮。在打开请求程序中选择OpenVPN作为VPN类型，然后按“创建”。在下一个窗口中，将OpenVPN的服务器名称添加为“网关”，将“类型”设置为“证书（TLS）”，将“用户证书”指向用户证书，“CA证书”指向CA证书，将“私钥”指向私钥文件。使用高级按钮启用压缩（例如comp lzo）、dev tap或您在服务器上设置的其他特殊设置。现在尝试建立您的VPN。

##### 1.7.2. 用于Mac OS X的带GUI的OpenVPN:Tunnelblick

Tunnelblick是OpenVPN for OS X GUI的一个优秀的免费开源实现http://code.google.com/p/tunnelblick/. 从那里下载最新的OSX安装程序并安装。然后将client.ovpn配置文件与应用程序文件夹中的/Users/username/Library/Application Support/Tunnelblick/Configurations/和lauch Tunnelblick中的证书和密钥放在一起。

#Tunnelblick客户端的示例client.ovpn

远程blue.example.com端口1194协议udp开发tun开发类型tun ns证书类型服务器reneg sec 86400身份验证用户通过身份验证nocache身份验证重试交互组件lzo是动词3 ca ca.crt证书客户端.crt密钥客户端.key

##### 1.7.3. 用于Win 7的带GUI的OpenVPN

首先下载并安装最新的OpenVPN Windows安装程序[380]。OpenVPN 2.3.2是写这篇文章时的最新版本。在撰写本文时，Windows二进制安装程序附带了管理GUI。

您需要启动OpenVPN服务。转到开始>计算机>管理>服务和应用程序

>服务。找到OpenVPN服务并启动它。将其启动类型设置为自动。当您第一次启动OpenVPN MI GUI时，您需要以管理员身份运行它。您必须右键单击它，您将看到该选项。

您必须将OpenVPN配置写入文本文件，并将其与CA证书一起放入C:\Program Files\OpenVPN\config\client.ovpn中。您可以将用户证书放在用户的主目录中，如下面的示例所示。

#C:\ProgramFiles\OpenVPN\config\client.ovpn client

远程服务器.example.com端口1194协议udp开发tun开发类型tun ns证书类型服务器reneg sec 86400身份验证用户通过身份验证重试交互组件lzo是动词3 ca ca ca.crt

证书“C:\\Users\\username\\My Documents\\openvpn\\client.crt”key“C:\\Users\\username\\My Documents\\openvpn\\client.key”管理127.0.0.1 1194管理挂起

管理查询密码验证重试交互；在此处设置Windows TAP网络接口设备的名称dev node MyTAP

注意：如果您不使用用户身份验证和/或希望在没有用户交互的情况下运行服务，请注释掉以下选项：

验证用户通过验证重试交互管理127.0.0.1 1194管理保留管理查询密码

您可能需要将Windows服务设置为“自动”。

##### 1.7.4. 用于OpenWRT的OpenVPN

OpenWRT被描述为嵌入式设备（如WLAN路由器）的Linux发行版。有某些类型的WLAN路由器可以通过闪存来运行OpenWRT。根据OpenWRT路由器上的可用内存，您可以运行类似OpenVPN的软件，例如，您可以构建一个小型廉价的分支办公室路由器，并将VPN连接到中心办公室。有关OpenWRT上OpenVPN的更多信息，请参见[381]。这是OpenWRT项目的主页：http://openwrt.org 登录您的OpenWRT路由器并安装OpenVPN：

**opkg更新opkg安装openvpn**

签出/etc/config/openvpn并将您的客户端配置放在那里。将证书和密钥复制到/etc/openvpn/

配置openvpn客户端1选项启用1选项客户端1#选项开发点击选项开发tun选项协议udp选项ca/etc/openvpn/ca.crt选项证书/etc/openvpn/client.crt选项密钥/etc/openvpn/client.key选项组件1

在OpenWRT路由器上重新启动OpenVPN以获取配置

您必须查看是否需要调整路由器的路由和防火墙规则。

#### 1.8. 工具书类

•有关更多信息，请参阅OpenVPN[382]网站。

•OpenVPN强化安全指南[383]

•此外，Pakt的OpenVPN：构建和集成虚拟专用网络[384]是一个很好的资源。

# 第二十三章。其他有用的应用

Ubuntu服务器团队开发了许多非常有用的应用程序，还有一些与Ubuntu Server Edition集成良好的应用程序，这些应用程序可能并不广为人知。本章将展示一些有用的应用程序，它们可以使管理Ubuntu服务器或许多Ubuntu服务器变得更加容易。

## 1.帕姆·莫特

当登录Ubuntu服务器时，你可能已经注意到当天的信息（MOTD）。

使用两个软件包获取并显示此信息：

•提供横向客户机的核心库，该库是使用横向[385]（专有）管理系统所需的。然而，该软件包还包括横向系统信息实用程序，该实用程序负责显示涉及cpu、内存、磁盘空间等的核心系统数据。例如：*常见景观：*

系统负载：0.0进程：76

/：30.2%已登录的3.11GB用户的使用率：1内存使用率：20%eth0的IP地址：10.153.107.115

交换使用率：0%绘制此数据并在https://landscape.canonical.com/

您可以随时手动运行横向系统信息。

•提供有关可用包更新、即将进行的文件系统检查（fsck）和所需重新启动（例如：内核升级后）的信息。*更新通知程序公用程序：*

pam\_motd根据脚本前面的数字按顺序执行/etc/update motd.d中的脚本。脚本的输出被写入/var/run/motd，保持数字顺序，然后与/etc/motd.tail连接。

您可以将自己的动态信息添加到MOTD中。例如，要添加本地天气信息，请执行以下操作：

•首先，安装weather util软件包：**sudo-apt安装weather-util**

•气象实用程序使用国家海洋和大气管理局的METAR数据以及国家气象局的预测。为了查找本地信息，您需要4字符ICAO位置指示器。这可以通过浏览国家气象局[386]网站来确定。

虽然国家气象局是美国政府的一个机构，但世界各地都有气象站。但是，可能无法获得美国以外所有地点的当地天气信息。

•创建/usr/local/bin/local weather，这是一个简单的shell脚本，用于将天气与本地ICAO指示器一起使用：

#!/垃圾箱/垃圾箱

#

##为MOTD打印本地天气信息。

#

#

#用当地气象站代替KINT可在此处找到本地电台：http://www.weather.gov/tg/siteloc.shtml

回声天气-我喜欢回声

•使脚本可执行：**sudo chmod 755/usr/local/bin/local weather**

•接下来，创建指向/etc/update-motd.d/98-local-weather的符号链接：**sudo ln-s/usr/local/bin/local weather/etc/update-motd.d/98-local-weather**

•最后，退出服务器并重新登录以查看新MOTD。

你现在应该得到一些有用的信息，以及一些关于当地天气的信息，这些信息可能不是很有用。希望本地天气的例子能够证明pam\_motd的灵活性。

#### 1.1. 资源

•有关更新motd的更多选项，请参见更新motd手册页[387]。

•Debian每日天气软件包[388]文章提供了有关使用weatherutility的更多详细信息。

## 2.埃克佩尔

etckeeper允许将/etc的内容存储在版本控制系统（VCS）存储库中。它与APT集成，并在安装或升级包时自动提交对/etc的更改。将/etc置于版本控制之下被认为是行业最佳实践，etckeeper的目标是使此过程尽可能轻松。

通过在终端中输入以下内容来安装etckeeper：**sudo-apt-install-etckeeper**

主配置文件/etc/etckeeper/etckeeper.conf相当简单。主要的选择是

要使用的VCS，默认情况下，etckeeper配置为使用Bazaar。存储库在包安装期间自动初始化（并首次提交）。可以通过输入以下命令撤消此操作：**sudo etckeeper uninit**

默认情况下，etckeeper将提交每天对/etc所做的未提交更改。可以使用“避免每日自动提交”配置选项禁用此功能。它还将在包安装前后自动提交更改。为了更精确地跟踪更改，建议手动提交更改，并使用提交消息：使用bzr的VCS命令，您可以查看日志信息：**sudo etckeeper提交“.配置更改的原因…”sudo bzr log/etc/passwd**

要演示与软件包管理系统（APT）的集成，请安装postfix：**sudoapt安装后缀**

安装完成后，应将所有postfix配置文件提交到存储库：

提交到：/etc/added aliases.db modified group modified groupmodified gshadow modified gshadowmodified passwd added postfix added resolvconf added rsyslog.d modified shadow modified shadow added init.d/postfix added network/if-down.d/postfix added postfix added postfix/dynamicmaps.cf added postfix/main.cf addedpostfix/master.cf添加了后缀/post-install添加了后缀/postfix文件添加了后缀/postfix脚本添加了后缀/sasl添加了ppp/ip-down.d添加了ppp/ip-down.d/postfix添加了ppp/ip-up.d/postfix添加了rc0.d/K20postfix添加了rc1.d/K20postfix添加了rc2.d/S20postfix添加了rc3.d/S20postfix添加了rc4.d/S20postfix添加了rc5.d/S20postfix添加了rc6.d/K20postfix添加了resolvconf/update libc.d添加了resolvconf/update-libc.d/postfix添加了rsyslog.d/postfix.conf添加了ufw/applications.d/postfix提交的修订版2。

有关etckeeper如何跟踪手动更改的示例，请将新主机添加到/etc/hosts。使用bzr可以查看哪些文件已被修改：

**sudo bzr状态/etc/**修改：主机

现在提交更改：**sudo etckeeper提交“添加了新主机”**

有关bzr的更多信息，请参见第1节“集市”[p.295]。

#### 2.1. 资源

•有关使用etckeeper的更多详细信息，请参阅etckeeper[389]网站。

•有关bzr的最新新闻和信息，请访问bzr[390]网站。

## 3.比奥布

对于任何系统管理员来说，最有用的应用程序之一是xterm多路复用器，如screen或tmux。它允许在一个终端中执行多个外壳。为了使一些高级多路复用器功能更加用户友好，并提供有关系统的一些有用信息，创建了byobu软件包。它充当这些程序的包装器。默认情况下，Byobu使用tmux（如果已安装），但这可以由用户更改。

只需使用以下命令调用它：**比奥布**

现在打开配置菜单。默认情况下，按F9键即可完成此操作。这将允许您：

•查看帮助菜单

•更改Byobu的背景色

•改变Byobu的前景色

•切换状态通知

•更改密钥绑定集

•改变逃生顺序

•创建新窗口

•管理默认窗口

•Byobu当前不会在登录时启动（切换开启）

键绑定决定转义序列、新窗口、更改窗口等。有两个键绑定集可从f键和屏幕转义键中选择。如果希望使用原始密钥绑定，请选择“无”集。

byobu提供了一个菜单，显示Ubuntu版本、处理器信息、内存信息以及时间和日期。其效果类似于桌面菜单。

使用“Byobu当前不在登录时启动（切换打开）”选项将导致在打开终端时执行Byobu。对byobu所做的更改基于每个用户，不会影响系统上的其他用户。

使用byobu时的一个区别是回滚模式。按F7键进入回滚模式。

回滚模式允许您使用类似vi的命令浏览过去的输出。以下是移动命令的快速列表：

•-将光标向左移动一个字符*H*

•-将光标向下移动一行*J*

•-将光标向上移动一行*K*

•-将光标向右移动一个字符*L*

•-移动到当前行的开头*0*

•-移动到当前行的末尾*$*

•-移动到指定行（默认为缓冲区的末尾）*G*

•-向前搜索*/*

•-向后搜索*?*

•-向前或向后移动到下一场比赛*N*

#### 3.1. 资源

•有关屏幕的更多信息，请参见屏幕网站[391]。

•以及Ubuntu Wiki屏幕[392]页面。

•更多信息，请参见byobu项目页面[393]。

# 附录A.附录

## 1.报告Ubuntu服务器版中的错误

Ubuntu项目，也就是Ubuntu服务器，使用Launchpad[394]作为错误跟踪器。为了归档bug，您需要一个Launchpad帐户。如有必要，在此处创建一个[395]。

#### 1.1. 使用apport cli报告错误

报告错误的首选方法是使用apport cli命令。它必须在受bug影响的机器上调用，因为它从运行它的系统收集信息，并将其发布到Launchpad上的bug报告中。因此，如果系统没有运行桌面环境以使用浏览器（与服务器共用）或没有Internet访问权限，则将该信息发送到Launchpad可能是一项挑战。在这些情况下采取的步骤如下所述。

命令apport cli和ubuntu bug应该在cli服务器上给出相同的结果。后者实际上是apport bug的一个符号链接，它足够智能，可以知道桌面环境是否正在使用，如果没有，将选择apport cli。由于服务器系统往往是CLI，因此本指南从一开始就选择了apport CLI。

Ubuntu中的错误报告需要针对特定软件包进行归档，因此受错误影响的软件包名称（源软件包或程序名/路径）需要提供给apport cli：**apport cli PACKAGENAME**

有关Ubuntu软件包的更多信息，请参见第3章，软件包管理[p.27]。

apport cli完成信息收集后，系统将询问您如何处理信息。例如，要报告vim中的错误：

**apport cli vim**\*\*\*收集问题信息

收集的信息可以发送给开发人员以改进应用程序。这可能需要几分钟。。。

\*\*\*向开发者发送问题报告？

发送问题报告后，请在自动打开的web浏览器中填写表格。

你想做什么？您的选项有：S:sendreport（2.8KB）

V:查看报告

K：保留报告文件以便以后发送或复制到其他地方I：取消并忽略此程序版本将来的崩溃

C:取消请选择（S/V/K/I/C）：

前三个选项描述如下：

•发送：将收集的信息提交到Launchpad，作为提交新错误报告过程的一部分。您将有机会用自己的话描述这个bug。

\*\*\*上载问题信息

收集的信息将被发送到bug跟踪系统。

这可能需要几分钟。

94%\*\*\*要继续，您必须访问以下URL：

https://bugs.launchpad.net/ubuntu/+source/vim/+filebug/09b2495ae2ab-11e3-879b-68B5996C8？您可以立即启动浏览器，或将此URL复制到另一台计算机上的浏览器中。

选项：1：立即启动浏览器

C:取消

请选择（1/C）：1

选择“1”时使用的浏览器将是通过Debian Alternations系统在系统上称为www浏览器的浏览器[396]。要安装的基于文本的浏览器示例包括links、elinks、lynx和w3m。您还可以手动将现有浏览器指向给定的URL。

•在屏幕上显示收集的信息以供查看。这可能是很多信息。按“回车”按屏幕滚动。按“q”退出并返回选择菜单。**视图：**

•将收集的信息写入磁盘。生成的文件可以稍后用于归档bug报告，通常是在将其传输到另一个Ubuntu系统之后。**保持：**

你想做什么？你的选择是：

S:发送报告（2.8KB）

V:查看报告

K：保留报告文件以便以后发送或复制到其他地方I：取消并忽略此程序版本将来的崩溃

C:取消

请选择（S/V/K/I/C）：K

问题报告文件：/tmp/apport.vim.1pg92p02.apport

要报告错误，请将该文件放到支持internet的Ubuntu系统上，并对其应用apport cli。这将导致菜单立即出现（信息已收集）。然后应按“s”发送：**apport cli apport.vim.1pg92p02.apport**

要直接将报表保存到磁盘（不带菜单），可以执行以下操作：报表名称应以.apport结尾。**apport cli vim—保存apport.vim.test.apport**

如果此启用internet的系统不是Ubuntu/Debian，则apport cli不可用，因此需要手动创建错误。apport报告也不能作为bug的附件包含，因此在这种情况下它是完全无用的。

#### 1.2. 报告应用程序崩溃

提供apport cli实用程序apport的软件包可以配置为自动捕获崩溃应用程序的状态。这是默认启用的（在/etc/default/apport中）。

应用程序崩溃后，如果启用，apport将在/var/crash下存储崩溃报告：

-rw-r-----1 peter whoopsie 150K Jul 24 16:17\_usr\_lib\_x86\_64-linux-gnu\_libmenucache2\_libexec\_menu-cached.1000.crash

使用不带参数的apport cli命令来处理任何挂起的崩溃报告。它将提供一个接一个的报告。

**阿波特cli**\*\*\*向开发者发送问题报告？

发送问题报告后，请在自动打开的web浏览器中填写表格。

你想做什么？你的选择是：

S:发送报告（153.0 KB）

V:查看报告

K：保留报告文件以便以后发送或复制到其他地方I：取消并忽略此程序版本将来的崩溃

C:取消

请选择（S/V/K/I/C）：S

如果发送报告（如上所述），将立即返回提示，/var/crash目录将包含2个额外文件：

-rw-r---1 peter whoopsie 150K Jul 24 16:17\u usr\u lib\u x86\u 64-linux-gnu libmenucache2\u libexec\u menu-cached.1000.crash-rw-rw-r---1 peter whoopsie 0 Jul 24 16:37\u usr\u lib\u x86\u 64-linux-gnu libmenucache2\u libexec\u menu-cached.1000.upload-rw------------1 whoopsie whoopsie 7月24日16:37\_usr\_lib\_x86\_64-linux-gnu libmenucache2\_libexec\_menu-cached.1000.upload

发送这样的崩溃报告不会立即导致创建新的公共bug。该报告将在Launchpad上保密，这意味着它将只对有限的bug分类者可见。然后，这些筛选者将在创建公共bug之前扫描报告以查找可能的私有数据。

#### 1.3. 资源

•参见报告bug[397]Ubuntu wiki页面。

•此外，Apport[398]页面还有一些有用的信息。尽管其中一些与使用GUI有关。

[[1]](" \l "_ftnref1" \o ")https://creativecommons.org/licenses/by-sa/3.0/

[[2]](" \l "_ftnref2" \o ")https://launchpad.net/~ubuntu核心文档

[[3]](" \l "_ftnref3" \o ")https://launchpad.net/~ubuntu服务器

[[4]](" \l "_ftnref4" \o ")https://help.ubuntu.com/community/

[[5]](" \l "_ftnref5" \o ")https://bazaar.launchpad.net/~ubuntu核心文档/serverguide/trunk/changes

[[6]](" \l "_ftnref6" \o ")https://bazaar.launchpad.net/~ubuntu核心文档/ubuntu文档/trunk/changes

[[7]](" \l "_ftnref7" \o ")https://help.ubuntu.com/18.04/installation-guide/

[[8]](" \l "_ftnref8" \o ")https://help.ubuntu.com

[[9]](" \l "_ftnref9" \o ")http://www.ubuntu.com/management

[[10]](" \l "_ftnref10" \o ")http://www.ubuntu.com/support

[[11]](" \l "_ftnref11" \o ")https://help.ubuntu.com/18.04/installation-guide/

[[12]](" \l "_ftnref12" \o ")https://wiki.ubuntu.com/S390X/InstallationGuide

[[13]](" \l "_ftnref13" \o ")http://www.kroah.com/lkn/

[[14]](" \l "_ftnref14" \o ")http://www.ubuntu.com/download/server/download

[[15]](" \l "_ftnref15" \o ")https://maas.io

[[16]](" \l "_ftnref16" \o ")https://maas.io

[[17]](" \l "_ftnref17" \o ")http://www.ubuntu.com/download/server/download

[[18]](" \l "_ftnref18" \o ")http://landscape.canonical.com/

[[19]](" \l "_ftnref19" \o ")https://help.ubuntu.com/18.04/installation-guide/

[[20]](" \l "_ftnref20" \o ")https://help.ubuntu.com/community/Installation#raid

[[21]](" \l "_ftnref21" \o ")http://www.faqs.org/docs/Linux-HOWTO/Software-RAID-HOWTO.html

[[22]](" \l "_ftnref22" \o ")http://oreilly.com/catalog/9781565927308/

[[23]](" \l "_ftnref23" \o ")https://help.ubuntu.com/community/Installation#lvm

[[24]](" \l "_ftnref24" \o ")http://tldp.org/HOWTO/LVM-HOWTO/index.html

[[25]](" \l "_ftnref25" \o ")http://www.linuxdevcenter.com/pub/a/linux/2006/04/27/managing-disk-space-with-lvm.html

[[26]](" \l "_ftnref26" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man8/fdisk.8.html

[[27]](" \l "_ftnref27" \o ")http://www.kernel.org/doc/Documentation/kdump/kdump.txt

[[28]](" \l "_ftnref28" \o ")http://people.redhat.com/~z~安德森/

[[29]](" \l "_ftnref29" \o ")http://www.dedoimedo.com/computers/crash-analyze.html

[[30]](" \l "_ftnref30" \o ")http://www.debian.org/doc/user-manuals#apt-如何

[[31]](" \l "_ftnref31" \o ")https://help.ubuntu.com/community/InstallingSoftware

[[32]](" \l "_ftnref32" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man1/dpkg.1.html

[[33]](" \l "_ftnref33" \o ")http://www.debian.org/doc/manuals/apt-howto/

[[34]](" \l "_ftnref34" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man8/apt.8.html

[[35]](" \l "_ftnref35" \o ")http://manpages.ubuntu.com/manpages/bionic/man8/aptitude.8.html

[[36]](" \l "_ftnref36" \o ")https://help.ubuntu.com/community/Repositories/Ubuntu

[[37]](" \l "_ftnref37" \o ")https://help.ubuntu.com/community/Network

[[38]](" \l "_ftnref38" \o ")https://netplan.io

[[39]](" \l "_ftnref39" \o ")http://manpages.ubuntu.com/manpages/man5/netplan.5.html

[[40]](" \l "_ftnref40" \o ")http://manpages.ubuntu.com/manpages/man1/systemd-resolve.1.html

[[41]](" \l "_ftnref41" \o ")http://manpages.ubuntu.com/manpages/man8/systemd-resolved.8.html

[[42]](" \l "_ftnref42" \o ")https://netplan.io/examples

[[43]](" \l "_ftnref43" \o ")http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge

[[44]](" \l "_ftnref44" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man7/tcp.7.html

[[45]](" \l "_ftnref45" \o ")http://manpages.ubuntu.com/manpages/bionic/man7/ip.7.html

[[46]](" \l "_ftnref46" \o ")http://www.redbooks.ibm.com/abstracts/gg243376.html

[[47]](" \l "_ftnref47" \o ")http://oreilly.com/catalog/9780596002978/

[[48]](" \l "_ftnref48" \o ")https://help.ubuntu.com/community/dhcp3-server

[[49]](" \l "_ftnref49" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man5/dhcpd.conf.5.html

[[50]](" \l "_ftnref50" \o ")http://www.isc.org/software/dhcp

[[51]](" \l "_ftnref51" \o ")https://chrony.tuxfamily.org/faq.html

[[52]](" \l "_ftnref52" \o ")http://www.pool.ntp.org/

[[53]](" \l "_ftnref53" \o ")https://www.freedesktop.org/software/systemd/man/timedatectl.html

[[54]](" \l "_ftnref54" \o ")https://www.freedesktop.org/software/systemd/man/systemd-timesyncd.service.html#

[[55]](" \l "_ftnref55" \o ")http://www.catb.org/gpsd/gpsd-time-service-howto.html#\_feeding\_chrony\_from\_gpsd

[[56]](" \l "_ftnref56" \o ")https://help.ubuntu.com/community/UbuntuTime

[[57]](" \l "_ftnref57" \o ")http://dpdk.org/doc/nics

[[58]](" \l "_ftnref58" \o ")http://dpdk.org/doc/guides/nics/e1000em.html

[[59]](" \l "_ftnref59" \o ")http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/

[[60]](" \l "_ftnref60" \o ")http://dpdk.org/browse/dpdk/tree/drivers/net/e1000/

[[61]](" \l "_ftnref61" \o ")http://dpdk.org/doc/guides/nics/ixgbe.html

[[62]](" \l "_ftnref62" \o ")http://dpdk.org/browse/dpdk/tree/drivers/net/i40e/

[[63]](" \l "_ftnref63" \o ")http://dpdk.org/doc/guides/nics/fm10k.html

[[64]](" \l "_ftnref64" \o ")http://dpdk.org/doc/guides/nics/cxgbe.html

[[65]](" \l "_ftnref65" \o ")http://dpdk.org/browse/dpdk/tree/drivers/net/enic

[[66]](" \l "_ftnref66" \o ")http://dpdk.org/doc/guides/nics/virtio.html

[[67]](" \l "_ftnref67" \o ")http://dpdk.org/doc/guides/nics/vmxnet3.html

[[68]](" \l "_ftnref68" \o ")http://dpdk.org/browse/dpdk/tree/drivers/net/af\_packet

[[69]](" \l "_ftnref69" \o ")http://dpdk.org/doc/guides/nics/pcap\_ring.html#rings-基于偏振模色散

[[70]](" \l "_ftnref70" \o ")http://dpdk.org/doc/guides/xen/pkt\_switch.html#xen-pmd前端先决条件

[[71]](" \l "_ftnref71" \o ")http://dpdk.org/doc/guides/nics/pcap\_ring.html#libpcap-基于偏振模色散

[[72]](" \l "_ftnref72" \o ")https://wiki.ubuntu.com/OpenStack/CloudArchive

[[73]](" \l "_ftnref73" \o ")http://dpdk.org/ml

[[74]](" \l "_ftnref74" \o ")http://openvswitch.org/mlists

[[75]](" \l "_ftnref75" \o ")https://bugs.launchpad.net/ubuntu/+来源/dpdk

[[76]](" \l "_ftnref76" \o ")http://dpdk.org/doc

[[77]](" \l "_ftnref77" \o ")http://dpdk.org/doc/guides/rel\_notes/release\_2\_2.html

[[78]](" \l "_ftnref78" \o ")http://dpdk.org/doc/guides/linux\_gsg/index.html

[[79]](" \l "_ftnref79" \o ")http://dpdk.org/doc/guides/testpmd\_app\_ug/run\_app.html

[[80]](" \l "_ftnref80" \o ")http://dpdk.org/doc/api/

[[81]](" \l "_ftnref81" \o ")https://github.com/openvswitch/ovs/blob/branch-2.5/INSTALL.DPDK.md

[[82]](" \l "_ftnref82" \o ")https://en.wikipedia.org/wiki/Data\_Plane\_Development\_Kit

[[83]](" \l "_ftnref83" \o ")http://wiki.debian.org/DebianInstaller/MultipathSupport

[[84]](" \l "_ftnref84" \o ")http://en.wikipedia.org/wiki/SCSI\_Inquiry\_Command

[[85]](" \l "_ftnref85" \o ")http://www-01.ibm.com/support/docview.wss?uid=isg3T1011985

[[86]](" \l "_ftnref86" \o ")https://help.ubuntu.com/community/SSH

[[87]](" \l "_ftnref87" \o ")http://www.openssh.org/

[[88]](" \l "_ftnref88" \o ")https://wiki.ubuntu.com/AdvancedOpenSSH

[[89]](" \l "_ftnref89" \o ")http://docs.puppetlabs.com/

[[90]](" \l "_ftnref90" \o ")http://forge.puppetlabs.com/

[[91]](" \l "_ftnref91" \o ")http://www.apress.com/9781430230571

[[92]](" \l "_ftnref92" \o ")https://wiki.zentyal.org/wiki/En/4.0/Appendix\_B:\_Development\_and\_advanced\_configuration#Advanced\_Service\_Customization

[[93]](" \l "_ftnref93" \o ")https://launchpad.net/~zentyal/

[[94]](" \l "_ftnref94" \o ")http://doc.zentyal.org/

[[95]](" \l "_ftnref95" \o ")http://trac.zentyal.org/wiki/Documentation

[[96]](" \l "_ftnref96" \o ")http://forum.zentyal.org/

[[97]](" \l "_ftnref97" \o ")http://tools.ietf.org/html/rfc4510

[[98]](" \l "_ftnref98" \o ")http://tools.ietf.org/html/rfc2849

[[99]](" \l "_ftnref99" \o ")http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html

[[100]](" \l "_ftnref100" \o ")http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html

[[101]](" \l "_ftnref101" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldaprenamemachine.1.html

[[102]](" \l "_ftnref102" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapadduser.1.html

[[103]](" \l "_ftnref103" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuserfromgroup.1.html

[[104]](" \l "_ftnref104" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapfinger.1.html

[[105]](" \l "_ftnref105" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapid.1.html

[[106]](" \l "_ftnref106" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapgid.1.html

[[107]](" \l "_ftnref107" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapmodifyuser.1.html

[[108]](" \l "_ftnref108" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldaprenameuser.1.html

[[109]](" \l "_ftnref109" \o ")http://manpages.ubuntu.com/manpages/en/man1/lsldap.1.html

[[110]](" \l "_ftnref110" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapaddusertogroup.1.html

[[111]](" \l "_ftnref111" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapsetpasswd.1.html

[[112]](" \l "_ftnref112" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapinit.1.html

[[113]](" \l "_ftnref113" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapaddgroup.1.html

[[114]](" \l "_ftnref114" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapdeletegroup.1.html

[[115]](" \l "_ftnref115" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapmodifygroup.1.html

[[116]](" \l "_ftnref116" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapdeletemachine.1.html

[[117]](" \l "_ftnref117" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldaprenamegroup.1.html

[[118]](" \l "_ftnref118" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapaddmachine.1.html

[[119]](" \l "_ftnref119" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapmodifymachine.1.html

[[120]](" \l "_ftnref120" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapsetprimarygroup.1.html

[[121]](" \l "_ftnref121" \o ")http://manpages.ubuntu.com/manpages/en/man1/ldapdeleteuser.1.html

[[122]](" \l "_ftnref122" \o ")http://www.openldap.org/

[[123]](" \l "_ftnref123" \o ")http://manpages.ubuntu.com/manpages/en/man8/slapd.8.html

[[124]](" \l "_ftnref124" \o ")http://manpages.ubuntu.com/manpages/en/man5/slapd-config.5.html

[[125]](" \l "_ftnref125" \o ")http://manpages.ubuntu.com/manpages/en/man5/slapd.access.5.html

[[126]](" \l "_ftnref126" \o ")http://manpages.ubuntu.com/manpages/en/man5/slapo-syncprov.5.html

[[127]](" \l "_ftnref127" \o ")http://manpages.ubuntu.com/manpages/en/man8/auth-client-config.8.html

[[128]](" \l "_ftnref128" \o ")http://manpages.ubuntu.com/manpages/en/man8/pam-auth-update.8.html

[[129]](" \l "_ftnref129" \o ")http://www.zytrax.com/books/ldap/

[[130]](" \l "_ftnref130" \o ")https://help.ubuntu.com/community/OpenLDAPServer

[[131]](" \l "_ftnref131" \o ")http://www.oreilly.com/catalog/ldapsa/

[[132]](" \l "_ftnref132" \o ")http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book

[[133]](" \l "_ftnref133" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupadd.8.html

[[134]](" \l "_ftnref134" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupdel.8.html

[[135]](" \l "_ftnref135" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupmod.8.html

[[136]](" \l "_ftnref136" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-groupshow.8.html

[[137]](" \l "_ftnref137" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-passwd.8.html

[[138]](" \l "_ftnref138" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-populate.8.html

[[139]](" \l "_ftnref139" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-useradd.8.html

[[140]](" \l "_ftnref140" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-userdel.8.html

[[141]](" \l "_ftnref141" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-userinfo.8.html

[[142]](" \l "_ftnref142" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-userlist.8.html

[[143]](" \l "_ftnref143" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-usermod.8.html

[[144]](" \l "_ftnref144" \o ")http://manpages.ubuntu.com/manpages/en/man8/smbldap-usershow.8.html

[[145]](" \l "_ftnref145" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[146]](" \l "_ftnref146" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html

[[147]](" \l "_ftnref147" \o ")http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/

[[148]](" \l "_ftnref148" \o ")https://help.ubuntu.com/community/Samba#samba-ldap

[[149]](" \l "_ftnref149" \o ")http://web.mit.edu/Kerberos/

[[150]](" \l "_ftnref150" \o ")https://help.ubuntu.com/community/Kerberos

[[151]](" \l "_ftnref151" \o ")http://oreilly.com/catalog/9780596004033/

[[152]](" \l "_ftnref152" \o ")http://freenode.net/

[[153]](" \l "_ftnref153" \o ")http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Configuring-Kerberos-with-OpenLDAP-back\u 002end

[[154]](" \l "_ftnref154" \o ")http://web.mit.edu/Kerberos/krb5-1.6/krb5-1.6.3/doc/krb5-admin.html#Global-Kerberos LDAP数据库上的操作

[[155]](" \l "_ftnref155" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man8/kdb5\_ldap\_util.8.html

[[156]](" \l "_ftnref156" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man5/krb5.conf.5.html

[[157]](" \l "_ftnref157" \o ")https://help.ubuntu.com/community/Kerberos#kerberos-ldap

[[158]](" \l "_ftnref158" \o ")https://github.com/SSSD/sssd

[[159]](" \l "_ftnref159" \o ")https://technet.microsoft.com/en-us/library/cc759550%28v=ws.10%29.aspx

[[160]](" \l "_ftnref160" \o ")http://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf\_files/krb5\_conf.html

[[161]](" \l "_ftnref161" \o ")https://help.ubuntu.com/community/BIND9ServerHowto

[[162]](" \l "_ftnref162" \o ")http://www.tldp.org/HOWTO/DNS-HOWTO.html

[[163]](" \l "_ftnref163" \o ")http://www.bind9.net/

[[164]](" \l "_ftnref164" \o ")http://shop.oreilly.com/product/9780596100575.do

[[165]](" \l "_ftnref165" \o ")http://shop.oreilly.com/product/0636920020158.do

[[166]](" \l "_ftnref166" \o ")http://freenode.net

[[167]](" \l "_ftnref167" \o ")http://www.shorewall.net/

[[168]](" \l "_ftnref168" \o ")https://wiki.ubuntu.com/UncomplicatedFirewall

[[169]](" \l "_ftnref169" \o ")http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html

[[170]](" \l "_ftnref170" \o ")http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html

[[171]](" \l "_ftnref171" \o ")https://help.ubuntu.com/community/IptablesHowTo

[[172]](" \l "_ftnref172" \o ")https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/1304134

[[173]](" \l "_ftnref173" \o ")https://bugs.launchpad.net/ubuntu/+source/apparmor/+filebug

[[174]](" \l "_ftnref174" \o ")http://www.novell.com/documentation/apparmor/apparmor201\_sp10\_admin/index.html?page=/documentation/apparmor/apparmor201\_sp10\_admin/data/

book\_apparmor\_admin.html

[[175]](" \l "_ftnref175" \o ")https://help.ubuntu.com/community/AppArmor

[[176]](" \l "_ftnref176" \o ")http://en.opensuse.org/SDB:AppArmor\_geeks

[[177]](" \l "_ftnref177" \o ")http://freenode.net

[[178]](" \l "_ftnref178" \o ")http://tldp.org/HOWTO/SSL-Certificates-HOWTO/index.html

[[179]](" \l "_ftnref179" \o ")http://en.wikipedia.org/wiki/HTTPS

[[180]](" \l "_ftnref180" \o ")http://www.openssl.org/

[[181]](" \l "_ftnref181" \o ")http://oreilly.com/catalog/9780596002701/

[[182]](" \l "_ftnref182" \o ")https://launchpad.net/ecryptfs

[[183]](" \l "_ftnref183" \o ")http://www.linuxjournal.com/article/9400

[[184]](" \l "_ftnref184" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man7/ecryptfs.7.html

[[185]](" \l "_ftnref185" \o ")http://www.nagios.org/

[[186]](" \l "_ftnref186" \o ")http://nagios.sourceforge.net/docs/3\_0/

[[187]](" \l "_ftnref187" \o ")http://www.nagios.org/propaganda/books/

[[188]](" \l "_ftnref188" \o ")https://help.ubuntu.com/community/Nagios3

[[189]](" \l "_ftnref189" \o ")http://munin-monitoring.org/

[[190]](" \l "_ftnref190" \o ")https://munin.readthedocs.io/en/latest/

[[191]](" \l "_ftnref191" \o ")http://www.ubuntu.com

[[192]](" \l "_ftnref192" \o ")http://www.ubuntu.com/community

[[193]](" \l "_ftnref193" \o ")http://httpd.apache.org/docs/2.4/

[[194]](" \l "_ftnref194" \o ")https://help.ubuntu.com/community/ServerSideIncludes

[[195]](" \l "_ftnref195" \o ")http://httpd.apache.org/docs/2.4/mod/mod\_negotiation.html#multiviews

[[196]](" \l "_ftnref196" \o ")http://httpd.apache.org/docs/2.4/

[[197]](" \l "_ftnref197" \o ")http://www.modssl.org/docs/

[[198]](" \l "_ftnref198" \o ")http://oreilly.com/catalog/9780596001919/

[[199]](" \l "_ftnref199" \o ")http://freenode.net/

[[200]](" \l "_ftnref200" \o ")https://help.ubuntu.com/community/ApacheMySQLPHP

[[201]](" \l "_ftnref201" \o ")http://www.php.net/docs.php

[[202]](" \l "_ftnref202" \o ")http://oreilly.com/catalog/0636920043034/

[[203]](" \l "_ftnref203" \o ")http://oreilly.com/catalog/9781565926813/

[[204]](" \l "_ftnref204" \o ")https://help.ubuntu.com/community/ApacheMySQLPHP

[[205]](" \l "_ftnref205" \o ")http://www.squid-cache.org/

[[206]](" \l "_ftnref206" \o ")https://help.ubuntu.com/community/Squid

[[207]](" \l "_ftnref207" \o ")http://rubyonrails.org/

[[208]](" \l "_ftnref208" \o ")http://pragprog.com/titles/rails3/agile-web-development-with-rails-third-edition

[[209]](" \l "_ftnref209" \o ")https://help.ubuntu.com/community/RubyOnRails

[[210]](" \l "_ftnref210" \o ")http://tomcat.apache.org/tomcat-7.0-doc/index.html

[[211]](" \l "_ftnref211" \o ")http://tomcat.apache.org/

[[212]](" \l "_ftnref212" \o ")http://shop.oreilly.com/product/9780596003180.do

[[213]](" \l "_ftnref213" \o ")http://wiki.apache.org/tomcat/Tomcat/Books

[[214]](" \l "_ftnref214" \o ")http://www.mysqlperformanceblog.com/2006/06/17/using-myisam-in-production/

[[215]](" \l "_ftnref215" \o ")http://en.wikipedia.org/wiki/ACID

[[216]](" \l "_ftnref216" \o ")http://tools.percona.com/members/wizard

[[217]](" \l "_ftnref217" \o ")http://www.mysql.com/

[[218]](" \l "_ftnref218" \o ")http://dev.mysql.com/doc/

[[219]](" \l "_ftnref219" \o ")http://www.informit.com/store/product.aspx?isbn=0768664128

[[220]](" \l "_ftnref220" \o ")https://help.ubuntu.com/community/ApacheMySQLPHP

[[221]](" \l "_ftnref221" \o ")http://www.postgresql.org/docs/current/static/admin.html

[[222]](" \l "_ftnref222" \o ")http://www.postgresql.org/docs/current/static/admin.html

[[223]](" \l "_ftnref223" \o ")http://www.postgresql.org/docs/current/static/backup.html

[[224]](" \l "_ftnref224" \o ")http://www.postgresql.org/docs/current/static/admin.html

[[225]](" \l "_ftnref225" \o ")http://www.informit.com/store/product.aspx?isbn=0768664128

[[226]](" \l "_ftnref226" \o ")https://help.ubuntu.com/community/PostgreSQL

[[227]](" \l "_ftnref227" \o ")http://moinmo.in/

[[228]](" \l "_ftnref228" \o ")http://moinmo.in/

[[229]](" \l "_ftnref229" \o ")https://help.ubuntu.com/community/MoinMoin

[[230]](" \l "_ftnref230" \o ")http://www.phpmyadmin.net/home\_page/docs.php

[[231]](" \l "_ftnref231" \o ")http://www.packtpub.com/phpmyadmin-3rd-edition/book

[[232]](" \l "_ftnref232" \o ")https://help.ubuntu.com/community/phpMyAdmin

[[233]](" \l "_ftnref233" \o ")https://codex.wordpress.org/

[[234]](" \l "_ftnref234" \o ")https://help.ubuntu.com/community/WordPress

[[235]](" \l "_ftnref235" \o ")http://vsftpd.beasts.org/vsftpd\_conf.html

[[236]](" \l "_ftnref236" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man5/vsftpd.conf.5.html

[[237]](" \l "_ftnref237" \o ")http://nfs.sourceforge.net/

[[238]](" \l "_ftnref238" \o ")https://help.ubuntu.com/community/NFSv4Howto

[[239]](" \l "_ftnref239" \o ")http://www.open-iscsi.com/

[[240]](" \l "_ftnref240" \o ")http://wiki.debian.org/SAN/iSCSI/open-iscsi

[[241]](" \l "_ftnref241" \o ")http://www.cups.org/

[[242]](" \l "_ftnref242" \o ")http://wiki.debian.org/SAN/iSCSI/open-iscsi

[[243]](" \l "_ftnref243" \o ")http://www.ietf.org/rfc/rfc2554.txt

[[244]](" \l "_ftnref244" \o ")http://www.ietf.org/rfc/rfc2222.txt

[[245]](" \l "_ftnref245" \o ")http://freenode.net

[[246]](" \l "_ftnref246" \o ")http://www.ubuntu.com/support/community/webforums

[[247]](" \l "_ftnref247" \o ")http://www.postfix-book.com/

[[248]](" \l "_ftnref248" \o ")http://www.postfix.org/documentation.html

[[249]](" \l "_ftnref249" \o ")https://help.ubuntu.com/community/Postfix

[[250]](" \l "_ftnref250" \o ")http://www.exim.org/

[[251]](" \l "_ftnref251" \o ")http://www.uit.co.uk/content/exim-smtp-mail-server

[[252]](" \l "_ftnref252" \o ")https://help.ubuntu.com/community/Exim4

[[253]](" \l "_ftnref253" \o ")https://wiki2.dovecot.org/MailboxFormat

[[254]](" \l "_ftnref254" \o ")http://www.dovecot.org/

[[255]](" \l "_ftnref255" \o ")https://help.ubuntu.com/community/Dovecot

[[256]](" \l "_ftnref256" \o ")http://lists.ubuntu.com

[[257]](" \l "_ftnref257" \o ")http://www.exim.org

[[258]](" \l "_ftnref258" \o ")http://www.list.org/mailman-install/index.html

[[259]](" \l "_ftnref259" \o ")http://www.exim.org/howto/mailman21.html

[[260]](" \l "_ftnref260" \o ")https://help.ubuntu.com/community/Mailman

[[261]](" \l "_ftnref261" \o ")http://www.ijs.si/software/amavisd/amavisd-new-docs.html

[[262]](" \l "_ftnref262" \o ")http://www.clamav.net/doc/latest/html/

[[263]](" \l "_ftnref263" \o ")http://wiki.clamav.net/Main/WebHome

[[264]](" \l "_ftnref264" \o ")http://wiki.apache.org/spamassassin/

[[265]](" \l "_ftnref265" \o ")http://sourceforge.net/apps/trac/pyzor/

[[266]](" \l "_ftnref266" \o ")http://razor.sourceforge.net/

[[267]](" \l "_ftnref267" \o ")http://dkim.org/

[[268]](" \l "_ftnref268" \o ")https://help.ubuntu.com/community/PostfixAmavisNew

[[269]](" \l "_ftnref269" \o ")http://freenode.net

[[270]](" \l "_ftnref270" \o ")http://www.irc.org/tech\_docs/ircnet/faq.html

[[271]](" \l "_ftnref271" \o ")http://codex.xiaoka.com/wiki/jabberd2:start

[[272]](" \l "_ftnref272" \o ")http://www.jabberdoc.org/

[[273]](" \l "_ftnref273" \o ")https://help.ubuntu.com/community/SettingUpJabberServer

[[274]](" \l "_ftnref274" \o ")https://launchpad.net/

[[275]](" \l "_ftnref275" \o ")http://bazaar-vcs.org/LaunchpadIntegration/

[[276]](" \l "_ftnref276" \o ")http://svnbook.red-bean.com/

[[277]](" \l "_ftnref277" \o ")http://bazaar.canonical.com/en/

[[278]](" \l "_ftnref278" \o ")https://launchpad.net/

[[279]](" \l "_ftnref279" \o ")http://git-scm.com

[[280]](" \l "_ftnref280" \o ")https://github.com/sitaramc/gitolite

[[281]](" \l "_ftnref281" \o ")http://subversion.apache.org/

[[282]](" \l "_ftnref282" \o ")http://svnbook.red-bean.com/

[[283]](" \l "_ftnref283" \o ")https://help.ubuntu.com/community/EasyBazaar

[[284]](" \l "_ftnref284" \o ")https://help.ubuntu.com/community/Subversion

[[285]](" \l "_ftnref285" \o ")http://www.samba.org

[[286]](" \l "_ftnref286" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[287]](" \l "_ftnref287" \o ")http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM

[[288]](" \l "_ftnref288" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[289]](" \l "_ftnref289" \o ")http://www.amazon.com/exec/obidos/tg/detail/-/0131882228

[[290]](" \l "_ftnref290" \o ")http://www.oreilly.com/catalog/9780596007690/

[[291]](" \l "_ftnref291" \o ")https://help.ubuntu.com/community/Samba

[[292]](" \l "_ftnref292" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[293]](" \l "_ftnref293" \o ")http://www.amazon.com/exec/obidos/tg/detail/-/0131882228

[[294]](" \l "_ftnref294" \o ")http://www.oreilly.com/catalog/9780596007690/

[[295]](" \l "_ftnref295" \o ")http://www.cups.org/

[[296]](" \l "_ftnref296" \o ")https://help.ubuntu.com/community/Samba

[[297]](" \l "_ftnref297" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id349531

[[298]](" \l "_ftnref298" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[299]](" \l "_ftnref299" \o ")http://www.amazon.com/exec/obidos/tg/detail/-/0131882228

[[300]](" \l "_ftnref300" \o ")http://www.oreilly.com/catalog/9780596007690/

[[301]](" \l "_ftnref301" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html

[[302]](" \l "_ftnref302" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/AccessControls.html#id397568

[[303]](" \l "_ftnref303" \o ")http://www.pathname.com/fhs/pub/fhs-2.3.html#SRVDATAFORSERVICESPROVIDEDBYSYSTEM

[[304]](" \l "_ftnref304" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/

[[305]](" \l "_ftnref305" \o ")http://www.amazon.com/exec/obidos/tg/detail/-/0131882228

[[306]](" \l "_ftnref306" \o ")http://www.oreilly.com/catalog/9780596007690/

[[307]](" \l "_ftnref307" \o ")http://samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html

[[308]](" \l "_ftnref308" \o ")http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html

[[309]](" \l "_ftnref309" \o ")https://help.ubuntu.com/community/Samba

[[310]](" \l "_ftnref310" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man1/smbclient.1.html

[[311]](" \l "_ftnref311" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man8/mount.cifs.8.html

[[312]](" \l "_ftnref312" \o ")https://help.ubuntu.com/community/Samba

[[313]](" \l "_ftnref313" \o ")http://tldp.org/LDP/abs/html/

[[314]](" \l "_ftnref314" \o ")http://safari.samspublishing.com/0672323583

[[315]](" \l "_ftnref315" \o ")https://help.ubuntu.com/community/CronHowto

[[316]](" \l "_ftnref316" \o ")http://www.gnu.org/software/tar/manual/index.html

[[317]](" \l "_ftnref317" \o ")http://en.wikipedia.org/wiki/Backup\_rotation\_scheme

[[318]](" \l "_ftnref318" \o ")http://www.gnu.org/software/cpio/

[[319]](" \l "_ftnref319" \o ")http://www.gnu.org/software/coreutils/

[[320]](" \l "_ftnref320" \o ")http://www.rsnapshot.org/

[[321]](" \l "_ftnref321" \o ")http://www.samba.org/ftp/rsync/rsync.html

[[322]](" \l "_ftnref322" \o ")http://blog.bacula.org/documentation/documentation/

[[323]](" \l "_ftnref323" \o ")http://www.bacula.org/

[[324]](" \l "_ftnref324" \o ")https://help.ubuntu.com/community/Bacula

[[325]](" \l "_ftnref325" \o ")https://help.ubuntu.com/18.04/installation-guide/

[[326]](" \l "_ftnref326" \o ")http://libvirt.org/uri.html

[[327]](" \l "_ftnref327" \o ")https://libvirt.org/migration.html#offline

[[328]](" \l "_ftnref328" \o ")https://libvirt.org/migration.html

[[329]](" \l "_ftnref329" \o ")http://wiki.qemu.org/Features/PostCopyLiveMigration

[[330]](" \l "_ftnref330" \o ")https://wiki.ubuntu.com/QemuKVMMigration

[[331]](" \l "_ftnref331" \o ")https://libvirt.org/formatdomain.html

[[332]](" \l "_ftnref332" \o ")https://www.kernel.org/doc/Documentation/vfio.txt

[[333]](" \l "_ftnref333" \o ")https://bugs.launchpad.net/ubuntu/+source/libvirt/+bug/1552241

[[334]](" \l "_ftnref334" \o ")http://wiki.apparmor.net/index.php/AppArmor\_Failures#Messages\_in\_the\_Log\_files

[[335]](" \l "_ftnref335" \o ")https://en.wikibooks.org/wiki/QEMU/Monitor

[[336]](" \l "_ftnref336" \o ")http://www.linux-kvm.org/

[[337]](" \l "_ftnref337" \o ")http://libvirt.org/

[[338]](" \l "_ftnref338" \o ")http://virt-manager.org/

[[339]](" \l "_ftnref339" \o ")http://freenode.net/

[[340]](" \l "_ftnref340" \o ")https://help.ubuntu.com/community/KVM

[[341]](" \l "_ftnref341" \o ")https://help.ubuntu.com/community/Xen

[[342]](" \l "_ftnref342" \o ")http://www.linux-kvm.org/page/How\_to\_assign\_devices\_with\_VT-d\_in\_KVM#Assigning\_the\_device

[[343]](" \l "_ftnref343" \o ")http://wiki.qemu.org/Main\_Page

[[344]](" \l "_ftnref344" \o ")http://wiki.qemu.org/download/qemu-doc.html#sec\_005finvocation

[[345]](" \l "_ftnref345" \o ")http://wiki.qemu.org/download/qemu-doc.html#pcsys\_005fmonitor

[[346]](" \l "_ftnref346" \o ")https://wiki.ubuntu.com/QemuKVMMigration#Upgrade\_machine\_type

[[347]](" \l "_ftnref347" \o ")https://lists.ubuntu.com/mailman/listinfo/ubuntu-server

[[348]](" \l "_ftnref348" \o ")http://docs.openstack.org/havana/install-guide/install/apt/content/

[[349]](" \l "_ftnref349" \o ")https://launchpad.net/~openstack

[[350]](" \l "_ftnref350" \o ")http://wiki.openstack.org

[[351]](" \l "_ftnref351" \o ")https://bugs.launchpad.net/nova

[[352]](" \l "_ftnref352" \o ")http://en.wikipedia.org/wiki/Cloud\_computing#Service\_Models

[[353]](" \l "_ftnref353" \o ")http://www.openstack.org/software/openstack-compute/

[[354]](" \l "_ftnref354" \o ")http://docs.openstack.org/diablo/openstack-compute/starter/content/GlanceMS-d2s21.html

[[355]](" \l "_ftnref355" \o ")http://docs.openstack.org/trunk/openstack-object-storage/admin/content/index.html

[[356]](" \l "_ftnref356" \o ")http://docs.openstack.org/trunk/openstack-object-storage/admin/content/installing-openstack-object-storage-on-ubuntu.html

[[357]](" \l "_ftnref357" \o ")http://blog.dustinkirkland.com/2015/09/container-summit-presentation-and-live.html

[[358]](" \l "_ftnref358" \o ")https://help.ubuntu.com/lts/serverguide/lxc.html

[[359]](" \l "_ftnref359" \o ")http://github.com/lxc/lxd

[[360]](" \l "_ftnref360" \o ")http://linuxcontainers.org/lxd/try-it

[[361]](" \l "_ftnref361" \o ")https://www.stgraber.org/2016/03/11/lxd-2-0-blog-post-series-012/

[[362]](" \l "_ftnref362" \o ")https://docs.jujucharms.com/devel/en/clouds-lxd

[[363]](" \l "_ftnref363" \o ")http://open-zfs.org

[[364]](" \l "_ftnref364" \o ")https://github.com/lxc/lxd/blob/master/doc/configuration.md

[[365]](" \l "_ftnref365" \o ")https://github.com/lxc/lxd/blob/master/doc/configuration.md

[[366]](" \l "_ftnref366" \o ")http://manpages.ubuntu.com/manpages/xenial/en/man5/subuid.5.html

[[367]](" \l "_ftnref367" \o ")http://manpages.ubuntu.com/manpages/xenial/en/man5/lxc.container.conf.5.html

[[368]](" \l "_ftnref368" \o ")https://launchpad.net/simplestreams

[[369]](" \l "_ftnref369" \o ")https://www.ibm.com/developerworks/linux/library/l-lxc-containers/

[[370]](" \l "_ftnref370" \o ")http://www.ibm.com/developerworks/linux/library/l-lxc-security/index.html

[[371]](" \l "_ftnref371" \o ")http://manpages.ubuntu.com/manpages/en/man7/capabilities.7.html

[[372]](" \l "_ftnref372" \o ")http://manpages.ubuntu.com/manpages/en/man5/lxc.conf.5.html

[[373]](" \l "_ftnref373" \o ")http://linuxcontainers.org

[[374]](" \l "_ftnref374" \o ")http://wiki.ubuntu.com/LxcSecurity

[[375]](" \l "_ftnref375" \o ")http://www.drbd.org/

[[376]](" \l "_ftnref376" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man5/drbd.conf.5.html

[[377]](" \l "_ftnref377" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man8/drbdadm.8.html

[[378]](" \l "_ftnref378" \o ")https://help.ubuntu.com/community/DRBD

[[379]](" \l "_ftnref379" \o ")http://openvpn.net/index.php/open-source/documentation/howto.html#security

[[380]](" \l "_ftnref380" \o ")http://www.openvpn.net/index.php/open-source/downloads.html

[[381]](" \l "_ftnref381" \o ")http://wiki.openwrt.org/doc/howto/vpn.overview

[[382]](" \l "_ftnref382" \o ")http://openvpn.net/

[[383]](" \l "_ftnref383" \o ")http://openvpn.net/index.php/open-source/documentation/howto.html#security

[[384]](" \l "_ftnref384" \o ")http://www.packtpub.com/openvpn/book

[[385]](" \l "_ftnref385" \o ")http://landscape.canonical.com/

[[386]](" \l "_ftnref386" \o ")http://www.weather.gov/tg/siteloc.shtml

[[387]](" \l "_ftnref387" \o ")http://manpages.ubuntu.com/manpages/bionic/en/man5/update-motd.5.html

[[388]](" \l "_ftnref388" \o ")http://debaday.debian.net/2007/10/04/weather-check-weather-conditions-and-forecasts-on-the-command-line/

[[389]](" \l "_ftnref389" \o ")http://etckeeper.branchable.com/

[[390]](" \l "_ftnref390" \o ")http://bazaar-vcs.org/

[[391]](" \l "_ftnref391" \o ")http://www.gnu.org/software/screen/

[[392]](" \l "_ftnref392" \o ")https://help.ubuntu.com/community/Screen

[[393]](" \l "_ftnref393" \o ")https://launchpad.net/byobu

[[394]](" \l "_ftnref394" \o ")https://launchpad.net/

[[395]](" \l "_ftnref395" \o ")https://help.launchpad.net/YourAccount/NewAccount

[[396]](" \l "_ftnref396" \o ")http://manpages.ubuntu.com/manpages/en/man8/update-alternatives.8.html

[[397]](" \l "_ftnref397" \o ")https://help.ubuntu.com/community/ReportingBugs

[[398]](" \l "_ftnref398" \o ")https://wiki.ubuntu.com/Apport