Release Notes for SUSE Linux Enterprise Desktop 11 Service Pack 3 (SP3)

Release Notes for SUSE Linux Enterprise Desktop 11 Service Pack 3 (SP3)

Version 11.3.17 (2013-05-27)

Abstract

These release notes are generic for all SUSE Linux Enterprise Desktop 11 based products. Some parts may not apply to particular architectures or products. Where this is not obvious, the respective architectures are listed explicitly.

An Installation Quick Start can be found in the `docu` directory on the media. Any documentation (if installed) can be found below `/usr/share/doc/` in the installed system.

Contents

1 Purpose

SUSE Linux Enterprise Desktop is the market's only enterprise-quality Linux desktop ready for routine business use. Developed and backed by SUSE, SUSE Linux Enterprise Desktop provides market-leading usability, seamless interoperability with existing IT systems, and dozens of essential applications—all at a fraction of the price of proprietary operating systems. It comes bundled with the latest versions of leading applications such as LibreOffice office productivity suite, Mozilla Firefox web browser, and Evolution email and calendar suite. In addition, it integrates with Microsoft SharePoint and Novell Teaming for group collaboration and supports a wide range of multimedia file formats, wireless and networking standards, and plug-and-play devices.

Through the latest enhancements in power management and security, SUSE Linux Enterprise Desktop also provides an environmentally friendly IT experience (Green IT) and an error-proof desktop. Finally, SUSE Linux Enterprise Desktop unparalleled flexibility. You can deploy it on a wide range of thick client devices (including desktops, notebooks, netbooks, and workstations), on thin client devices, or as a virtual desktop. By leveraging the power of SUSE Linux Enterprise Desktop, your business can dramatically reduce costs, improve end-user security and increase workforce productivity.

2 Important Upgrade Information

For users upgrading from a previous SUSE Linux Enterprise Desktop release it is recommended to review:

- Chapter 3, *Support Statement for SUSE Linux Enterprise Desktop*
- Section 6.1, “General Update Notes”
- Chapter 12, *Technical Information*

These Release Notes are identical across all architectures, and the most recent version is always available online at http://www.suse.com/releasenotes/.

3 Support Statement for SUSE Linux Enterprise Desktop

To receive support, see http://www.suse.com/products/desktop/.

3.1 Erasing All Registration Data

Sometimes you may want to remove all data that was created during the registration of a SUSE Linux Enterprise system, so you can cleanly re-register it with different credentials.

This can now be accomplished with `suse_register` by using the new option "--erase-local-regdata". Note that this does not free the subscription that the system may have consumed in the Customer Center. This needs to be done from the Customer Center's Web UI.

3.2 Software Requiring Specific Contracts

The following packages require additional support contracts to be obtained by the customer in order to receive full support:

3.2.1 Adobe Acrobat Update Cycles for Linux

Adobe has announced to change the Acrobat Reader update cycles for Linux to twice a year.

SUSE will adjust the frequence of security updates of Adobe Reader 9.x for Linux accordingly. It is recommended to switch to an alternate PDF viewer such as evince or okular, if possible. SUSE may in future releases discontinue Acrobat Reader due to Adobe's update policy.

4 Installation Related Notes

This section includes installation related information for this release.

4.1 Current Limitations in a UEFI Secure Boot Context

When booting in Secure Boot mode, the following restrictions apply:

- bootloader, kernel and kernel modules must be signed
- kexec and kdump are disabled
- hibernation (suspend on disk) is disabled
- access to `/dev/kmem` and `/dev/mem` is not possible, even as root user
- access to IO port is not possible, even as root user. All X11 graphical drivers must use a kernel driver
- PCI BAR access through sysfs is not possible
- 'custom_method' in ACPI is not available
- debugfs for "asus-wmi" module is not available
- 'acpi_rsdp' parameter doesn't have any effect on kernel

4.2 uEFI Secure Boot

SLES11-SP3 and SLED11-SP3 implement uEFI Secure Boot. Installation media supports Secure Boot. Secure Boot is only supported on new installations (not on upgraded systems from older SLES11 installations), if Secure Boot flag is enabled in the uEFI firmware at installation time.

For more informations, see Administration Guide, section Secure Boot.

4.3 Support for 4 KB/Sector Hard Disk Drives

Support for 4 KB/sector hard disk drives requires support from all code that directly accesses the hard disk drives.

SUSE Linux Enterprise fully supports 4 KB/sector drives in all conditions and architectures with one exception. The 4KB/sector hard disk drives are not supported as a boot drive on x86_64 systems booting with a legacy BIOS.

4.4 UEFI 2.3.1 Support

SP3 is supporting booting systems following UEFI specification up to version 2.3.1 errata C.

Note: Installating SLE 11 SP3 on Apple hardware is not supported.

4.5 Installation via USB

FATE 312662 RN missing

4.6 Mapping Network Interface Names to Names Written on the Chassis (biosdevname)

This feature addresses the issue that eth0 does not map to em1 (as labeled on server chassis), when a server has multiple network adapters.

This issue is solved for Dell hardware, which has the corresponding BIOS support, by renaming onboard network interfaces to em[1234], which maps to Embedded NIC[1234] as labeled on server chassis. (em stands for ethernet-on-motherboard.)

The renaming will be done by using the biosdevname utility.

biosdevname is automatically installed and used if YaST2 detects hardware suitable to be used with biosdevname. biosdevname can be disabled during installation by using "biosdevname=0" on the kernel commandline. The usage of biosdevname can be enforced on every hardware with "biosdevname=1". If the BIOS has no support, no network interface names are renamed.

4.7 CJK Languages Support in Text-mode Installation

CJK (Chinese, Japanese, and Korean) languages do not work properly during text-mode installation if the framebuffer is not used (Text Mode selected in boot loader).

There are three alternatives to resolve this issue:

1. Use English or some other non-CJK language for installation then switch to the CJK language later on a running system using YaST › System › Language.
2. Use your CJK language during installation, but do not choose Text Mode in the boot loader using F3 Video Mode. Select one of the other VGA modes instead. Select the CJK language of your choice using F2 Language, add **`textmode=1`** to the boot loader command-line and start the installation.

3. Use graphical installation (or install remotely via SSH or VNC).

4.8 Unable to Detect Display with Lid Closed

During the installation YaST resp. SaX2 tries to detect displays and determine the display size and resolution. If you are installing on a notebook with a closed lid it is not be possible to detect the display. To avoid this problem you must keep the lid open during installation.

If the detection fails, start YaST and click Hardware › Graphics Card and Monitor. Then configure the display manually.

4.9 Development Packages Moved to the SDK

As many development packages and sub-packages as possible have been moved to the SDK.

4.10 Installation Using Persistent Device Names

The installer uses persistent device names by default. If you plan to add storage devices to your system after the installation, we strongly recommend you use persistent device names for all storage devices.

To switch to persistent device names on a system that has already been installed, start the YaST2 partitioner. For each partition, select Edit and go to the FStab Options dialog. Any mount option except **`Device name`** provides you persistent device names. In addition, rerun the boot loader module in YaST to switch the bootloader to using the persistent device name. Start the module Boot Loader and select Finish to write the new proposed configuration to disk. This needs to be done before adding new storage devices.

For further information, visit http://en.opensuse.org/SDB:Persistant_storage_device_names.

4.11 MD Devices on Top of iSCSI Not Supported

iSCSI devices cannot be used for Linux Software RAID. Using MD devices on top of iSCSI triggers a cyclic dependency that leads to a system crash.

4.12 Using NetworkManager and DHCP

To make NetworkManager send the hostname to the DHCP server, create a new network profile (see the Administration Guide for more information). Modify this profile with GNOME Configuration Editor

(**gconf-editor**) and add the key `/system/networking/connections/$number/ipv4/dhcp-hostname` (replace "$number" with the actual number) with a string value. NetworkManager will send this value to the DHCP server. A special value `system-hostname` can be used to send the current hostname.

5 New Features

5.1 Desktop

- GNOME 2.28

  GNOME was updated to version 2.28 with SP1, only selected packages got an update for SP2 or SP3.

- KDE 4.3

  SUSE introduced KDE 4 with SUSE Linux Enterprise Desktop 11 as an innovative free software desktop and applications such as the Konqueror web browser, the Dolphin file manager, the Okular document reader, the System Settings control center and more.

  KDE was updated to 4.3.4 version with SP1.

  This new version of KDE is built on KDE Libraries which provide easy access to resources on the network by means of KIO and advanced visual capabilities through Qt4. Phonon and Solid. Customers migrating from SUSE Linux Enterprise Desktop 10 using KDE are getting a new user experience in version 11 Service Pack 1 and later. We recommend backing up your user home directory when upgrading from SUSE Linux Enterprise Desktop 10. (Partly based on http://www.kde.org/announcements/4.0/.)

- X.org 7.4

  The X server libraries were updated to version 1.6.5. The client libraries were kept the same, except for libgl.

5.1.1 FreeRDP Is Going to Replace rdesktop

In some scenarios, FreeRDP performs better than the rdesktop client, which is currently available as the Linux RDP client. Thus we add support for FreeRDP in SUSE Linux Enteprise Desktop 11 SP2. With the upcoming SP3, we will drop rdesktop in favor of FreeRDP.

5.1.2 The LibreOffice Suite replaces the OpenOffice.org Packages

OpenOffice.org has been replaced with LibreOffice with SP1. If you perform an upgrade, manual interaction is needed, otherwise you will stay with the old OpenOffice.org packages. Future updates will only

be prepared and published for LibreOffice. Some parts of the documentation packages still mention 'OpenOffice.org'.

5.2 Security

5.2.1 OpenSCAP Tools and Libraries Added

OpenSCAP is a set of open source libraries providing a path for integration of SCAP (Security Content Automation Protocol). SCAP is a collection of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information. For more information about SCAP, see http://nvd.nist.gov.

5.2.2 PAM Configuration

The common PAM configuration files (`/etc/pam.d/common-*`) are now created and managed with **`pam-config`**.

5.3 Network

5.3.1 Mapping Network Interface Names to Names Written on the Chassis (biosdevname)

This feature addresses the issue that eth0 does not map to em1 (as labeled on server chassis), when a server has multiple network adapters.

This issue is solved for Dell hardware, which has the corresponding BIOS support, by renaming onboard network interfaces to em[1234], which maps to Embedded NIC[1234] as labeled on server chassis. (em stands for ethernet-on-motherboard.)

The renaming will be done by using the biosdevname utility.

biosdevname is automatically installed and used if YaST2 detects hardware suitable to be used with biosdevname. biosdevname can be disabled during installation by using "biosdevname=0" on the kernel commandline. The usage of biosdevname can be enforced on every hardware with "biosdevname=1". If the BIOS has no support, no network interface names are renamed.

5.4 Server

5.4.1 Upgrading MySQL to Version 5.5

Replacing an unmaintained version of MySQL.

SLES11-SP3 introduces the upgrade of the MySQL database to version 5.5. This upgrade involves a change of the database format and the database needs to be converted before MySQL can run again. Therefore MySQL is not running directly after the upgrade.

To mgirate the MySQL database, run following commands as root:

```
touch -/var/lib/mysql/.force_upgrade
rcmysql restart
```

To verify failures during the server start check the log files under `/var/log/mysql/` .

We strongly recommend to back up the database before migrating it (mostly `/var/lib/mysql`).

5.5 Systems Management

- Improved Update Stack

  SUSE Linux Enterprise Desktop 11 comes with an improved update stack and the command line tool **`zypper`** to manage the install/update packages and repositories.

- Enhanced YaST Partitioner
- Extended Built-in Management Infrastructure

  CIM enablement with SFCB CIMON.

5.6 Kernel and Toolchain

- GCC 4.3.4
- glibc 2.11
- Linux kernel 3.0.10

5.6.1 USB3 Power Savings Features

USB3 Link Power Management and Latency Tolerance Messaging have been implemented for improved power efficiency.

5.7 Other Changes and Version Updates

- EVMS2 Replaced with LVM2
- Default Filesystem

  The default file system in new installations was changed from ReiserFS to ext3 with SUSE Linux Enterprise Desktop 11. A public statement can be found at http://www.suse.com/products/server/technical-information/#FileSystem.
- Samba 3.4.3
- UEFI Enablement on AMD64
- SWAP over NFS
- Python 2.6.0
- Perl 5.10
- Ruby 1.87

6 Update-Related Notes

This section includes update-related information for this release.

6.1 General Update Notes

6.1.1 Upgrading PostgreSQL Installations from 8.3 to 9.1.

To upgrade a PostgreSQL server installation from version 8.3 to 9.1, the database files need to be converted to the new version.

Newer versions of PostgreSQL come with the `pg_upgrade` tool that simplifies and speeds up the migration of a PostgreSQL installation to a new version. Formerly dump and restore was needed that was much slower.

`pg_upgrade` needs to have the server binaries of both versions available. To allow this, we had to change the way PostgreSQL is packaged as well as the naming of the packages, so that two or more versions of PostgreSQL can be installed in parallel.

Starting with version 9.1, PostgreSQL package names contain numbers indicating the major version. In PostgreSQL terms the major version consists of the first two components of the version number, i.e. 8.3, 8.4, 9.0, or 9.1. So, the packages for Postgresql 9.1 are named postgresql91, postgresql91-server, etc. Inside the packages the files were moved from their standard locations to a versioned location such as `/usr/lib/postgresql83/bin` or `/usr/lib/postgresql91/bin` to avoid file conflicts if packages are installed in parallel. The `update-alternatives` mechanism creates and maintains symbolic links that cause one version (by default the highest installed version) to re-appear in the standard locations. By default, database data are stored under `/var/lib/pgsql/data` on SUSE Linux.

The following preconditions have to be fulfilled before data migration can be started:

1. If not already done, the packages of the old PostgreSQL version must be upgraded to the new packaging scheme through a maintenance update. For SLE11 this means to install the patch that upgrades PostgreSQL from version 8.3.14 to 8.3.19 or higher.

2. The packages of the new PostgreSQL major version need to be installed. For SLE11 this means to install postgresql91-server and all the packages it depends on. As `pg_upgrade` is contained in postgresql91-contrib, that one has to be installed as well, at least until the migration is done.

3. Unless `pg_upgrade` is used in link mode, the server must have enough free disk space to temporarily hold a copy of the database files. If the database instance was installed in the default location, the needed space in megabytes can be determined by running the follwing command as root: "du -hs /

var/lib/pgsql/data". If space is tight, it might help to run the "VACUUM FULL" SQL command on each database in the instance to be migrated, but be aware that it might take very long.

Upstream documentation about `pg_upgrade` including step by step instructions for performing a database migration can be found under `file:///usr/share/doc/packages/postgresql91/html/pgupgrade.html` (if the postgresql91-docs package is installed), or online under http://www.postgresql.org/docs/9.1/static/pgupgrade.html . NOTE: The online documentation starts with explaining how you can install PostgreSQL from the upstream sources (which is not necessary on SLES) and also uses other directory names (`/usr/local` instead of the `update-alternatives` based path as described above).

For background information about the inner workings of `pg_admin` and a performance comparison with the old dump and restore method, see http://momjian.us/main/writings/pgsql/pg_upgrade.pdf .

6.1.2 Migrating to SLE 11 SP3 Using Zypper

To migrate the system to the Service Pack 3 level with **`zypper`**, proceed as follows:

- Open a root shell.
- Run **`zypper ref -s`** to refresh all services and repositories.
- Run **`zypper patch`** to install package management updates.
- Now it is possible to install all available updates for SLES/SLED 11 SP2; run **`zypper patch`** again.
- Now the installed products contain information about distribution upgrades and which migration products should be installed to perform the migration. Read the migration product information from `/etc/products.d/*.prod` and install them.
- Enter the following command:

  ```
  grep -'<product' -/etc/products.d/*.prod
  ```

  A sample output could be as follows:

  ```
  <product>sle-sdk-SP3-migration</product>
  <product>SUSE_SLED-SP3-migration</product>
  ```

- Install these migration products (example):

  ```
  zypper in --t product sle-sdk-SP3-migration SUSE_SLED-SP3-migration
  ```

- Run **`suse_register -d 2 -L /root/.suse_register.log`** to register the products in order to get the corresponding SP3 Update repositories.
- Run **`zypper ref -s`** to refresh services and repositores.

- Check the repositories using `zypper lr`. Disable SP1 and SP2 repositories after the registration and enable the new SP3 repositories (such as SP3-Pool, SP3-Updates):

```
zypper mr ---disable <repo-alias>
zypper mr ---enable <repo-alias>
```

  Also disable repositories you do not want to update from.

- Then perform a distribution upgrade by entering the following command:

```
zypper dup ---from SLES11-SP3-Pool ---from SLES11-SP3-Updates \
--from SLE11-SP2-WebYaST-1.3-Pool ---from SLE11-SP2-WebYaST-1.3-Updates
```

  Add more SP3 repositories here if needed, e.g. in case add-on products are installed. For WebYaST, it is actually `SLE11-SP2-*`, because there is one WebYaST release that runs on two SP code bases.

Note

If you make sure that only repositories, which you migrate from, are enabled, you can omit the `--from` parameters.

- zypper will report that it will delete the migration product and update the main products. Confirm the message to continue updating the RPM packages.
- To do a full update, run `zypper patch`.
- After the upgrade is finished, register the new products again:

```
suse_register --d 2 --L -/root/.suse_register.log
```

- Run `zypper patch` after re-registering. Some products donot use the update repositories during the migration and they are not active at this point of time.
- Reboot the system.

6.1.3 Online Migration from SP2 to SP3

Online migration from SP2 to SP3 is not supported, if debuginfo packages are installed.

6.1.4 Graphics Drivers Using KMS

Beginning with SLE11-SP1, we switched to use KMS (Kernel Mode Setting) for Intel graphics support. This means that mode setting is now done in kernel space instead of user space (X driver).

If—in rare cases—the new driver concept does not work for you, create an X.Org configuration manually:

1. Boot into failsafe mode without X (add "`3`" to the failsafe mode options) and run '**`sax2 -r -m 0=fbdev`**' to create an fbdev based `xorg.conf`.
2. Then disable KMS permanently by setting the `NO_KMS_IN_INITRD` sysconfig variable to "`yes`" and run **`mkinitrd`**.
3. Finally, reboot again (normal mode) to activate this new X.Org configuration.

6.1.5 Updating KDE

You can update your previous KDE installation (SUSE Linux Enterprise Desktop 11 or earlier) during system upgrade as described in the manual or as a package update using YaST or **`zypper`**. Because of a huge amount of package renaming, it is not possible to update your previous KDE installation using plain **`rpm`** commands.

For more information about KDE 4.3, see Section 5.1, “Desktop”.

6.1.6 GroupWise 8 Client

We ship the GroupWise 8 client with this release. If you want to keep the GroupWise 7 client, enter Software Manager and disable the GroupWise update.

The Groupwise 7 client is available in the `extras`-repository which can be enabled after registration.

6.1.7 Kernel Package Split in Subpackages

With SUSE Linux Enterprise Desktop11 the kernel RPMs are split into different parts:

- kernel-flavor-base

  Very reduced hardware support, intended to be used in virtual machine images.

- kernel-flavor

  Extends the base package; contains all supported kernel modules.

- kernel-flavor-extra

  All other kernel modules which may be useful but are not supported. This package will not be installed by default.

6.1.8 Displaying Manual Pages with the Same Name

The `man` command now asks which manual page the user wants to see if manual pages with the same name exist in different sections. The user is expected to type the section number to make this manual page visible.

If you want to get back the previous behavior, set `MAN_POSIXLY_CORRECT=1` in a shell initialization file such as `~/.bashrc`.

6.1.9 AppArmor

This release of SUSE Linux Enterprise Desktop ships with AppArmor. The AppArmor intrusion prevention framework builds a firewall around your applications by limiting the access to files, directories, and POSIX capabilities to the minimum required for normal operation. AppArmor protection can be enabled via the AppArmor control panel, located in YaST under Security and Users. For detailed information about using AppArmor, see the documentation in `/usr/share/doc/packages/apparmor-docs`.

The AppArmor profiles included with SUSE Linux have been developed with our best efforts to reproduce how most users use their software. The profiles provided work unmodified for many users, but some users find our profiles too restrictive for their environments.

If you discover that some of your applications do not function as you expected, you may need to use the AppArmor Update Profile Wizard in YaST (or use the aa-logprof(8) command line utility) to update your AppArmor profiles. Place all your profiles into learning mode with the following: **`aa-complain /etc/apparmor.d/*`**

When a program generates a high number of complaints, the system's performance is degraded. To mitigate this, we recommend periodically running the Update Profile Wizard (or aa-logprof(8)) to update your profiles, even if you choose to leave them in learning mode. This reduces the number of learning events logged to disk, which improves the performance of the system.

6.1.10 Fine-Tuning Firewall Settings

SuSEfirewall2 is enabled by default. That means that by default you cannot log in from remote systems. It also interferes with network browsing and multicast applications, such as SLP and Samba ("Network Neighborhood"). You can fine-tune the firewall settings using YaST.

6.2 Update from SUSE Linux Enterprise Desktop 11 SP 2

6.2.1 Augeas Framework Updated

The Augeas framework was updated to version 0.9.

6.2.2 Postfix: Incompatibility Issues and New Features

To benefit from enhancements and improvements which have been developed in the upstream community, postfix is upgraded from version 2.5.13 to the current version 2.9.4.

Incompatibility Issues:

- The default milter_protocol setting is increased from 2 to 6; this enables all available features up to and including Sendmail 8.14.0.
- When a mailbox file is not owned by its recipient, the local and virtual delivery agents now log a warning and defer delivery. Specify "strict_mailbox_ownership = no" to ignore such ownership discrepancies.
- The Postfix SMTP client(!) no longer tries to use the obsolete SSLv2 protocol by default, as this may prevent the use of modern SSL features. Lack of SSLv2 support should never be a problem, since SSLv3 was defined in 1996, and TLSv1 in 1999. You can undo the change by specifying empty `main.cf` values for smtp_tls_protocols and lmtp_tls_protocols.
- Postfix SMTP server replies for address verification have changed. unverified_recipient_reject_code and unverified_sender_reject_code now handle "5XX" rejects only. The "4XX" rejects are now controlled with unverified_sender_defer_code and unverified_recipient_defer_code.
- `postfix-script` , `postfix-files` and `post-install` are moved away from `/etc/postfix` to $daemon_directory.
- Postfix now adds (Resent-) From:, Date:, Message-ID: or To: headers only when clients match $local_header_rewrite_clients. Specify "always_add_missing_headers = yes" for backwards compatibility.
- The verify(8) service now uses a persistent cache by default (address_verify_map = btree: $data_directory/verify_cache). To disable, specify "address_verify_map ="
- The meaning of an empty filter next-hop destination has changed (for example, "content_filter = foo:" or "FILTER foo:"). Postfix now uses the recipient domain, instead of using $myhostname as in Postfix 2.6 and earlier. To restore the old behavior specify "default_filter_nexthop = $myhostname", or specify a non-empty next-hop content filter destination.
- Postfix now requests default delivery status notifications when adding a recipient with the Milter smfi_addrcpt action, instead of "never notify" as with Postfix automatically-added recipients.
- Postfix now reports a temporary delivery error when the result of virtual alias expansion would exceed the virtual_alias_recursion_limit or virtual_alias_expansion_limit.

- To avoid repeated delivery to mailing lists with pathological nested alias configurations, the `local(8)` delivery agent now keeps the owner-alias attribute of a parent alias, when delivering mail to a child alias that does not have its own owner alias.

- The Postfix SMTP client no longer appends the local domain when looking up a DNS name without ".". Specify "smtp_dns_resolver_options = res_defnames" to get the old behavior, which may produce unexpected results.

- The format of the "postfix/smtpd[pid]: queueid: client=host[addr]" logfile record has changed. When available, the before-filter client information and the before-filter queue ID are now appended to the end of the record.

- Postfix by default no longer adds a "To: undisclosed-recipients:;" header when no recipient specified in the message header. For backwards compatibility, specify: "undisclosed_recipients_header = To: undisclosed-recipients:;"

- The Postfix SMTP server now always re-computes the SASL mechanism list after successful completion of the STARTTLS command. Earlier versions only re-computed the mechanism list when the values of smtp_sasl_tls_security_options and smtp_sasl_security_options differ. This could produce incorrect results, because the Dovecot authentication server may change responses when the SMTP session is encrypted.

- The smtpd_starttls_timeout default value is now stress-dependent. By default, TLS negotiations must now complete under overload in 10s instead of 300s.

- Postfix no longer appends the system-supplied default CA certificates to the lists specified with *_tls_CAfile or with *_tls_CApath. This prevents third-party certificates from getting mail relay permission with the permit_tls_all_clientcerts feature. Unfortunately this change may cause compatibility problems when configurations rely on certificate verification for other purposes. Specify "tls_append_default_CA = yes" for backwards compatibility.

- The VSTREAM error flags are now split into separate read and write error flags. As a result of this change, all programs that use Postfix VSTREAMs MUST be recompiled.

- For consistency with the SMTP standard, the (client-side) smtp_line_length_limit default value was increased from 990 characters to 999 (i.e. 1000 characters including <CR><LF>). Specify "smtp_line_length_limit = 990" to restore historical Postfix behavior.

- To simplify integration with third-party applications, the Postfix sendmail command now always transforms all input lines ending in <CR><LF> into UNIX format (lines ending in <LF>). Specify "sendmail_fix_line_endings = strict" to restore historical Postfix behavior.

- To work around broken remote SMTP servers, the Postfix SMTP client by default no longer appends the "AUTH=<>" option to the MAIL FROM command. Specify "smtp_send_dummy_mail_auth = yes" to restore the old behavior.

- Instead of terminating immediately with a "fatal" message when a database file can't be opened, a Postfix daemon program now logs an "error" message, and continues execution with reduced functionality. Logfile-based alerting systems may need to be updated to look for "error" messages in addition to "fatal" messages. Specify "daemon_table_open_error_is_fatal = yes" to get the historical behavior (immediate termination with "fatal" message).

- Postfix now logs the result of successful TLS negotiation with TLS logging levels of 0.

- The default inet_protocols value is now "all" instead of "ipv4", meaning use both IPv4 and IPv6. To avoid an unexpected loss of performance for sites without global IPv6 connectivity, the commands "make upgrade" and "postfix upgrade-configuration" now append "inet_protocols = ipv4" to main.cf when no explicit inet_protocols setting is already present.

New Features:

- Support for managing multiple Postfix instances. Multi-instance support allows you to do the following and more: - Simplify post-queue content filter configuration by using separate Postfix instances before and after the filter. - Implement per-user content filters (or no filter) via transport map lookups instead of content_filter settings. - Test new configuration settings (on a different server IP address or TCP port) without disturbing production instances.

- check_reverse_client_hostname_access, to make access decisions based on the unverified client hostname.

- With "reject_tempfail_action = defer", the Postfix SMTP server immediately replies with a 4xx status after some temporary error.

- The Postfix SMTP server automatically hangs up after replying with "521". This makes overload handling more effective. See also RFC 1846 for prior art on this topic.

- Stress-dependent behavior is enabled by default. Under conditions of overload, smtpd_timeout is reduced from 300s to 10s, smtpd_hard_error_limit is reduced from 20 to 1, and smtpd_junk_command_limit is reduced from 100 to 1.

- Specify "tcp_windowsize = 65535" (or less) to work around routers with broken TCP window scaling implementations.

- New "lmtp_assume_final = yes" flag to send correct DSN "success" notifications when LMTP delivery is "final" as opposed to delivery into a content filter.

- The Postfix SMTP server's SASL authentication was re-structured. With "smtpd_tls_auth_only = yes", SASL support is now activated only after a successful TLS handshake. Earlier Postfix SMTP server versions could complain about unavailable SASL mechanisms during the plaintext phase of the SMTP protocol.

- Improved before-queue filter performance. With "smtpd_proxy_options = speed_adjust", the Postfix SMTP server receives the entire message before it connects to a before-queue content filter. This means you can run more SMTP server processes with the same number of running content filter processes, and thus, handle more mail. This feature is off by default until it is proven to create no new problems.

- sender_dependent_default_transport_maps, a per-sender override for default_transport.

- milter_header_checks: Support for header checks on Milter-generated message headers. This can be used, for example, to control mail flow with Milter-generated headers that carry indicators for badness or goodness. Currently, all header_checks features are implemented except PREPEND.

- Support to turn off the TLSv1.1 and TLSv1.2 protocols. Introduced with OpenSSL version 1.0.1, these are known to cause inter-operability problems with for example hotmail. The radical workaround is to temporarily turn off problematic protocols globally: smtp_tls_protocols = !SSLv2, !TLSv1.1, ! TLSv1.2 smtp_tls_mandatory_protocols = !SSLv2, !TLSv1.1, !TLSv1.2

- `Prototype postscreen(8)` server that runs a number of time-consuming checks in parallel for all incoming SMTP connections, before clients are allowed to talk to a real Postfix SMTP server. It detects clients that start talking too soon, or clients that appear on DNS blocklists, or clients that hang up without sending any command.

- Support for address patterns in DNS blacklist and whitelist lookup results.

- The Postfix SMTP server now supports DNS-based whitelisting with several safety features: permit_dnswl_client whitelists a client by IP address, and permit_rhswl_client whitelists a client by its hostname. These features use the same syntax as reject_rbl_client and reject_rhsbl_client, respectively. The main difference is that they return PERMIT instead of REJECT.

- The SMTP server now supports contact information that is appended to "reject" responses. This includes SMTP server responses that aren't logged to the maillog file, such as responses to syntax errors, or unsupported commands.

- tls_disable_workarounds parameter specifies a list or bit-mask of OpenSSL bug work-arounds to disable.

- The lower-level code in the TLS engine was simplified by removing an unnecessary layer of data copying. OpenSSL now writes directly to the network.

- enable_long_queue_ids Introduces support for non-repeating queue IDs (also used as queue file names). These names are encoded in a mix of upper case, lower case and decimal digit characters. Long queue IDs are disabled by default to avoid breaking tools that parse logfiles and that expect queue IDs with the smaller [A-F0-9] character set.

- memcache lookup and update support. This provides a way to share `postscreen(8)` or `verify(8)` caches between Postfix instances.

- Support for TLS public key fingerprint matching in the Postfix SMTP client (in smtp_tls_policy_maps) and server (in check_ccert access maps).

- Support for external SASL authentication via the XCLIENT command. This is used to accept SASL authentication from an SMTP proxy such as NGINX. This support works even without having to specify "smtpd_sasl_auth_enable = yes".

6.2.3 unixODBC Updated to Version 2.3.1

unixODBC 2.3.1 provides the most recent upstream fixes; this helps for seamless population of DB2 data using automated tools and improves interoperability with MS SQL server.

7 Driver Updates

7.1 X.Org: fbdev Used in UEFI Secure Boot Mode (ASpeed Chipset)

The unaccelerated fbdev driver is used as a fallback in UEFI secure boot mode with the ast KMS driver, EFI VGA, and other currently unknown frame buffer drivers.

7.2 X.Org Driver Used in UEFI Secure Boot Mode (Matrox)

The unaccelerated "mgag200"/"modesetting" (generic X.Org) driver combo is used instead of the "mga" X.Org driver if machine is running in UEFI secure boot mode. The driver does not load in other cases and a warning message is written into the kernel log.

7.3 Network Drivers

7.3.1 Emulex be2net Driver

Updating Ethernet Firmware

The Emulex Ethernet driver supports updating the firmware image in the UCNA flash through the request_firmware interface in Linux. You can perform this update when the UCNA is online and passing network/storage traffic.

To update the ethernet firmware image:

Copy the latest firmware image under the /lib/firmware directory:

```
cp be3flash.ufi -/lib/firmware
```

Start the update process:

```
ethtool --f eth<X> be3flash.ufi 0
```

Limitation in Bridging on Emulex 10Gb E Virtual Fabric Adapter with SR-IOV Enabled

PING is not working when attempting to bridge the ports of the Emulex 10Gb E Virtual Fabric adapter to the virtual machines when SR-IOV is enabled in the BIOS. This issue occurs due to limitations of the virtual Ethernet bridge in the adapter. Please reference the Emulex Release Notes for further information before enabling SR-IOV

7.3.2 Support for Intel Centrino Wireless Adapters

This Service Pack adds official support for the following Intel Centrino Wireless Adapters:

- Centrino Advanced-N 6235
- Centrino Wireless-N 2230
- Centrino Wireless-N 2200
- Centrino Wireless-N 135
- Centrino Wireless-N 105

7.4 Storage Drivers

7.5 Other Drivers

7.5.1 Updated Support for Intel Integrated Graphics

This Service Pack adds support for the 4th Generation Intel® Core™ Processor integrated graphics core.

8 Other Updates

8.1 openJDK 7 as a Replacement for openJDK 6

Because openJDK 6 will no longer get security fixes we need to perform the upgrade to openJDK 7.

The upgrade for openJDK 7 as a replacement for openJDK 6 introduces some incompatibilities. The most important changes are:

Some APIs in the sun.* packages have changed. These APIs are not intended to be used by developers. Developers importing from sun.* packages do so at their own risk. For more information, see Why Developers Should Not Write Programs That Call sun.* Packages (referenced in the Web resource below).

Other changes are documented at http://www.oracle.com/technetwork/java/javase/compatibility-417013.html.

8.2 Update of ICAClient

Citrix has released version 12 of the Citrix Server, which is incompatible with version 11. We have therefore updated the client to version 12.

8.3 Package python-ethtool

The Python bindings for ethtool were updated in SLE11 SP3 to version 0.7. This update introduced several stability bugfixes and support for handling IPv6.

8.4 Update Python to 2.6.8

Python 2.6.7 and 2.6.8 are security only updates to 2.6.6.

Python 2.6 helps with migrating to Python 3.0, which is a major redesign of the language. Whenever possible, Python 2.6 incorporates new features and syntax changes from 3.0 while remaining compatible with existing code. In case of conflict, Python 2.6 adds compatibility functions in a `future_builtins` module and a `-3` switch to warn about usages that will become unsupported in 3.0.

Some significant new packages have been added to the standard library, such as the multiprocessing and json modules.

9 Technology Previews

Technology Preview features are either not supported or supported in a limited fashion. These features are mainly included for customer convenience and be functionally incomplete, unstable or in other ways not suitable for production use.

9.1 eCryptfs Filesystem

The eCryptfs kernel modules and the ecryptfs-utils package shipped with SUSE Linux Enterprise Desktop 11 are a preview of a stacked cryptographic filesystem for Linux.

9.2 KVM

SUSE Linux Enterprise Desktop 11 contains KVM as an additional virtualization solution. It is not supported by SUSE, but is an area of interest for future development and deliveries.

9.3 Read-Only Root Filesystem

It is possible to run SUSE Linux Enterprise Desktop 11 on a read-only root filesystem. Due to the huge number of possible configurations, this is currently not a supported scenario.

The `/tmp` and `/var` directories need to be on a separate partition and cannot be mounted read-only.

After the installation has finished and all services are configured, login as *root* and do the following modifications:

Modify `/etc/fstab` and add "ro" to the mount options of the root filesystem entry.

```
rm -/etc/mtab
ln --s -/proc/mounts -/etc/mtab
mkdir -/var/lib/hwclock
mv -/etc/adjtime -/var/lib/hwclock
ln --s -/var/lib/hwclock/adjtime -/etc/adjtime
# the following two steps are only necessary if you use dhcp:
mv -/etc/resolv.conf -/var/lib/misc/
ln --s -/var/lib/misc/resolv.conf -/etc/resolv.conf
# Now mount root filesystem read-only and reboot
mount --o remount,ro -/
reboot
```

9.4 Linux Filesystem Capabilities

Our kernel is compiled with support for Linux Filesystem Capabilities. It is disabled by default. Enable it by adding `file_caps=1` as a kernel boot option.

10 Deprecated Functionality

10.1 X.Org: fbdev Used in UEFI Secure Boot Mode (ASpeed Chipset)

The unaccelerated fbdev driver is used as a fallback in UEFI secure boot mode with the ast KMS driver, EFI VGA, and other currently unknown frame buffer drivers.

10.2 X.Org Driver Used in UEFI Secure Boot Mode (Matrox)

The unaccelerated "mgag200"/"modesetting" (generic X.Org) driver combo is used instead of the "mga" X.Org driver if machine is running in UEFI secure boot mode. The driver does not load in other cases and a warning message is written into the kernel log.

10.3 Support for the JFS File System

In connection with the change in the JFS support status the corresponding kernel module has been moved to the extra kernel RPM (kernel-flavor-extra).

10.4 Deprecation of Package ncpfs

The package ncpfs is now deprecated and will be removed with SLED 11 SP4. The functionality provided by ncpfs is also provided by novell-qtgui-cli in combination with novell-novfsd.

10.5 Support for Portmap to End with SUSE Linux Enterprise 11 SP3

In SUSE Linux Enterprise we provide "rpcbind", which is compatible with portmap. "rpcbind" provides full IPv6 support. Thus portmap is now deprecated, and support for portmap will end end with the release of SUSE Linux Enterprise 11 SP3.

10.6 L3 Support for Openswan Is Scheduled to Expire

L3 support for Openswan is scheduled to expire. This decision is driven by the fact that Openswan development stalled substantially and there are no tangible signs that this will change in the future.

In contrast to this the strongSwan project is vivid and able to deliver a complete implementation of current standards. Compared to Openswan all relevant features are available by the package strongSwan plus strongSwan is the only complete Open Source implementation of the RFC 5996 IKEv2 standard whereas Openswan only implements a small mandatory subset. For now and the expected future only strongSwan qualifies to be an enterprise-ready solution for encrypted TCP/IP connectivity.

10.7 FreeRDP Is Going to Replace rdesktop

In some scenarios, FreeRDP performs better than the rdesktop client, which is currently available as the Linux RDP client. Thus we add support for FreeRDP in SUSE Linux Enteprise Desktop 11 SP2. With the upcoming SP3, we will drop rdesktop in favor of FreeRDP.

10.8 Removed Packages

The following list of current functionalities has been removed with this SUSE Linux Enterprise Desktop release.

- amor
- dante
- powertweak
- zmd

10.9 Deprecated Packages

The following packages are deprecated and will be removed with SUSE Linux Enterprise Desktop 12:

- **`lprng`**
- **`sendmail`**
- **`qt3`**

10.10 JFS File System

The JFS file system is no longer supported for new installations. The kernel file system driver is still available, but YaST does not offer partitioning with JFS.

11 Infrastructure, Package and Architecture Specific Information

11.1 Systems Management

11.1.1 Providing the URL of an Add-on Media at the Command Line during Installation

Add-on media like the Software Development Kit or third party driver media can be added to SUSE Linux Enterprise during installation or later in the running system. Sometimes it's advisable that an add-on media is available from the very beginning, for example to make drivers for new hardware available.

It is now possible to provide one or more URLs that point to the location of add-on media at the installer's command line by providing an "addon=url" parameter. Multiple add-ons need to be provided as a comma-separated list ("addon=url1,url2,...").

11.1.2 Snapper Enhancements

Snapper, which was introduced in previous service pack, has been implemented following enhancements:

- snapshots can be managed also by non-root users
- the performance of snapshots comparison has been improved
- snapper provides a D-Bus interface for better integration into other applications
- added support for LVM Thin Provisioning

For more information, see the Administration Guide.

11.2 Architecture Independent Information

11.2.1 Current Limitations in a UEFI Secure Boot Context

When booting in Secure Boot mode, the following restrictions apply:

- bootloader, kernel and kernel modules must be signed
- kexec and kdump are disabled
- hibernation (suspend on disk) is disabled
- access to `/dev/kmem` and `/dev/mem` is not possible, even as root user
- access to IO port is not possible, even as root user. All X11 graphical drivers must use a kernel driver
- PCI BAR access through sysfs is not possible
- 'custom_method' in ACPI is not available
- debugfs for "asus-wmi" module is not available
- 'acpi_rsdp' parameter doesn't have any effect on kernel

11.2.2 Change of libzypp History

The libzypp history in `/var/log/zypp/history` now contains a transaction ID added to each record. Any scripts, which parse the history file and which rely on the order of data fields, need to be checked that they still parse the history file properly.

11.2.3 Changes in Packaging and Delivery

11.2.3.1 Python Updated to Version 2.6.8 with "collections.OrderedDict" Functionality

The "OrderedDict" functionality ensures that Python dictionaries emitted for conversion into strings maintain their original order. This functionality is important for data analytics applications.

11.2.3.2 Postfix: Incompatibility Issues and New Features

To benefit from enhancements and improvements which have been developed in the upstream community, postfix is upgraded from version 2.5.13 to the current version 2.9.4.

Incompatibility Issues:

- The default milter_protocol setting is increased from 2 to 6; this enables all available features up to and including Sendmail 8.14.0.
- When a mailbox file is not owned by its recipient, the local and virtual delivery agents now log a warning and defer delivery. Specify "strict_mailbox_ownership = no" to ignore such ownership discrepancies.
- The Postfix SMTP client(!) no longer tries to use the obsolete SSLv2 protocol by default, as this may prevent the use of modern SSL features. Lack of SSLv2 support should never be a problem, since SSLv3 was defined in 1996, and TLSv1 in 1999. You can undo the change by specifying empty `main.cf` values for smtp_tls_protocols and lmtp_tls_protocols.
- Postfix SMTP server replies for address verification have changed. unverified_recipient_reject_code and unverified_sender_reject_code now handle "5XX" rejects only. The "4XX" rejects are now controlled with unverified_sender_defer_code and unverified_recipient_defer_code.
- `postfix-script` , `postfix-files` and `post-install` are moved away from `/etc/postfix` to $daemon_directory.
- Postfix now adds (Resent-) From:, Date:, Message-ID: or To: headers only when clients match $local_header_rewrite_clients. Specify "always_add_missing_headers = yes" for backwards compatibility.
- The verify(8) service now uses a persistent cache by default (address_verify_map = btree: $data_directory/verify_cache). To disable, specify "address_verify_map ="
- The meaning of an empty filter next-hop destination has changed (for example, "content_filter = foo:" or "FILTER foo:"). Postfix now uses the recipient domain, instead of using $myhostname as in Postfix 2.6 and earlier. To restore the old behavior specify "default_filter_nexthop = $myhostname", or specify a non-empty next-hop content filter destination.
- Postfix now requests default delivery status notifications when adding a recipient with the Milter smfi_addrcpt action, instead of "never notify" as with Postfix automatically-added recipients.
- Postfix now reports a temporary delivery error when the result of virtual alias expansion would exceed the virtual_alias_recursion_limit or virtual_alias_expansion_limit.
- To avoid repeated delivery to mailing lists with pathological nested alias configurations, the `local(8)` delivery agent now keeps the owner-alias attribute of a parent alias, when delivering mail to a child alias that does not have its own owner alias.
- The Postfix SMTP client no longer appends the local domain when looking up a DNS name without ".". Specify "smtp_dns_resolver_options = res_defnames" to get the old behavior, which may produce unexpected results.
- The format of the "postfix/smtpd[pid]: queueid: client=host[addr]" logfile record has changed. When available, the before-filter client information and the before-filter queue ID are now appended to the end of the record.
- Postfix by default no longer adds a "To: undisclosed-recipients:;" header when no recipient specified in the message header. For backwards compatibility, specify: "undisclosed_recipients_header = To: undisclosed-recipients:;"

- The Postfix SMTP server now always re-computes the SASL mechanism list after successful completion of the STARTTLS command. Earlier versions only re-computed the mechanism list when the values of smtp_sasl_tls_security_options and smtp_sasl_security_options differ. This could produce incorrect results, because the Dovecot authentication server may change responses when the SMTP session is encrypted.

- The smtpd_starttls_timeout default value is now stress-dependent. By default, TLS negotiations must now complete under overload in 10s instead of 300s.

- Postfix no longer appends the system-supplied default CA certificates to the lists specified with *_tls_CAfile or with *_tls_CApath. This prevents third-party certificates from getting mail relay permission with the permit_tls_all_clientcerts feature. Unfortunately this change may cause compatibility problems when configurations rely on certificate verification for other purposes. Specify "tls_append_default_CA = yes" for backwards compatibility.

- The VSTREAM error flags are now split into separate read and write error flags. As a result of this change, all programs that use Postfix VSTREAMs MUST be recompiled.

- For consistency with the SMTP standard, the (client-side) smtp_line_length_limit default value was increased from 990 characters to 999 (i.e. 1000 characters including <CR><LF>). Specify "smtp_line_length_limit = 990" to restore historical Postfix behavior.

- To simplify integration with third-party applications, the Postfix sendmail command now always transforms all input lines ending in <CR><LF> into UNIX format (lines ending in <LF>). Specify "sendmail_fix_line_endings = strict" to restore historical Postfix behavior.

- To work around broken remote SMTP servers, the Postfix SMTP client by default no longer appends the "AUTH=<>" option to the MAIL FROM command. Specify "smtp_send_dummy_mail_auth = yes" to restore the old behavior.

- Instead of terminating immediately with a "fatal" message when a database file can't be opened, a Postfix daemon program now logs an "error" message, and continues execution with reduced functionality. Logfile-based alerting systems may need to be updated to look for "error" messages in addition to "fatal" messages. Specify "daemon_table_open_error_is_fatal = yes" to get the historical behavior (immediate termination with "fatal" message).

- Postfix now logs the result of successful TLS negotiation with TLS logging levels of 0.

- The default inet_protocols value is now "all" instead of "ipv4", meaning use both IPv4 and IPv6. To avoid an unexpected loss of performance for sites without global IPv6 connectivity, the commands "make upgrade" and "postfix upgrade-configuration" now append "inet_protocols = ipv4" to main.cf when no explicit inet_protocols setting is already present.

New Features:

- Support for managing multiple Postfix instances. Multi-instance support allows you to do the following and more: - Simplify post-queue content filter configuration by using separate Postfix instances before and after the filter. - Implement per-user content filters (or no filter) via transport map lookups instead of content_filter settings. - Test new configuration settings (on a different server IP address or TCP port) without disturbing production instances.

- check_reverse_client_hostname_access, to make access decisions based on the unverified client hostname.
- With "reject_tempfail_action = defer", the Postfix SMTP server immediately replies with a 4xx status after some temporary error.
- The Postfix SMTP server automatically hangs up after replying with "521". This makes overload handling more effective. See also RFC 1846 for prior art on this topic.
- Stress-dependent behavior is enabled by default. Under conditions of overload, smtpd_timeout is reduced from 300s to 10s, smtpd_hard_error_limit is reduced from 20 to 1, and smtpd_junk_command_limit is reduced from 100 to 1.
- Specify "tcp_windowsize = 65535" (or less) to work around routers with broken TCP window scaling implementations.
- New "lmtp_assume_final = yes" flag to send correct DSN "success" notifications when LMTP delivery is "final" as opposed to delivery into a content filter.
- The Postfix SMTP server's SASL authentication was re-structured. With "smtpd_tls_auth_only = yes", SASL support is now activated only after a successful TLS handshake. Earlier Postfix SMTP server versions could complain about unavailable SASL mechanisms during the plaintext phase of the SMTP protocol.
- Improved before-queue filter performance. With "smtpd_proxy_options = speed_adjust", the Postfix SMTP server receives the entire message before it connects to a before-queue content filter. This means you can run more SMTP server processes with the same number of running content filter processes, and thus, handle more mail. This feature is off by default until it is proven to create no new problems.
- sender_dependent_default_transport_maps, a per-sender override for default_transport.
- milter_header_checks: Support for header checks on Milter-generated message headers. This can be used, for example, to control mail flow with Milter-generated headers that carry indicators for badness or goodness. Currently, all header_checks features are implemented except PREPEND.
- Support to turn off the TLSv1.1 and TLSv1.2 protocols. Introduced with OpenSSL version 1.0.1, these are known to cause inter-operability problems with for example hotmail. The radical workaround is to temporarily turn off problematic protocols globally: smtp_tls_protocols = !SSLv2, !TLSv1.1, ! TLSv1.2 smtp_tls_mandatory_protocols = !SSLv2, !TLSv1.1, !TLSv1.2
- `Prototype postscreen(8)` server that runs a number of time-consuming checks in parallel for all incoming SMTP connections, before clients are allowed to talk to a real Postfix SMTP server. It detects clients that start talking too soon, or clients that appear on DNS blocklists, or clients that hang up without sending any command.
- Support for address patterns in DNS blacklist and whitelist lookup results.
- The Postfix SMTP server now supports DNS-based whitelisting with several safety features: permit_dnswl_client whitelists a client by IP address, and permit_rhswl_client whitelists a client

by its hostname. These features use the same syntax as reject_rbl_client and reject_rhsbl_client, respectively. The main difference is that they return PERMIT instead of REJECT.

- The SMTP server now supports contact information that is appended to "reject" responses. This includes SMTP server responses that aren't logged to the maillog file, such as responses to syntax errors, or unsupported commands.
- tls_disable_workarounds parameter specifies a list or bit-mask of OpenSSL bug work-arounds to disable.
- The lower-level code in the TLS engine was simplified by removing an unnecessary layer of data copying. OpenSSL now writes directly to the network.
- enable_long_queue_ids Introduces support for non-repeating queue IDs (also used as queue file names). These names are encoded in a mix of upper case, lower case and decimal digit characters. Long queue IDs are disabled by default to avoid breaking tools that parse logfiles and that expect queue IDs with the smaller [A-F0-9] character set.
- memcache lookup and update support. This provides a way to share `postscreen(8)` or `verify(8)` caches between Postfix instances.
- Support for TLS public key fingerprint matching in the Postfix SMTP client (in smtp_tls_policy_maps) and server (in check_ccert access maps).
- Support for external SASL authentication via the XCLIENT command. This is used to accept SASL authentication from an SMTP proxy such as NGINX. This support works even without having to specify "smtpd_sasl_auth_enable = yes".

11.2.3.3 openJDK 7 as a Replacement for openJDK 6

Because openJDK 6 will no longer get security fixes we need to perform the upgrade to openJDK 7.

The upgrade for openJDK 7 as a replacement for openJDK 6 introduces some incompatibilities. The most important changes are:

Some APIs in the sun.* packages have changed. These APIs are not intended to be used by developers. Developers importing from sun.* packages do so at their own risk. For more information, see Why Developers Should Not Write Programs That Call sun.* Packages (referenced in the Web resource below).

Other changes are documented at http://www.oracle.com/technetwork/java/javase/compatibility-417013.html.

11.2.3.4 Ftrace Linux Kernel Internal Tracer Enablement

`trace-cmd` is now provided to make ftrace kernel facility accessible to SLE users. See `trace-cmd(1)` manual page and `/usr/src/linux/Documentation/trace/ftrace.txt` for more details.

11.2.4 Cross Architecture Information

11.2.4.1 Myricom 10-Gigabit Ethernet Driver and Firmware

SUSE Linux Enterprise 11 (x86, x86_64 and IA64) is using the Myri10GE driver from mainline Linux kernel. The driver requires a firmware file to be present, which is not being delivered with SUSE Linux Enterprise 11.

Download the required firmware at http://www.myricom.com.

11.3 AMD64/Intel64 64-Bit (x86_64) and Intel/AMD 32-Bit (x86) Specific Information

11.3.1 Virtualization

12 Technical Information

This section contains a number of technical changes and enhancements for the experienced user.

12.1 Kernel Limits

12.2 Xen Limits

12.2.1 XEN: Secure Boot

Xen hypervisor is shipped as an EFI application, and signed. It will negotiate with the shim loader to validate the Dom0 kernel signature before booting it. Enabling the alternative kernel image format takes as a prerequisite the bumping of the backward compatibility level from 3.2 to 4.X, so we are not able to boot a SLE11 SP3 PV guest on SLE10 SP4, even if secure boot is not enable.

12.3 File Systems

12.3.1 XFS Realtime Volumes

XFS Realtime Volumes is an experimental feature, available for testing and experimenting. If you encounter any issues, SUSE is interested in feedback. Please, submit a support request through the usual access methods.

12.3.2 ext4: Runtime Switch for Write Support

The SLE 11 SP3 kernel contains a fully supported ext4 file system module, which provides read-only access to the file system.

Read-write access to an ext4 file system can be acquired by setting the `rw` kernel module parameter to 1, either through module load time options or after module load through the kernel sysctl interface. Be aware that this action will render the kernel module and the kernel as the whole as unsupported upon first read-write mount of an ext4 file system.

ext4 is not supported for the installation of the SUSE Linux Enterprise operating system.

Since SUSE Linux Enterprise 11 SP2 we support offline migration from ext4 to the supported btrfs file system.

12.4 IPv6 Implementation and Compliance

SUSE Linux Enterprise Desktop 11 is compliant to IPv6 Logo Phase 2. However, when running the respective tests, you may see some tests failing. For various reasons, we cannot enable all the configuration options by default, which are necessary to pass all the tests.

12.4.1 IPv6 Support for NFSv3

Kernel configuration and NFS userland utilities have been updated to fully support NFSv3 over the IPv6 protocol. The same functionality for NFSv4 has already been enabled since SUSE Linux Enterprise 11 SP2.

12.4.2 IPv6 Support to AutoFS

AutoFS now mounts NFS volumes over IPv6.

12.5 Other Technical Information

- Locale Settings in `~/.i18n`

  If you are not satisfied with locale system defaults, change the settings in `~/.i18n`. Entries in `~/.i18n` override system defaults from `/etc/sysconfig/language`. Use the same variable names but without the `RC_` namespace prefixes. For example, use `LANG` instead of `RC_LANG`. For information about locales in general, see "Language and Country-Specific Settings" in the Administration Guide.

- Configuration of kdump

  The kernel is crashing or otherwise not behaving normally and a kernel core dump needs to be captured for analysis.

  A description on how to setup kdump can be found at http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3374462&sliceId=SAL_Public.

- Realtime Applications

  When running real-time applications on larger systems, lower maximum latencies can be achieved by employing the new `disable_buffer_lru` kernel command-line option. This disables the per-CPU LRU in the buffer cache, and may thus decrease overall filesystem performance.

- JPackage Standard for Java Packages

  Java packages are changed to follow the JPackage Standard (http://www.jpackage.org/). Read the documentation in `/usr/share/doc/packages/jpackage-utils/` for information.

- Loading Unsupported Kernel Drivers

  Every kernel module has a 'supported' flag. If this flag is not set, then loading this module will taint the kernel. Kernels which are tainted are not supported. To avoid this, unsupported Kernel modules are part of an extra RPM (kernel-<flavor>-extra). Since this would a problem for most desktops, the loading of those drivers is allowed by default.

  To prevent the loading of unsupported kernel drivers automatically during boot, change the line `allow_unsupported_modules 1` in `/etc/modprobe.d/unsupported-modules` to `allow_unsupported_modules 0`.

- Nonexecutable Stack

  Already introduced for SUSE Linux Enterprise Desktop 9 on the x86-64 (AMD64) architecture with 64-bit kernels, the Linux kernel in SUSE Linux Enterprise Desktop also supports nonexecutable stack (NX) on x86 for CPUs that support it (Intel Prescott and AMD64) with 32-bit kernels. For this to work, the kernel with PAE support, kernel-pae, must be installed. Go into YaST and install that kernel instead of your default kernel. For 64-bit kernels, all kernels support NX.

  The nonexecutable stack improves the security of your system. Many security vulnerabilities are stack overflows, where an attacker overwrites the stack of your program by feeding oversized data to the application that fails to properly check the length. Depending on the details of the program (with a nonexecutable stack), these vulnerabilities may either not be exploitable (and only crash the program, resulting in a Denial of Service) or at least be significantly harder to exploit.

  Some applications do require executable stacks. The compiler detects this during compilation and marks the binaries accordingly. The kernel enables an executable stack to allow them to work.

  To provide a higher level of security on x86-64, the user can pass `noexec=on` on the kernel command line. The kernel then uses a nonexecutable stack unconditionally and also marks the data section of a program as nonexecutable. This provides a higher protection level than just the nonexecutable stack, but potentially causes problems for some applications. SUSE has not found any problems during testing the most commonly used applications and services. Because it is not the default, this has not

been tested as extensively as the stack protection alone, so SUSE only recommends this setup for servers after the administrator has verified that all needed services continue to function properly.

12.5.1 Boot Device Larger Than 2 TiB

Due to limitations of the legacy x86 and x86_64 BIOS implementations booting from devices larger than 2 TiB is technically not possible using legacy partition tables (DOS MBR).

With SUSE Linux Enterprise Desktop 11 Service Pack 2 we support installation and boot using uEFI on the x86_64 architecture and certified hardware.

12.5.2 Better Sound Functionality with Pulseaudio 0.9.14 or Higher

For better sound functionality we strongly recommend that pulseaudio 0.9.14 or higher is installed. This version is available via maintenance channels for SUSE Linux Enterprise systems registered with SUSE.

12.5.3 netconfig Utility to Apply Additional Network Settings

The **`modify_resolvconf`** script is removed in favor of the more versatile **`netconfig`** script. This new script handles specific network settings from multiple sources more flexibly and transparently. For more information, see the updated manuals and the `netconfig` man-page.

12.5.4 Atheros Wireless Cards

Instead of the madwifi driver the ath5k/ath9k in-kernel replacement is now available. ath5k/ath9k does not support access point mode yet, but normal networks (infrastructure and ad-hoc) are well supported by the new driver.

12.5.5 Detecting Lenovo ThinkPad Laptops

Lenovo ThinkPad laptops have special code in the MBR (master boot record) because of the "Blue ThinkVantage button" functionality. If proper detection and preparation fails, it might be necessary to restore the boot sector.

If you have a ThinkPad, ensure that the bootloader is not installed into the MBR (verify it in the installation proposal!) and the MBR is not rewritten by generic code (in installation proposel select Bootloader -> Boot Loader Installation -> Boot Loader Options -> Write Generic Boot Code to MBR -- should be unchecked).

If your MBR gets rewritten, the ThinkVantage button will not work anymore. The back-up of the MBR is stored in `/var/lib/YaST2/backup_boot_sectors/`.

12.5.6 Stopping Cron Status Messages

To avoid the mail-flood caused by cron status messages, the default value of `SEND_MAIL_ON_NO_ERROR` in `/etc/sysconfig/cron` is now set to "`no`" for new installations. Even with this setting to "`no`", cron data output will still be send to the `MAILTO` address, as documented in the cron manpage.

In the update case it is recommended to set these values according to your needs.

13 Known Issues

13.1 Latest Release Notes

For the latest version of SUSE Linux Enterprise Desktop 11 SP3 Release Notes, see http://www.suse.com/releasenotes/i586/SUSE-SLED/11-SP3/.

13.2 Network Issues After Updating

If you were using a static IP with NetworkManager, you will lose this configuration while updating from SLED 10 SP4 to SLED 11. You must re-enter this information. The traditional networking method with `ifup` is not affected by this issue.

Name server lookup information of `resolv.conf` configured with the traditional networking method with ifup is missing after updating.

13.3 Kopete Lacks IRC Support

Kopete as shipped with KDE4 does not support the IRC protocol. Install and use xchat, if you want to participate in IRC messaging.

13.4 Hardware Related Issues

13.4.1 Limited Graphics Support on IBM SurePOS 700 4800-7X3 during Installation

There is only limited graphics support on IBM SurePOS 700 4800-7X3 systems with 4820-2GN monitors. During a graphical installation you can encounter an error message from the monitor (OSD = On Screen Display) such as:

```
OUT OF RANGE
H: --48.4 KHz V: --60.1 Hz.
```

To work around this issue try a different resolution, VESA or text-mode for installation. Another option is to choose the native driver by specifying `acceleratedx=1` on the boot prompt. It might also help to update the BIOS.

After system installation the problem no longer occurs and the graphics system is fully supported.

13.4.2 Graphical Distortions on the FIC GE2 Plattform (Transtec SENYO600)

On the FIC GE2 platform (when using 24 BPP color depth and resolutions >= 1280x1024 on the DVI interface) stripes are displayed on the X server. This distorts all windows.

Changing to 16 BPP color depth seems to solve this problem.

14 Documentation

For SUSE Linux Enterprise Desktop 11 documentation, see http://www.suse.com/documentation/sled11/, where you can download PDF documents. For installation with YaST software management or with zypper, packages are available on the installation media. Some of these packages are installed by default. These are the package names:

- `sled-installquick_en-pdf`: SLED 11 Installation Quick Start
- `sled-gnomequick_en-pdf`: SLED 11 GNOME Quick Start
- `sled-kdequick_en-pdf`: SLED 11 KDE Quick Start
- `sled-gnomeuser_en-pdf`: SLED 11 GNOME User Guide
- `sled-kdeuser_en-pdf`: SLED 11 KDE User Guide
- `sled-apps_en-pdf`: SLED 11 Application Guide
- `sled-admin_en-pdf`: SLED 11 Administration Guide
- `sled-deployment_en-pdf`: SLED 11 Deployment Guide
- `sled-security_en-pdf`: SLED 11 Security Guide
- `sle-apparmor-quick_en-pdf` : AppArmor 2.3.1 Quick Start
- `sle-audit-quick_en-pdf`: Linux Audit Quick Start
- `sled-xen_en-pdf`: SLED 11 Virtualization Guide
- `sled-tuning_en-pdf`: SLED 11 Tuning Guide
- `sled-manuals_en`: the set of all SLED books in HTML format

14.1 Application Guide: Firefox—Disabling Features

By default, Firefox does not honor settings made with the GConf system. In order to make the GConf lockdown keys effective, edit `/usr/lib/firefox/local-configuration.js` and set `config.use_system_prefs` to `true`. This file allows the administrator to set and lock preferences that will apply to every Firefox user.

15 More Information and Feedback

- Read the READMEs on the CDs.
- Get the detailed changelog information about a particular package from the RPM:

  ```
  rpm ---changelog --qp <FILENAME>.rpm
  ```

  <FILENAME>. is the name of the RPM.
- Check the `ChangeLog` file in the top level of CD1 for a chronological log of all changes made to the updated packages.
- Find more information in the `docu` directory of CD1 of the SUSE Linux Enterprise Desktop 11 CDs. This directory includes PDF versions of the SUSE Linux Enterprise Desktop 11 Installation Quick Start and Deployment Guides.
- http://www.suse.com/documentation/sled11/ contains additional or updated documentation for SUSE Linux Enterprise Desktop 11.
- Visit http://www.suse.com/products/ for the latest product news from SUSE and http://www.suse.com/download-linux/source-code.html for additional information on the source code of SUSE Linux Enterprise products.

16 Miscellaneous

17 Legal Notices

SUSE makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SUSE reserves the right to revise this publication and to make changes to its content, at any time, without the obligation to notify any person or entity of such revisions or changes.

Further, SUSE makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, SUSE reserves the right to make changes to any and all parts of SUSE software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classifications to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical/biological weaponry end uses. Please refer to http://www.novell.com/info/exports/ for more information on exporting SUSE software. SUSE assumes no responsibility for your failure to obtain any necessary export approvals.

SUSE has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and other countries.

For SUSE trademarks, see Novell Trademark ad Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html). All third-party trademarks are the property of their respective owners.