



Turbolinux Enterprise Server 8 powered by UnitedLinux

白皮书



商标声明

出版商声明使用商标名称仅仅用于编辑目的，而不是有意侵权，因此文中引用处没有列出拥有这些商标的公司或实体或在每次插入商标符号时注明商标名称。

目 录

1 引言	1
1.1 什么是 Turbolinux Enterprise Server 8 powered by UnitedLinux?	1
1.2 UnitedLinux 的优点	1
1.2.1 对于客户	1
1.2.2 对于业界	2
1.3 文档范围和组织	2
2 概述	3
2.1 体系结构	3
2.2 支持的平台	3
2.3 标准符合性	3
2.3.1 Linux Standard Base	4
2.3.2 本地化与国际化 – L10N 和 I18N	4
2.4 企业特性	4
2.5 基本核心组件	6
2.6 基本功能	7
2.6.1 服务器，服务和应用	7
2.7 文档	8
3 可扩展性和高可用性	9
3.1 可扩展性	9
3.2 高可用性	9
4 文件系统	10
4.1 Ext2	10
4.2 日志文件系统	10
4.2.1 Ext3	10
4.2.2 ReiserFS	10
4.2.3 JFS	11
4.3 其它文件系统	11
4.4 LVM	12
5 网络	13
5.1 带 IPSec 的 VPN	13
5.2 SNMP	13
5.3 Quality of Service (QoS)	14

5.4 高级路由能力	14
6 异种环境的互操作性	15
6.1 Windows 网络	15
6.2 Novell 网络	15
6.3 UNIX 网络	15
6.4 认证互操作性	15
7 安全	17
7.1 认证灵活性	17
7.2 用户信息数据	17
7.3 加密支持	17
7.4 一般特性	18
7.5 易于软件升级	19
7.6 防火墙	19
7.7 网络侵入检测	19
8 开发环境	21
9 中文化	22
10 结论	23
11 更多信息	24

1 引言

1.1 什么是 Turbolinux Enterprise Server 8 powered by UnitedLinux?

Turbolinux Enterprise Server 8 powered by UnitedLinux 是 Turbolinux 公司基于 UnitedLinux 的最新 Linux 服务器发行版本。而 UnitedLinux 是业界领导者厂商 Conectiva、SCO Group、SuSE 和 Turbolinux 组成联合组织并决定开发的高质量 Linux 操作系统。

根据协定，四家公司将围绕一个共同的 Linux 版本组织开发力量。它设计作为一种企业级 Linux 操作系统，UnitedLinux 将为应用开发、认证和部署提供一个稳定、统一的平台。

通过开发和提供统一的 Linux 系统，UnitedLinux 将促进 Linux 销售商、ISV、IHV 和 OEM 提供高价值的统一 Linux 系统。它将有助于集中更多的资源促进 Linux 发展，获得质量更高、功能更强的产品。

UnitedLinux 定义一个共同的基准（“UL 基准”），它作为各销售商的所有 Linux 发布的基础。共享核心系统将简化 OEM 和 ISV 认证，这样，所有软、硬件产品只需要对一个平台进行认证，而不是对多个 Linux 发行版本进行认证。

各公司可以通过自己的市场定位和优势将 UnitedLinux 再次品牌化，并增加其它增值扩展。因此，UnitedLinux 必须清楚地定义什么构成其 UL 基准，哪些组件可以作为销售商添加的扩展，以及它们与 UL 基准的关系。

1.2 UnitedLinux 的优点

1.2.1 对于客户

- 联合多家顶级 Linux 公司的专长

通过联合，各 UL 联盟成员可以为其客户提供共同开发的成果。

- 稳定性

由于构筑于可靠的基础之上，UnitedLinux 可以为客户提供企业级操作系统，具有极其优异的稳定性和可靠性。

- 质量保证

经过国际 QA 小组和认证实验室的试验，基于开放源代码操作系统的 UnitedLinux 可以提供与昂贵的专有系统相媲美的一流品质水平。

- 认证

经过主要软件和硬件销售商的认证，UnitedLinux 为应用软件提供一个完美的平台环境，并与硬件平台和外围设备完全兼容。

- 全球供货

UnitedLinux 可以在世界各地购买，并在世界范围内支持代理支持。

1.2.2 对于业界

- 较少的认证发布

基于 UnitedLinux 的 Linux 发布，共享一个共同的系统内核和一组标准应用软件。软件和硬件的认证只需要进行一次，但对所有基于 UnitedLinux 的 Linux 发行版本均有效。

- 认证

UnitedLinux 为应用软件提供一个完美的平台环境，经过认证的硬件和软件可以非常容易地满足客户的要求。

- 标准相容性

在运行时和开发环境方面，UnitedLinux 完全符合当前业界标准和 Internet 标准。对于无标准可遵循的场合，则遵守“事实上”的通行规则。

- 全球供货

UnitedLinux 可以在世界各地购买，并在世界范围内支持代理支持。

1.3 文档范围和组织

本文档将详细地介绍 UnitedLinux 基准系统和标准特性。第 1 节对 UnitedLinux 进行简单的介绍及其优点。第 2 节将简单介绍有关体系结构，UnitedLinux 所遵循的标准，以及它所提供的企业特性。第 3 节介绍有关 UnitedLinux 的高可用性和可扩展性。第 4 节将介绍 UnitedLinux 所支持的文件系统，包括日志文件系统在内的主要文件系统。UnitedLinux 网络能力及其主要特性将在第 5 节介绍。UnitedLinux 和其它操作系统之间的互操作性将在第 6 节介绍。

UnitedLinux 客户关心的两个主要话题，即“安全”与“开发”，也将在此文档的第 7 节和第 8 节中介绍。

2 概述

2.1 体系结构

SCO Hooks	Conectiva Hooks	SuSE Hooks	Turbolinux Hooks	UL 特性	LSB 未来扩展
LSB					
通用硬件数据 库和通用自动 监测信息库	通用包 库，内核，驱动程 序及更新		通用配置，文件位 置，句法和语义		

2.2 支持的平台

UnitedLinux 最初将提供基于下述平台的发布 x86 32 位, IA64, x86-64 和 IBM z, i 和 pSeries。

2.3 标准符合性

UL 将遵守当前和未来的 Linux 标准和业界标准，允许 ISV 开发的软件在相似的 Linux 基准之间迁移。相关的标准清单如下所述：

- FHS
文件系统体系标准 (Filesystem Hierarchy Standard)，包括类UNIX操作系统文件和目录的一系列要求和指南。
- LSB
(参见节 2.3.1)
- OpenI18N
(参见节 2.3.2)
- GB18030

UnitedLinux 提供与 GB18030 兼容的中文字形用于输入、输出和打印。

GB18030 规定了一个映射表，它覆盖所有 Unicode 编码点，并保持与 GBK 和 GB2312 编码的文本兼容。

对于无标准可遵循的场合，如果存在“事实上”的通行规则，则遵守“事实上”的通行规则。如果通行的规则不适用，则 Linux 开发商协定一个新的“事实上”标准。

如果可能，UnitedLinux 应当为非 UL 系统提供兼容模式或移植工具。

2.3.1 Linux Standard Base

Linux标准基准 (Linux Standard Base, LSB) 的目标是开发和推广一组标准。它们将增加各Linux发布之间的兼容性,并允许软件应用运行于任何兼容的Linux系统。此外,LSB还将协调和号召软件销售商,为Linux移植和编写产品。

2.3.2 本地化与国际化 – L10N 和 I18N

所有 UL 软件应遵从国际化标准,这些标准可以从 <http://www.linux.org/> 获得。

OpenI18N2000 技术规范包括所有商用 UNIX 系统已经成功实现的最优国际化功能。同时,在此基础上进行扩充,使得 Linux 国际化满足所有国家和地区的要求。通过遵循 OpenI18N2000 技术规范,“基于 UnitedLinux”的产品将受益于基于 UNICODE 的多语言特性,并且可相互之间可以移植。

OpenI18N的赞助商包括 Compaq Computer, Conectiva Linux, Digital Factory 和 Kondar Project, Fujitsu 有限公司, Hitachi 有限公司, IBM 公司, 日本 PPC Linux 用户集团 (JPLIG), NEC 公司, Red Hat 公司, SGI, SuSE Linux AG. 和 Turbolinux 公司。

关于 OpenI18N

OpenI18N 是自由标准组织 (Free Standards Group) 属下的一个工程。其成员由与 Linux 和开放源代码相关的从事全球化 (国际化和本地化相结合) 工作的贡献者构成。它创始于 1999 年 8 月,其最终目的是在全球范围内为 Linux 和其它开放源代码工程实现软件/应用的可移植性和互操作性。其活动主要集中于 API 核心集和 Linux 发布组件的国际化,以便实现一个通用的 Linux 环境。

2.4 企业特性

UnitedLinux 对大量标准和未来的硬件和软件技术提供支持,简述如下:

- 自动安装

通过从一个 XML 文件读取所有安装选项, UnitedLinux 安装程序能够进行自动安装。它也可以将 KickStart 配置转换为 UL 的 XML 格式来进行。

- 多种安装方法

UL 可以通过下述来源之一进行安装:

- 本地 CDROM
- NFS 装载目录
- 本地硬盘分区

- 高可用性

参见节 3.2

- 日志文件系统

参见节 4.2

- LVM

参见节 4.4

- NGPT

下一代 POSIX 线程是 GNU Pthreads 的派生物,它基本上与 POSIX 完全兼容,并将增加 MxN 线程能力,显著改善 Linux Pthreads 的 POSIX 兼容性。通过使用 Pthreads 库,所有应用的性能得到显著地提高,尤其是 SMP 机器。同时,它还允许 Linux 提供商使用 UNIX 操作系统如 IBM AIX 和 SGI IRIX 的线程服务能力。

- MXT

内存扩展支持 (Memory eXpansion Technology, MXT) 是一种用于压缩主内存内容的硬件技术。它可有效地使内存容量翻倍。MXT 对 CPU、I/O 设备、应用软件和设备驱动是透明的,不需要进行任何软件修改。

- POSIX 异步 I/O

异步 I/O (Asynchronous I/O, AIO) 工具实现 POSIX 标准定义的接口。通过使用分段 I/O,初始请求 (如 aioread) 可以真正地使设备 I/O 作为 I/O 请求的第一阶段进行排队;作为 I/O 完成部分的 I/O 请求的第二阶段将用于传递请求的结果。结果中可能包括一次读操作中 I/O 缓冲区的内容,读写的字节数和任何错误状态。

- 原始 I/O

通过直接传输数据到应用地址空间,绕过 SCSI 和 FibreChannel 设备的内核缓冲区和 I/O 队列代码,原始 I/O 增强特性可以提供高带宽、低开销 SCSI 盘的 I/O 能力。

- 直接 I/O

直接 I/O 通过直接在用户空间缓冲区和 I/O 设备之间移动数据,而不需要依靠内核空间进行拷贝。由于避免大量的拷贝操作和绕过操作系统的分页高速缓存,总体性能得到改进。

- 超线程

Hyper-Threading (超线程) 允许多线程服务器软件在各服务器处理器内并行地执行线程,因此显著地改善企业和 e-Business 软件的交易率、响应时间和其它特性。

- SNMP

简单网络管理协议 (Simple Network Management Protocol, SNMP) 是一种负责网络管理和监控网络设备及其功能的协议 (参见节 5.2)。

- 大内存支持

对于 x86 32 位平台, Linux 内核通常限于 1GB 的物理内存和 4GB 的虚拟寻址空间。使用大内存支持特性, Linux 可以利用 Intel 的物理寻址扩展功能,支持高达 64GB 的物理 RAM 和各进程的全部 4GB 的虚拟寻址空间。此外,对于 AMD 的 x86-64 体系结构, Linux 允许对企业系统提供高效的平展式 64 位内存寻址能力。

- IPv6

IPv6 表示“ Internet Protocol Version 6”(Internet 协议版本 6)。它设计用于替代当前的 Internet IPv4 协议。IPv6 修订了 IPv4 中的一系列问题，如有限数量的 IPv4 地址；相对 IPv4 而言，增加了许多改进，如路由和网络自动配置。

- 目录服务

通过使用最新的 LDAP 和 LDAPv3 协议，UL 可以更好地管理大用户集，更好地与如邮件服务器、认证服务器等应用集成。

2.5 基本核心组件

基于 UL 的 Linux 系统构筑于下述核心组件之上：

- LSB 1.2 运行时环境（所有库、命令和接口）
- glibc 2.2.5
- 标准 Linux 和 UNIX 外壳程序：bash, csh, ksh
- textutils
- fileutils
- sh-utils
- sharutils
- util-linux
- SysVinit
- vixie-cron
- 远程外壳程序工具：ssh, scp
- 网络工具（ping, traceroute, nslookup）
- IPv6（基本工具如 ifconfig/route 和 config 定位）
- 防火墙工具（ipchains, iptables, masquerading）
- 脚本语言：python, perl, PHP, TCL/TK, ruby
- Java 运行时
- XFree86 4.2（库与服务器）
- X 打印服务（libXp.so.6）
- 针对宽字符支持的自由字形
- 针对宽字符支持的自由输入方法
- KDE 3.0 库
- 高可用性
- Postgresql
- SNMP
- CUPS
- I18n（ptBR, es, XFree 死键补钉）
- 硬件监控工具（lmsensors 等）
- 远程启动（TFTP, PXE 等）

2.6 基本功能

2.6.1 服务器，服务和应用

- Web 服务器（基本功能）
 - Apache web 服务器
 - Apache 扩展模块
 - PHP
 - PHP 扩展
 - Tomcat
- 文件和打印
 - Windows (Samba 2.2.4)
 - Mac (netatalk)
 - UNIX (带 LPR symlink 的 CUPS 打印系统, NFS 服务器)
- 域名服务器和 Internet/Intranet 连接服务器
 - DNS (bind)
 - WINS (Samba)
 - DHCP 服务器和客户
 - FTP
 - TFTP
- 邮件和新闻服务器
 - SMTP (sendmail)
 - POP
 - IMAP
- 代理服务器
 - Squid
- SQL 数据库服务器
 - 基本功能
 - 基于相关标准的扩展，用于异种 OS 访问支持 (ODBC , JDBC)
- 认证服务器（基本功能）
 - OpenLDAP
 - Kerberos 5
 - PAM 模块
 - NIS 服务器
- 时间服务器
 - NTP
- 文本编辑器
 - vim
- 卷管理器
 - LVM
- Acrobat Reader
- KDE 3.0 最小系统 (kdebase 和 Konqueror)
- GNOME 2.0 最小系统

- Mozilla 1.0
- OpenLDAP 2.1

2.7 文档

UnitedLinux 将受益于全球不同公司的开发成果，加强其在多种语言方面的国际专长。所有本地化工作被反馈到软件文档的原始作者和维护者，使得本地化的特性可以向所有人开放，同时确保未来的版本中包括更多、更完整的翻译。

3 可扩展性和高可用性

3.1 可扩展性

UnitedLinux 带有用于构筑服务器群的全套软件和工具，它允许系统管理单一机器难于胜任的负载。它将改善所有 UnitedLinux 特性，带宽可以扩展到超过千兆比特，服务器集群的节点数可以远远超过 64，从而改善系统的能力和灵活性。

3.2 高可用性

UnitedLinux 的高可用性支持基于模块方式，是 Linux-HA 工程中的一种稳定、可靠的技术。其功能强大的软件包覆盖 HA 集群的各个领域，从简单的双节点切换集群到负载均衡服务器庄园。它得到如开放集群架构（Open Clustering Framework）和高可用性服务论坛（Service Availability Forum）等公众标准化努力的支持，便于无缝地与其它软件集成，并不断地跟踪世界范围内安装客户的需要。

为了防止出现服务停机时间，并增加系统可用性，UL 提供了用于服务监控、自动切换、数据镜像和文件系统恢复等一系列工具。

如果通过 Turbolinux TurboHA 6，系统可以得到完全符合电信级需求的 24 × 7 系统。

4 文件系统

4.1 Ext2

Ext2 文件系统是 Linux 特有的文件系统,它拥有传统 UNIX 文件系统的许多特性,如块、inode 和目录等概念。Ext2 非常健壮,具有很多优良的性能。同时,Ext2 也是可扩展的,它提供的扩展功能允许用户在不格式化文件系统的情况下使用新的特性。表 1 给出了 ext2 文件系统的基本特性。

最大文件大小:	1TB
最大文件极限:	仅受文件系统大小限制
最大分区/文件系统大小:	4TB
最大文件名长度:	255 字符
缺省最小/最大块大小:	1024/4096 字节
缺省 inode 分配:	每 4096 字节为 1
在强制 FS 检查前的最大装载:	20 (可配置)

表 1 Ext2 特性

4.2 日志文件系统

4.2.1 Ext3

Ext3 文件系统构筑于 ext2 文件系统之上,对标准的 Linux ext2 文件系统进行了日志扩展。日志特性显著地减少文件系统崩溃后的恢复时间,它被广泛地应用于带有共享磁盘的 HA 站点。表 2 给出了 ext3 文件系统的基本特性。

最大文件大小:	1TB
最大文件极限:	仅受文件系统大小限制
最大分区/文件系统大小:	4TB
最大文件名长度:	255 字符
缺省最小/最大块大小:	1024/4096 字节
缺省 inode 分配:	每 4096 字节为 1
在强制 FS 检查前的最大装载:	20 (可配置)

表 2 Ext3 极限

4.2.2 ReiserFS

ReiserFS 文件系统 3.2.25 版是一种可选的日志文件系统。其优点包括更好的磁盘空间利用率、更好的磁盘访问性能和更快的崩溃恢复功能。表 3 给出了 ReiserFS 的基本特性。

最大文件大小：	1TB
最大文件极限：	32k 目录，42 亿文件
最大分区/文件系统大小：	4TB
最大文件名长度：	255 字符

表 3 ReiserFS 极限

4.2.3 JFS

日志文件系统 (Journaled File System, JFS) 是一种全 64 位文件系统。所有文件系统结构字段均为 64 位大小。它允许 JFS 同时支持大文件和分区。JFS 由 IBM 根据 GPL 许可开发，它是从其 AIX 系统移植过来的。

JFS 提供基于日志的字节级文件系统，它可以开发用于面向交易的高性能系统。它是可扩展的，且稳定可靠，其优于非日志文件系统之处在于其快速重新启动能力。JFS 可以在数秒钟或分钟之间将文件系统恢复到完好一致的状态。

尽管它主要针对服务器的高吞吐量和可靠性要求(从单一处理器系统到高级多处理器和集群系统) 而设计，JFS 同样也适用于要求性能和可靠性的客户配置。

表 4 给出 JFS 的基本特性。

最小文件系统大小	16 MB
最大文件大小：	受体系结构限制
最大文件极限：	受文件系统大小限制
缺省最小/最大块大小：	1024/4096 字节
缺省 inode 分配：	动态

表 4 JFS 基本特性

4.3 其它文件系统

为了确保最大的兼容性以及便于与其它系统进行数据交换，它同时也支持一系列其它文件系统：

- ISO9660 (CDROM)
- UDF (DVD/包模式CDRW)
- EFS (非ISO9660 CDROM, IRIX < 5.3 XFS)
- CRAMFS (压缩ROM文件系统)
- ROMFS (小ROM 文件系统)
- TMPFS (RAM盘文件系统)
- NTFS (Microsoft Windows NT)
- BFS (UnixWare启动文件系统)
- SYSV (SCO/Xenix/Coherent)
- UFS (BSD及派生文件系统)

- FAT/VFAT (Microsoft DOS和Windows 9x)
- HFS (Macintosh)
- HPFS (OS/2)
- UMSDOS (用于DOS磁盘映像的类UNIX FS)
- QNX4
- Minix

4.4 LVM

逻辑卷管理程序 (Logical Volume Manager, LVM) 是一种在线磁盘存储管理的子系统，它已经成为跨 Linux 存储管理的“事实上”标准。

LVM 支持磁盘和磁盘子系统的企业级卷管理，它可以成组任意数量的磁盘到卷组。卷组的总能力可以分配给逻辑卷，这些逻辑卷可以按正常块设备来进行访问。

此外，LVM 还提供存储的逻辑分离。当在线地对块设备进行大小调整的过程中，可以将数据从一个物理设备移动到另一个物理设备。LVM 也允许系统管理员轻松地对系统进行升级，去除有故障的磁盘，重新组织负载，并适应变化了的系统需求。表 5 列出了 UL 中使用的 LVM 基本特性。

最大逻辑卷大小	从使用 4 Mb 盘区的 256 Gb 到使用较大 PE 的 1 Pb
最大逻辑卷数：	256
最大逻辑组数：	99
每 PV 的最大 PE 数：	65534
缺省物理盘区大小：	4 Mb

表 5 LVM 基本特性

5 网络

5.1 带 IPSec 的 VPN

虚拟私有网络 (Virtual Private Network, VPN) 是私有网络的扩展, 它包括跨共享网络或公共网络如 Internet 的连接。VPN 允许用户在家中、在路上或分支办事处通过公共 Internet 以一种安全的方式连接到远程公司服务器。

与其他系统的互操作性:

- Windows 2000 SP2, 使用 PSK (预共享密钥) 或基于认证的授权 (X.509)
- SSH Sentinel V1.3
- 任何使用与 IPsec 相同协议的平台

协议:

- 密钥管理协议: IKE (Internet 密钥交换), 按 RFC 2409
- 授权协议: MD5 (RFC 2403) 或 SHA (RFC 2404)
- 加密学算法: 3DES
- 密钥交换算法: Diffie-Hellman, 组 2 和 3.

UL VPN 实现遵守下 RFC 中的规定:

- 2401 (用于 Internet 协议的安全体系结构)
- 2402 (IP 授权头)
- 2406 (IP 封装安全开销 - ESP)
- 2367 (PF_KEY 密钥管理 API, 版本 2)
- 2408 (Internet 安全协会和密钥管理协议 - ISAKMP)
- 2409 (Internet 密钥交换 - IKE)
- 2528 (Internet X.509 公共密钥基础设施)
- 2207 (用于 IPSEC 数据流的 RSVP 扩展)
- 2451 (ESP CBC-模式密码算法)
- 2230 (用于 DNS 的密钥交换授权记录)

5.2 SNMP

简单网络管理协议 (Simple Network Management Protocol, SNMP) 是一种广泛应用于 TCP/IP 和 IPX 网络的网络管理标准。

通过一个运行网络管理软件的中央计算机, SNMP 提供了一种管理网络主机 (如工作站或服务器、路由器、桥接器和集线器) 的方法。SNMP 通过使用分布体系结构的管理系统和代理来进行管理服务。

5.3 Quality of Service (QoS)

UnitedLinux 通过使用内置于 Linux 内核的功能强大的网络基础结构，充分的利用了其先进的包过滤特性（参见节 7.6）。

5.4 高级路由能力

Linux 拥有非常先进的路由能力，在其基本发布中即已支持大部分主要的路由协议。使用 UL，您可以基于下述方面实现路由：

- 源地址
- 服务
- 在某一特定流量的包上设置任意的“标志”
- MAC 地址
- 时间
- 包内容
- 用户 ID
- 负载均衡（例如，与 Internet 共享不同的链）

6 异种环境的互操作性

UL 可以与许多企业中常见的不同操作系统进行通讯和相互操作，包括 Microsoft Windows 家族操作系统，Novell NetWare 和绝大部分 UNIX 和类 UNIX 系统，它可以作为服务器，也可以作为客户。

6.1 Windows 网络

Windows 网络使用服务器消息块 (Server Message Block, SMB) 协议共享文件和打印机。(SMB 也被应用于 OS/2 LAN Manager, Digital 现为 Compaq, PATHWORKS, SCO VisionFS, Syntax TotalNET 等。)

通过 UL 对 SMB 的支持，系统可以在 Windows 网络中完成一系列的客户端和服务端任务，例如，为 Windows 共享和访问打印机，为 Windows 95/98、NT 和 2000 工作站授权域登录，给 NT 和 2000 工作站的域用户授予管理员权限，给 NT 和 2000 工作站按域策略文件实施策略，当用户登录到域时运行登录脚本，以及在服务器维持用户的本地配置。

6.2 Novell 网络

Netware 是一种网络操作系统，它提供一系列的分布网络服务，包括打印机和文件共享。UnitedLinux 可以访问 Novell 的目录、文件和打印机服务。在运行 Linux 应用的同时，允许与现存 NetWare 网络无缝地集成。(注：对某些服务的支持取决于 Netware 版本。)

6.3 UNIX 网络

UL 完全兼容所有标准 UNIX 网络服务和协议，例如，TCP/IP，Sun Microsystem 的网络文件系统 (Network File System, NFS) 和网络信息服务 (Network Information Service, NIS)，Berkeley Internet BIND 和 DNS，Berkeley 打印机假脱机系统的打印机共享，远程登录机制，无盘主机的远程启动等。

UL 标准应用还包括对 LDAP 和 Kerberos 的支持，它提供一种可管理的安全环境。NIS 也可用于支持继承安装。

6.4 认证互操作性

Linux 拥有非常灵活的认证机制，它将在节 7.1 作更详细的介绍。作为一个客户，UL 可以针对下述方面进行认证并从中获取用户信息：

- Windows NT 服务器
- Windows 2000 服务器，使用 LDAP 或 Kerberos 5
- 其它使用 NIS 的 Unix
- 类属 LDAPv3 服务器 (支持 RFC2037 或 MSFU (用于 UNIX 的 Microsoft 服务)，如 Novell 的 NDS)

- Novell NDS (使用 LDAP)
- Netware 4 (仅认证, 无用户信息)

UL 也可以为下述客户端用作认证服务器:

- Kerberos 5 客户
- Windows NT 机器
- Windows 95/98 机器
- 通过使用 RFC2307 方案 (如 Linux 本身), 针对 LDA Pv3 服务进行客户认证, 并从中获取用户信息数据。
- Netware 3 客户
- NIS 客户

7 安全

7.1 认证灵活性

Linux 对认证方法从来就不陌生。在其基本的版本中，Linux 服务器就提供对许多不同的服务进行认证。

支持的认证方法如表 6 所示。

7.2 用户信息数据

用户信息是一种额外的数据，它代表了用户的属性。例如，home 目录，登录 shell 程序，UID，GID，所属的组等。此信息通常存储于本地机器的普通文件中，但是通过配置系统库，也可以从不同的位置获取这些数据，例如：

- OpenLDAP
- 二进制本地文件（更快）
- NIS
- Windows NT
- Windows 2000 的有效目录
- Novell 的 NDS

此外，通过单独配置一些应用程序，也将这些信息存储于其它地方，使得其不依赖于系统库和全局配置。

7.3 加密支持

- 用于生成 VPN 的 IPSEC，或作为宿主安全通讯的主机（有关 IPSEC 的实现细节，参见节 5.1）
- 可加载的安全模块
- 允许 SSL 用于多个协议和应用：IMAP，POP3，SMTP，LDAP，HTTP
- 加密文件系统支持
- 强大的加密支持（128 位或更高对称加密，和 1024 位或更高非对称加密）
- 支持的算法：3DES, CAST5, blow_sh, AES, AES192, AES256, two_sh, RSA, RSA-E, RSA-S, ELG-E, DSA, ELG, RC2, RC4
- 支持的协议和加密适用于：SSLv2, SSLv3, TLSv1

方法	支持	说明
PAM	Kerberos 5 OpenLDAP Windows NT Netware 4 NDS Windows 2000, 通过AD MySQL 其它	PAM非常普遍：所有需要使用新认证方法的应用都采用PAM模块，它对应用是透明的。
Kerberos 5	Windows 2000, 通过Kerberos MIT Kerberos 其它Kerberos 5实现	认证-数据字段仅在最近公开，到目前为止，还没有被非MS应用使用。注：当用于非MS客户时，Windows 2000仅支持DES加密。
SASL	GSS-API (Kerberos 5) CRAM-MD5 DIGEST-MD5 PLAIN和LOGIN ANONYMOUS	实际上，SASL具有许多不同的认证机制。目前主要用于email服务器（IMAP, POP3和SMTP）和LDAP（OpenLDAP 使用SASL）。 注：这两种为明文方法
智能卡		
X.509	IPSec HTTP (基于web)认证授权	在安全网关之间基于VPN认证
SASL2: 与SASL相同, 加上:	OTP (单次口令) SRP (安全远程口令) SASLDB	SASL2正处于开发阶段 Database (磁盘二进制文件)

表6：UL的认证方法

7.4 一般特性

- 缺省没有启动的服务
- 按最小特权原则运行多个服务，root 帐户仅在的确需要的地方和时候使用。

7.5 易于软件升级

- 所有软件均数字签名
- 用于安全通告的邮件清单
- 软件升级程序自动获取安装程序的最新版本

7.6 防火墙

表 7 给出了 UL 的一些防火墙特性。正如在本文档的其它部分（主要是节 5.3）所介绍的那样，所有这些特性都可以进行组合并集成，以完成一些特定的任务。

特性	细节
SPF (状态包过滤)	防火墙跟踪连接，知道某一包是否属于一个新连接或者是一个现存连接的一部分。它对不是面向连接的协议也有效，如 ICMP 和 UDP。 一般来讲，SPF 允许管理员生成简单的规则，例如，“仅是我所要求的、且响应某某条件的包才可以进入此网络”。
特定应用支持	它包括如 FTP，IRC (带 DCC)，Netmeeting 等模块。这些模块允许相应的协议通过防火墙使用。
完全 NAT	完全支持 NAT，包括源 NAT (源地址被翻译) 和目标 NAT (目标地址被翻译)，在任何配置下，两者都有一个或多外 IP 地址。
包标记	可以对包进行标记，与 QoS 或其它特定的高级路由一起使用。

表 7：UnitedLinux 防火墙能力

7.7 网络侵入检测

表 8 给出了 UnitedLinux IDS 能力介绍。

特性	细节
基于签名	对于缺省安装，其签名数据库包括数以千计的安全事件
多平台	检测器不仅仅工作于多平台，它同时还包括大量平台和应用的安全事件签名。
完全 TCP 流再装配	通过对 TCP 流进行重新装配，可以避免 NIDS 的检测攻击。这样，检测器在与签名数据库比较之前，可以“看见”完整的数据流。
应用级解码	在将数据流传送到检测引擎之前，检测器对数据流进行规整。因此，可以避免绕过NIDS的攻击，例如，采用十六进制代替ASCII编码URL（如GET %2E%2E 实际上是GET..）
IP 碎片整理支持	检测某种类型的攻击，如避免碎片IP包被NIDS检测。
端口扫描检测	通过特定的签名（例如，对NMAP通用扫描程序），或通过行为。
多个输出插件	可以发送警报数据到一个SQL数据库、文本文件、tcp-转储二进制文件或到syslog精灵。支持的数据库包括MySQL, PostgreSQL, MSSQL和Oracle。同时也支持UnixODBC。
SNMP 陷阱	发送SNMP陷阱用于报警
报警分类	报警可以按类型和重要性、相关性和紧急性进行分类
多检测器支持	可以部署和配置多个检测器，以报告到一个中央数据库
即时生成多个有用的报告	当登录到一个SQL数据库时，可以实时生成多份报告，生成的报警包括从一些统计数据到流量的实际内容
方便灵活的签名描述语言	允许管理器快速有效地生成自己的攻击签名
广泛支持	Security Focus的ARIS，CERT的AIR CERT，Arachnids。有关这类网络脆弱性方面的典型安全报警已经通过Snort签名实现。

表 8 UL 的网络入侵检测要点

8 开发环境

UL 提供用于 ISV 的最小开发环境。它包括所有编译器，允许 ISV 为 UL 建造应用程序库、源代码和工具。

它们包括：

- C (gcc)
- C++ (g++)
- Java
- Perl
- Python
- Ruby
- Tck/Tk
- diff
- patch
- make (GNU make)
- lex (flex)
- yacc (bison)
- GNU automake 和 autoconf
- GNU binutils
- libtool
- gdb

为了提供稳定的、可维护的 C++ 支持，UL 使用 GCC 3.1 作为其缺省的编译器，但同时也提供安装 GCC 2.95 的选项。所有相关的包（如 C++ 库）也提供两种版本。

9 中文化

Turbolinux Enterprise Server 8 powered by UnitedLinux 包含了目前最好的控制台中日韩字符显示方案 UNICON, 由于使用了内核级的显示方案, 和其他的外挂中文控制台软件相比, 它保持了非常好的终端兼容性, 甚至直接支持 gpm 鼠标接口。使您感觉不到中文控制台和西文控制台使用上的区别。对于大多数的程序, 不需要经过任何修改, 即可轻松处理多国文字, 进行正确的制表符识别, 鼠标操作, 屏幕回滚。

在中文执行标准方面, Turbolinux Enterprise Server 8 powered by UnitedLinux 完全符合 GB18030-2000 国家标准。可以支持显示 2 万 7 千多个汉字。中文输入法使用了最新开发的 SCIM, 和系统紧密集成, 而且具备良好的可扩展性。

SCIM 是一个通用的输入法平台。由于采用完全模块化设计, SCIM 具有非常灵活的结构和良好的可扩展性。SCIM 由核心库、前端模块、输入法服务器模块、配置文件读写模块等部分组成。目前可用的模块有: X11 前端模块、GConf 配置文件模块、simple 简单配置文件模块、rawcode 内码输入法模块、table 通用码表输入法模块以及拼音中文输入法模块。

10 结论

UnitedLinux 是一种结合了四种主要 Linux 厂商（SuSE, SCO, Conectiva 和 Turbolinux）优势的 Linux 产品。由于这些公司的共同努力，它在世界范围内得到更广泛的支持。基于其无与伦比的品质、可靠性、性能和价值，它是一种稳定可靠的 Linux 系统。

UnitedLinux 是一种得到业界广泛支持的企业级系统，它可以满足或超过大部分服务器业界标准。它保证最终用户的经过认证的应用和硬件可以可靠地工作，同时，在开发和认证方面，硬件和软件销售商也将受益于标准化的 Linux 平台。

11 更多信息

有关 Turbolinux Enterprise Server 8 powered by UnitedLinux 的更多信息，请访问 <http://www.turbolinux.com.cn>。

有关 UnitedLinux 的进一步信息，请访问 <http://www.unitedlinux.com>。