UNITEDLINUX

13th November 2002

Contents

Trademarks

1 Introduction

1.1 What is UnitedLinux?

Industry leaders Conectiva, SCO Group, SuSE and Turbolinux have formed a consortium to develop the high quality operating system called UnitedLinux.

Under terms of agreement, the four companies will streamline development efforts around one common version of Linux. Designed to be an enterprise-grade and industry standard Linux operating system, UnitedLinux provides a stable and uniform platform for application development, certification and deployment.

Being developed to unify rather than to fragment Linux offerings, UnitedLinux helps Linux vendors, ISVs, IHVs and OEMs to support a single, high value Linux offering, instead of many different versions. This focuses more resources on the advancement of Linux, thus creating a much higher quality, more functional product than could be developed otherwise.

UnitedLinux defines a common base (“UL base”) to be used as a foundation for all Linux offerings of the participating Linux vendors. Sharing the core system simplifies certification for OEMs and ISVs, who can certify against one platform instead of multiple distributions.

Participants can rebrand UnitedLinux with their own “look & feel” and value-added extensions. Therefore, UnitedLinux must clearly define what constitutes the UL base, which parts are vendor-added extensions and how they interact with this foundation. UnitedLinux shall also provide a “sample look & feel”.

1.2 Advantages of UnitedLinux

1.2.1 For the customer

- **Combined expertise of top Linux vendors**
  Working together, UL consortium members will provide customers with the result of their joint effort and combined expertise.

- **Stability**
  Built on top of a solid and tested foundation, UnitedLinux delivers an enterprise-class operating system with exceptional stability and reliability.

- **Quality Assurance**
  Tested by QA teams and certification labs worldwide, UnitedLinux brings unsurpassed quality levels to Open Source operating systems, previously available only from more expensive proprietary systems.

- **Certification**
  Being certified by major software and hardware vendors, UnitedLinux offers a per-

fect environment for applications and for complete compatibility with hardware platforms and peripherals.

- **Worldwide presence**
  UnitedLinux is commercially available on virtuallly all continents and can provide better support offerings and a worldwide presence of support representatives.

1.2.2 For the industry

- **Fewer distributions to certify**
  Linux distributions powered by UnitedLinux share a common system core and a standard set of applications. Software and hardware certification can be performed only once and still be valid for all UnitedLinux-based distributions.

- **Certification**
  Easier to meet customers expectations on certified hardware and software, since UnitedLinux offers a perfect environment for applications and complete compatibility with hardware platforms and peripherals.

- **Standards compliance**
  UnitedLinux is compliant with current industry and Internet standards in both runtime and development environments. In cases where there is no standard, the "de facto" common practice is followed.

- **Worldwide presence**
  Since UnitedLinux is commercially available on virtually all continents, it can provide better support offerings and a worldwide presence of support representatives.

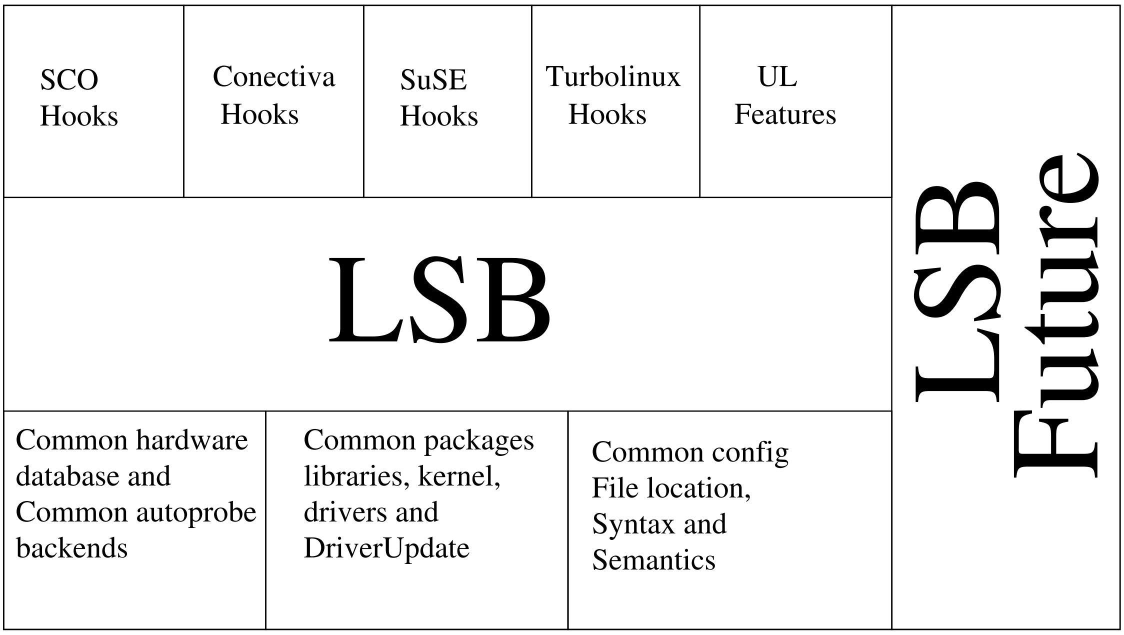
1.3 Document scope and organization

This document details the UnitedLinux base system and standardized features. Section 1 presents a brief introduction of UnitedLinux and its benefits for the customer and the industry. Section 2 contains an architecture overview, the standards followed by UnitedLinux and the enterprise features it offers. High availability and scalability features of UL are covered in Section 3. Section 4 introduces supported file systems and describes limits of the main file systems available, including journaling file systems. UL networking capabilities and main features are described in Section 5. Interoperability between UL and other operating systems is described in Section 6.

Two topics of major concern to UnitedLinux customers are also discussed in this document, security in Section 7 and development in Section 8.

2 Overview

2.1 Architecture


SCO Hooks
Conectiva Hooks
SuSE Hooks
Turbolinux Hooks
UL Features
LSB
LSB Future
Common hardware database and Common autoprobe backends
Common packages libraries, kernel, drivers and DriverUpdate
Common config File location, Syntax and Semantics

2.2 Supported platforms

UnitedLinux will initially be available for the following platforms: x86 32-bit, IA64, x86-64 and IBM z, i and pSeries.

2.3 Compliance with standards

UL adheres to current and emerging Linux and industry standards, allowing ISVs to develop software that is portable across similar Linux bases. The following is a list of relevant standards:

- **FHS**
  The Filesystem Hierarchy Standard (FHS) consists of a set of requirements and guidelines for file and directory placement under UNIX-like operating systems.
- **LSB**
  (see Section 2.3.1)
- **OpenI18N**
  (see Section 2.3.2)
- **GB18030**
  UnitedLinux offers GB18030 compliant Chinese fonts for input, output and print.

> GB18030 specifies a mapping table that covers all Unicode code points and maintains compatibility of GB-encoded text with GBK and GB2312.

In cases where no standard has been defined yet, but a “de facto” common practice exists, the common practice will be followed. If the common practice is not suitable for the focus of UnitedLinux, then the Linux vendors should agree on a new “de facto” standard.

Where possible, compatibility modes or migration tools for non-UL systems should be provided.

2.3.1 Linux Standard Base

The goal of the Linux Standard Base (LSB) is to develop and promote a set of standards that will increase compatibility among Linux distributions and enable software applications to run on any compliant Linux system. In addition, the LSB will help coordinate efforts to recruit software vendors to port and write products for Linux.

2.3.2 Localization and Internationalization — L10N and I18N

All UL software is in accordance with internationalization standards, as available at `http://www.li18nux.org/`.

The OpenI18N2000 specification includes the best of globalization functionality that commercial UNIX systems have successfully implemented and compliments this functionality with extensions that will make Linux internationalization comprehensive for all national and local requirements. By conforming to the OpenI18N2000 specification, “Powered by UnitedLinux” products will benefit from UNICODE-based, multi-lingual capabilities in a portable manner, with this support available to all UnitedLinux customers.

Among the supporters of OpenI18N are Compaq Computer, Conectiva Linux, Digital Factory and Kondara Project, Fujitsu Limited, Hitachi, Ltd., IBM Corporation, Japan PPC Linux Users Group (JPLUG), NEC Corporation, Red Hat, Inc., SGI, SuSE Linux AG. and Turbolinux, Inc.

About OpenI18N

OpenI18N is a project under the Free Standards Group. The members of the project consist of Linux and Open Source related contributors who are working on globalization, a combination of internationalization and localization. The project was formed in August 1999 with the ultimate goal to achieve software/application portability and interoperability in the International context for Linux and other open source projects. Its activities are focused on the internationalization of a core set of APIs and components of Linux distributions, in order to achieve a common Linux environment.

2.4 Enterprise features

UnitedLinux offers support for a number of standard and emerging hardware and software technologies, briefly summarized in the following list:

- **Automated installation**
  The UnitedLinux installer is able to read all of its options from an XML file, so that automated installations are possible. It can also convert KickStart's configuration files to UL's XML format.

- **Installation methods**
  UL can be installed from any of the following sources:

  - local CDROM
  - NFS-mounted directory
  - local hard disk partition

- **High Availability**
  see Section 3.2

- **Journaling file systems**
  see Section 4.2

- **LVM**
  see Section 4.4.

- **NGPT**
  The Next Generation POSIX Threads is a derivative of the GNU Pthreads and achieves near full POSIX compliance. It will add MxN threading capability and improve significantly on the POSIX compliance of pthreads on Linux. This will allow significant performance improvements for all applications that make use of the pthreads library, particularly on SMP machines. It will also enable Linux to provide threading services that are more in line with the capabilities of commercial UNIX operating systems, such as IBM AIX and SGI IRIX.

- **MXT**
  Memory eXpansion Technology (MXT) is a hardware technology for compressing main memory contents. MXT effectively doubles the amount of memory. MXT is transparent to CPU, I/O devices, application software and device drivers. No software changes are needed.

- **POSIX Asynchronous I/O**
  The asynchronous I/O (AIO) facility implements interfaces defined by the POSIX standard. With split-phase I/O, the initiating request (such as an aio_read) truly queues the I/O at the device as the first phase of the I/O request; a second phase of the I/O request, performed as part of the I/O completion, propagates results of

the request. The results may include the contents of the I/O buffer on a read, the number of bytes read or written, and any error status.

- **Raw I/O**
  Raw I/O enhancements provide high-bandwidth, low-overhead SCSI disk I/O capabilities by transferring data directly to a buffer in the application address space, bypassing the kernel buffers and I/O queueing code for SCSI and FibreChannel devices.

- **Direct I/O**
  Direct I/O moves data directly between the userspace buffer and the device performing the I/O, without copying through kernel space. It improves overall performance by avoiding expensive copy operations and bypassing the operating system's page cache.

- **Hyper-Threading**
  Hyper-Threading enables multi-threaded server software applications to execute threads in parallel within each individual server processor, thereby dramatically improving transaction rates, response times, and other characteristics of enterprise and e-Business software.

- **SNMP**
  Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions (see Section 5.2).

- **Large memory support**
  The Linux kernel is ordinarily limited to 1 GB of physical memory on the x86 32-bit platform, with 4 GB of virtual addressing space. With large memory support, Linux can take advantage of the Intel Physical Address Extension to support up to 64 GB of physical RAM and the full 4 GB of virtual addressing space per process. In addition, with AMD x86-64, Linux can enable highly efficient flat 64-bit memory addressibility for enterprise systems.

- **IPv6**
  IPv6 is short for "Internet Protocol Version 6," the next generation protocol designed by the IETF to replace the current version Internet Protocol, IPv4. IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses, adding many improvements to IPv4 in areas such as routing and network autoconfiguration.

- **Directory Services**
  Using the latest available protocol for LDAP, LDAPv3, UL offers a better way to manage large user bases and a better integration with applications such as mail servers, authentication servers, etc.

2.5 Essential core components

A Linux system based on UL is built on top of the following core components:

- LSB 1.2 runtime environment (all libs, all commands, all interfaces)
- glibc $\geq$ 2.2.5
- Standard Linux and UNIX shells: bash, csh, ksh
- textutils
- fileutils
- sh-utils
- sharutils
- util-linux
- SysVinit
- vixie-cron
- Remote shell tools: ssh, scp
- Networking tools (ping, traceroute, nslookup)
- IPv6 (basic tools like ifconfig/route and config location)
- Firewalling tools (ipchains, iptables, masquerading)
- Scripting languages: python, perl, PHP, TCL/TK, ruby
- Java runtime
- XFree86 $\geq$ 4.2 (libs and server)
- X print service (libXp.so.6)
- Free fonts for wide character support
- Free input methods for wide character support
- KDE 3.0 libraries
- GNOME 2.0 libraries
- High availability
- Postgresql

- SNMP
- CUPS
- I18n (pt_BR, es, XFree deadkeys patch)
- Hardware monitoring tools (lmsensors, etc)
- Remote boot (TFTP, PXE, etc)

2.6 Essential functionality

2.6.1 Servers, Services and Applications

- Web server (basic functionality)
  - Apache web server
  - Apache extension modules
  - PHP
  - PHP Extensions
  - Tomcat
- File and Print
  - Windows (Samba $\geq$ 2.2.4)
  - Mac (netatalk)
  - UNIX (CUPS printing system with LPR symlinks, NFS server)
- Name server and internet/intranet connection server
  - DNS (bind)
  - WINS (Samba)
  - DHCP server and client
  - FTP
  - TFTP
- Mail and news server
  - SMTP (sendmail)
  - POP
  - IMAP
- Proxy server

  - Squid
- SQL database server
  - basic functionality
  - appropriate standards based extension for heterogeneous OS access support (OBDC, JBDC)
- Authentication server (basic functionality)
  - OpenLDAP
  - Kerberos 5
  - PAM modules
  - NIS server
- Time server
  - NTP
- Text editors
  - vim
- Volume manager
  - LVM
- Acrobat Reader
- KDE 3.0 minimal system (kdebase and Konqueror)
- GNOME 2.0 minimal system
- Mozilla 1.0
- OpenLDAP 2.1

2.7 Documentation

UnitedLinux benefits from its development by geographically distant companies, consolidating its international expertise into documentation in several languages.

All localization filters back to the original authors and maintainers of the software documentation, making localization expertise available to everyone and also ensuring that future releases include additional and more complete translations.

3 Scalability and High Availability

3.1 Scalability

UnitedLinux comes with a complete set of software and tools to build server farms, enabling the system to manage workloads which would be otherwise unmanageable for a single machine.

This setup can benefit of all the UnitedLinux features, scaling across gigabit bandwidth and extend well beyond 64 available nodes in a server farm, giving more power and flexibility to your system.

3.2 High availability

High availability support in UnitedLinux leverages proven and stable technology from the Linux-HA project in a modular fashion. Powerful software packages are provided which cover major areas of HA clustering, from simple two-node failover clusters to load balancing server farms. This support is permanently guided by community standardisation efforts such as Open Clustering Framework and Service Availability Forum, in order to allow for seamless integration with other software and continuous tracking of the needs of the installed user base worldwide.

To prevent service downtime and increase the system dependability, UL offers tools for service monitoring, automatic failover, data mirroring and filesystem recovery.

4 File Systems

4.1 Ext2

The ext2 file system is the Linux native file system and shares many properties with traditional UNIX file systems. It has the concept of blocks, inodes, and directories. Ext2 is very robust and has excellent performance. Ext2 is also extensible in that it provides hooks to allow users to benefit from new features without reformatting their file system. Table 1 is a summary of the ext2 file system limits.

Maximum file size:	1TB
Maximum file limit:	limited only by file system size
Maximum partition/file system size:	4TB
Maximum filename length:	255 characters
Default minimum/maximum block size:	1024/4096 bytes
Default inode allocation:	1 for every 4096 bytes
Maximum mounts before a forced FS check:	20 (configurable)

Table 1: Ext2 Limits

4.2 Journaling File Systems

4.2.1 Ext3

The ext3 filesystem is a journaling extension to the standard ext2 filesystem on Linux. Journaling dramatically reduces filesystem crash recover time and is widely used in HA sites with shared disks. Ext3 is built on top of the ext2 filesystem, Table 2 shows the ext3 filesystem limits.

Maximum file size:	1TB
Maximum file limit:	limited only by file system size
Maximum partition/file system size:	4TB
Maximum filename length:	255 characters
Default minimum/maximum block size:	1024/4096 bytes
Default inode allocation:	1 for every 4096 bytes
Maximum mounts before a forced FS check:	20 (configurable)

Table 2: Ext3 Limits

4.2.2 ReiserFS

Reiser file system version 3.2.25 is an optional journaling file system whose benefits include better disk space utilization, better disk access performance, and faster crash recovery. Table 3 shows ReiserFS limits.

Maximum file size:	1 TB
Maximum file limit:	32k directories, 4.2 billion files
Maximum partition/file system size:	1TB
Maximum filename length:	255 characters

Table 3: ReiserFS Limits

4.2.3 JFS

The Journaled File System (JFS) is a full 64-bit file system. All of the appropriate file system structure fields are 64-bits in size. This allows JFS to support both large files and partitions. JFS was developed by IBM under the GPL license and is ported from its AIX systems.

JFS provides a log-based, byte-level file system that was developed for transaction-oriented, high performance systems. Scalable and robust, its advantage over non-journaled file systems is its quick restart capability. JFS can restore a file system to a consistent state in a matter of seconds or minutes.

While tailored primarily for the high throughput and reliability requirements of servers (from single processor systems to advanced multi-processor and clustered systems), JFS is also applicable to client configurations where performance and reliability are desired.

Table 4 lists JFS limits.

Minimum file system size:	16 MB
Maximum file size:	limited by the architecture
Maximum file limit:	limited by file system size
Default minimum/maximum block size:	512/4096 bytes
Default inode allocation:	Dynamic

Table 4: JFS Limits

4.3 Other File Systems

To ensure maximum compatibility with different media and to facilitate data exchange with foreign systems, a number of other file systems are also supported:

- ISO9660 (CDROM)
- UDF (DVD/packet mode CDRW)
- EFS (non-ISO9660 CDROM, IRIX < 5.3 XFS)
- CRAMFS (compressed ROM file system)
- ROMFS (small ROM file system)
- TMPFS (RAM disk file system)
- NTFS (Microsoft Windows NT)
- BFS (UnixWare. boot file system)
- SYSV (SCO/Xenix/Coherent)
- UFS (BSD and derivatives)
- FAT/VFAT (Microsoft DOS and Windows 9x)
- HFS (Macintosh)
- HPFS (OS/2)
- UMSDOS (UNIX-like FS for DOS disk images)
- QNX4
- Minix

4.4 LVM

The Logical Volume Manager, or LVM, is a subsystem for on-line disk storage management, which has become a "de-facto" standard for storage management across Linux implementations.

LVM supports enterprise level volume management of disk and disk subsystems by grouping arbitrary disks into volume groups. The total capacity of volume groups can be allocated to logical volumes, which are accessed as regular block devices.

Further, LVM provides logical separation of storage, the ability to move data from one physical device to another while on-line, and dynamic block device resizing. LVM also enables system administrators to upgrade systems, remove failing disks, reorganize workloads, and adapt to changing system needs, with a minimum amount of time and effort. Table 5 lists the limits of the LVM implementation used in UL.

Maximum Logical Volume size:	256 Gb using 4 Mb extents up to 1 Pb using larger PEs
Maximum number of Logical Volumes:	256
Maximum number of Volume Groups:	99
Maximum number of PEs per PV:	65534
Default Physical Extent size:	4Mb

Table 5: LVM Limits

5 Networking

5.1 VPN with IPSec

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. VPNs allow users working at home, on the road or at a branch office to connect in a secure fashion to a remote corporate server using the public Internet.

Interoperability:

- Windows 2000 SP2 using PSK (pre-shared key) or certificate-based authentication (X.509)
- SSH Sentinel V1.3
- Any platform which adheres to the same protocols used by this IPsec implementation

Protocols:

- Key management protocol: IKE (Internet Key Exchange), in accordance to RFC 2409
- Authentication protocol: MD5 (RFC 2403) or SHA (RFC 2404)
- Cryptography algorithm: 3DES
- Key exchange algorithm: Diffie-Hellman, groups 2 and 3.

UL VPN implementation adheres to the specified in the following RFCs:

- 2401 (Security Architecture for the Internet Protocol)
- 2402 (IP Authentication Header)
- 2406 (IP Encapsulating Security Payload - ESP)
- 2367 (PF_KEY Key Management API, Version 2)
- 2408 (Internet Security Association and Key Management Protocol - ISAKMP)
- 2409 (The Internet Key Exchange - IKE)
- 2528 (Internet X.509 Public Key Infrastructure)
- 2207 (RSVP Extensions for IPSEC Data Flows)
- 2451 (The ESP CBC-Mode Cipher Algorithms)
- 2230 (Key Exchange Delegation Record for the DNS)

5.2 SNMP

The Simple Network Management Protocol (SNMP) is a network management standard widely used in TCP/IP and in IPX networks.

SNMP provides a method of managing network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally-located computer running network management software. SNMP performs management services by using a distributed architecture of management systems and agents.

5.3 Quality of Service (QoS)

UnitedLinux uses the powerful networking infrastructure built into the Linux kernel, taking full advantage of its advanced packet filtering features (see Section 7.6)

5.4 Advanced routing capabilities

Linux has very advanced routing capabilities and supports most major routing protocols out of the box. With UL you can perform routing based on:

- source address
- service
- arbitrary "marks" set on a packet that belongs to a certain traffic
- MAC addresses
- time of day
- packet content
- user ID
- load balancing (e.g. sharing different links to the internet)

6 Interoperability in heterogeneous environment

UL communicates and interoperates with many different operating systems commonly found in the enterprise, including the Microsoft Windows family of operating systems, Novell NetWare and the majority of UNIX and UNIX-like systems, either as a server or as a client.

6.1 Windows networks

Windows networks use the Server Message Block (SMB) protocol to share files and printers. (SMB is also used by the OS/2 LAN Manager, Digital — now Compaq — PATHWORKS, SCO VisionFS, Syntax TotalNET, among others.)

UL's SMB support allows the system to perform a number of client and server tasks in a Windows network, such as: share and access files and printers to and from Windows systems, authenticate domain logons for Windows 95/98, NT and 2000 workstations, grant administrator privileges to particular domain users on NT and 2000 workstations, apply policies from a domain policy file to NT and 2000 workstations, run logon scripts when a user logs on to the domain and maintain a user's local profile on the server.

6.2 Novell networks

Netware is a network operating system providing a number of distributed network services, including printer and file sharing. UnitedLinux can access Novell's directory, file and printer services, allowing a seamless integration to existing NetWare-based networks, while still running Linux applications. (Note: support to certain services depends on the Netware version.)

6.3 UNIX networks

UL has total compatibility with all standard UNIX network services and protocols, such as TCP/IP, Sun Microsystem's Network File System (NFS) and Network Information Service (NIS), Berkeley Internet Name Domain (BIND) and Domain Name System (DNS), printer sharing through the Berkeley printer spooler, remote login mechanisms, remote booting for diskless hosts, etc.

UL standard applications come with LDAP and Kerberos support, providing a manageable and secure environment. NIS is also available to support legacy installations.

6.4 Interoperability regarding authentication

Linux has a very flexible authentication mechanism, which is explained in more detail in Section 7.1. UL, as a client, can authenticate against and obtain user information from:

- a Windows NT server
- a Windows 2000 server using LDAP or Kerberos 5
- other Unices using NIS
- a generic LDAPv3 server which supports the RFC2037 or MSFU (Microsoft Services for UNIX) schema, such as NDS from Novell
- Novell's NDS (using LDAP)
- Netware 4 (only authentication, not user information)

UL can also be used as an authentication server for:

- Kerberos 5 clients
- Windows NT machines
- Windows 95/98 machines
- clients that authenticate against an LDAPv3 server and fetch user information data from it using the RFC2307 schema (such as Linux itself, of course)
- Netware 3 clients
- NIS clients

7 Security

7.1 Authentication flexibility

Linux has never been a stranger to authentication methods. Right out of the box, a Linux server can be configured to authenticate using many different services.

Supported authentication methods are included in Table 6.

7.2 User information data

User information data is additional data that represents the user and his/her properties. Examples are: home directory, login shell, UID, GID, groups he/she belongs to, etc. This information is usually stored in flat files on the local machine, but the system libraries can be configured to fetch this data from different locations, such as:

- OpenLDAP
- binary local files instead of text files (faster)
- NIS
- Windows NT
- Windows 2000's Active Directory
- Novell's NDS

Additionally, some applications can be configured individually to store this information elsewhere, thus being independent from the system libraries and a global configuration.

7.3 Cryptography support

- IPSEC for creating VPNs or just a host to host secure communication (for more details on this specific implementation of IPSEC please check Section 5.1)
- loadable security modules
- SSL enabled for several protocols and applications: IMAP, POP3, SMTP, LDAP, HTTP
- encrypted file system support
- strong cryptography support (128 bits or higher for symmetric ciphers, and 1024 bits and higher for asymmetric ciphers)

Method	Supports	Comments
PAM	Kerberos 5 OpenLDAP Windows NT Netware 4 NDS Windows 2000 via AD MySQL	
	others	PAM is very generic: all that is needed for a new authentication method to be used by an application is a PAM module, this is transparent to the application
Kerberos 5	Windows 2000 via Kerberos	The authorization-data field was just recently disclosed, so far it has not been used by non-MS applications. Note: Windows 2000 only supports DES encryption when used with non-MS clients.
	MIT Kerberos Other Kerberos 5 implementations	
SASL	GSS-API (Kerberos 5)	SASL actually has many different authentication mechanisms. It is mainly used today with email servers (IMAP, POP3 and SMTP) and LDAP (OpenLDAP uses SASL).
	CRAM-MD5 DIGEST-MD5	
	PLAIN and LOGIN	Note: these two are clear text methods
	ANONYMOUS	
Smart card		
X.509	IPSec	Certificate-based VPN authentication between the secure gateways
	HTTP (web based) certificate authentication	
SASL2: same as SASL, plus:	OTP (One Time Passwords)	SASL2 is still in development stages
	SRP (Secure Remote Password)	
	SASLDB	Database (binary file on disk)

Table 6: UL's authentication methods

- supported algorithms: 3DES, CAST5, blowfish, AES, AES192, AES256, twofish, RSA, RSA-E, RSA-S, ELG-E, DSA, ELG, RC2, RC4
- supported protocols and cipher suits: SSLv2, SSLv3, TLSv1

7.4 Generic features

- services are not started by default
- several services run with the least privilege principle, the root account is only used when and where it is really needed

7.5 Easy software updates

- all software updates are digitally signed
- mailling lists for security announcements
- software updaters automatically fetch new versions of the installed programs

7.6 Firewalling

Table 7 shows some of UL's firewalling characteristics. As mentioned in other parts of this document (mainly in Section 5.3), all of these features can be combined and integrated to perform some specific task.

7.7 Network intrusion detection

Table 8 provides a summary of the UnitedLinux IDS capabilities.

8 Development environment

UL provides a minimal development environment for ISVs. This contains all the compilers, includes, libraries, sources and tools to enable ISVs to build applications for UL.

These include, among others:

- C (gcc)
- C++ (g++)
- Java

Feature	Details
SPF (Stateful Packet Filtering)	The firewall tracks connections and knows if a packet belongs to a new connection or is part of an already established one. This works even for protocols that are not connection-oriented, such as ICMP and UDP. Basically, SPF allows the administrator to create simple rules that say things like 'Only packets that are a response to something I asked for can enter this network'.
Specific application support	There are modules for FTP, IRC (with DCC), Netmeeting and others. These models allow such protocols to be used through the firewall.
Full NAT	Full NAT support, including source NAT (source addresses are translated) and destination NAT (destination addresses are translated), both with one or more IP addresses in any configuration.
Packet marking	Packets can be marked to be used, for example, with QoS or other specific advanced routing.

Table 7: UnitedLinux firewall capabilities

- Perl
- Python
- Ruby
- Tck/Tk
- diff
- patch
- make (GNU make)
- lex (flex)
- yacc (bison)
- GNU automake and autoconf
- GNU binutils
- libtool
- gdb

In order to provide stable and maintainable C++ support going forward, UL will use GCC 3.1 as the default compiler but will provide the option to install GCC 2.95 instead. All dependent packages (like C++ libraries) are provided in two versions.

Feature	Details
Signatures based	A default installation contains thousands of security incidents in its signature database
Multi-platform	Not only does the sensor work on multiple platforms, it also has signatures for security incidents for a variety of platforms and applications
Full TCP stream reassembly	Detects attacks that have been designed to avoid NIDS by doing a full TCP stream reassembly, thus making the sensor 'see' the complete data stream before comparing it to the signature database
Application level decoding	The sensor normalizes the data stream before passing it onto the detection engine, avoiding attacks designed to bypass a NIDS, such as encoding an URL in hexadecimal instead of ASCII (GET %2E%2E is actually GET ..)
IP defragmentation support	Detects certain type of attacks that fragment IP packets in order to avoid detection by NIDSs
Port scan detection	Via specific signatures (for example, for the NMAP popular scanner), or via behaviour.
Several output plugins	Alert data can be sent do a SQL database, text file, tcpdump binary file or to the syslog daemon. Supported databases include MySQL, PostgreSQL, MSSQL and Oracle. UnixODBC is also supported.
SNMP trap	Sends SNMP traps for the alerts
Alert classifications	Alerts can be classified by type and importance, relevance and urgency
Support for multiple sensors	Several sensors can be deployed and configured to report to a central database.
Several useful reports generated on the fly	When logging to a SQL database several reports can be generated in real time, ranging from just some statistics to the actual contents of the traffic that generated the alerts.
Easy and flexible signature description language	Allows the administrator to create his/her own attack signatures quickly and efficiently
Widely supported	ARIS from Security Focus, AIR CERT from CERT, Arachnids. Typically security alerts about some network vulnerability already come out with Snort signatures.

Table 8: UL's network intrusion detection highlights

9 Conclusion

UnitedLinux is a product that combines the unified expertise of four major Linux distributors: SuSE, SCO, Conectiva and Turbolinux. The result of the joint effort of these companies is a worldwide supported, solid and stable Linux system with unsurpassed quality, reliability, performance and value.

UnitedLinux is an industry-backed, enterprise-grade system that meets or exceeds most industry standards for servers. End users are assured that certified applications and hardware will work properly, while hardware and software vendors will benefit from a standardized Linux platform for development and certification.

10 More information

For further information on UnitedLinux, please refer to `http://www.unitedlinux.com`.