Make Your Linux More Secure

Marcus Kraft
SUSE

March 12th 2014
Session 14809

www.SHARE.org

Agenda

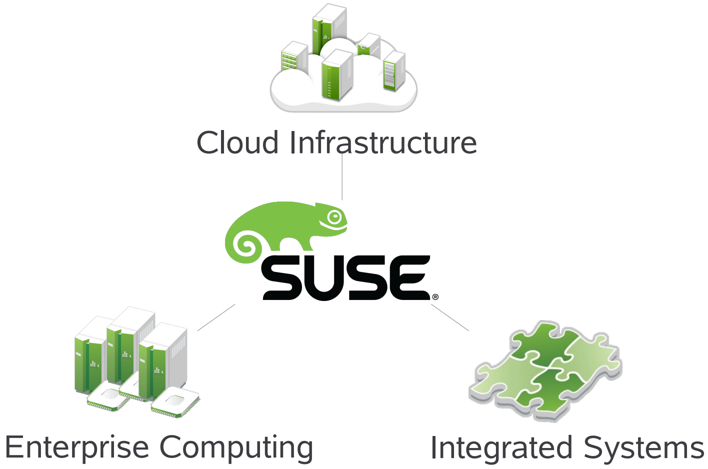
- SLES processes & certifications
  - SUSE intro
  - Certifications (CC/OSPP EAL 4+)
  - Collaboration (vendor SEC, etc) / IBM (development)
- SUSE tools
  - AppArmor Application Confinement
  - Advance Intrusion Detection Environemt (AIDE)
  - Data encryption (disk, volume, file system, file)
- Summary

SUSE

- **SUSE**, headquartered in Nürnberg / Germany, is an independently operating business unit of The Attachmate Group, Inc.

- The Attachmate Group is a privately held 1 billion+ $ revenue software company with four brands:

SUSE
Attachmate
Novell
NetIQ



SUSE Linux Enterprise Server

A highly reliable, scalable and secure
server operating system,
built to power
physical, virtual and cloud-based
mission-critical workloads.

Linux you can rely on—for years to come

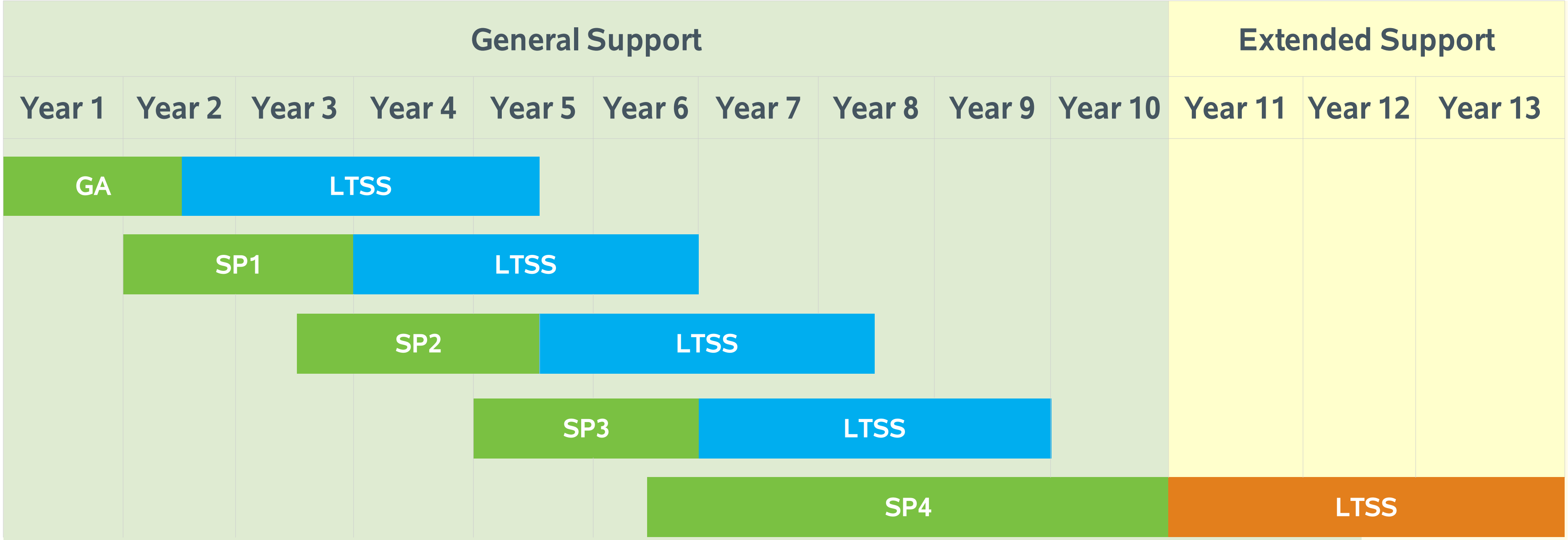
Run more mission-critical applications—physical, virtual and cloud

Processes & Certifications

SUSE® Linux Enterprise
Security and Certifications

- Certified to be compliant with the Common Criteria (CC) Controlled Access Protection Profile (CAPP) at Evaluation Assurance Level 4 with augmentations (EAL 4+) for the x86-64, POWER/ppc, and s390x architectures - from SUSE Linux Enterprise Server 10 Service Pack 1 onward.
- Common criteria certification in Evaluation Assurance Level 4 with augmentation according to the BSI OSPP (CC/OSPP EAL 4+) for SLES 11 SP2
- FIPS 140-2 certification for selected modules

SUSE® Linux Enterprise Server 12
Lifecyle Model



General Support

Extended Support

Year 1 Year 2 Year 3 Year 4 Year 5 Year 6 Year 7 Year 8 Year 9 Year 10 Year 11 Year 12 Year 13

GA LTSS

SP1 LTSS

SP2 LTSS

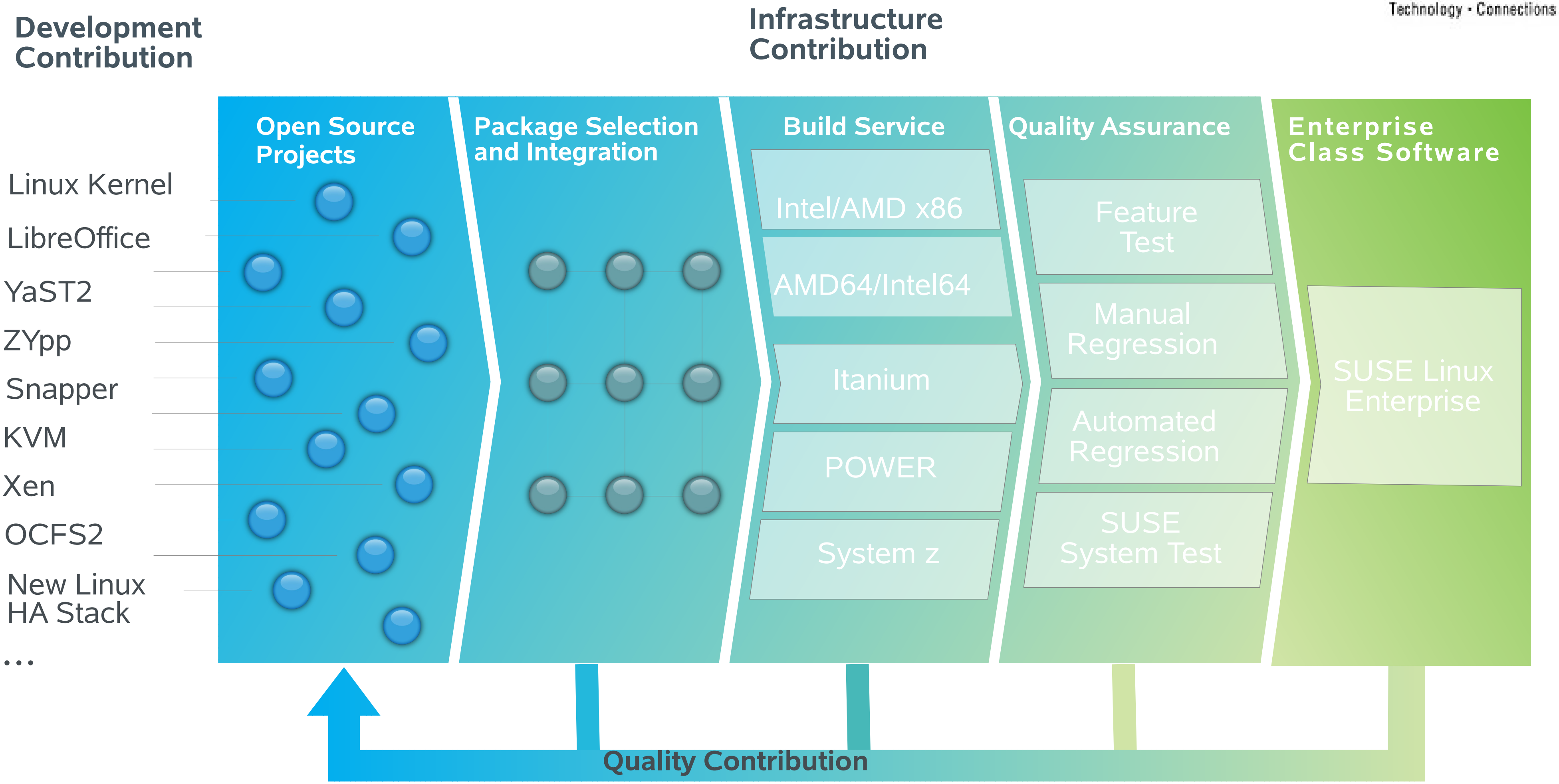
SP3 LTSS

SP4 LTSS

- **13-year lifecycle** (10 years general support, 3 years extended support)
- **5-year lifecycle per Service Pack** (2 years general + 3 years extended support)
- Long Term Service Pack Support (LTSS) available for all versions, including GA

SUSE® Linux Enterprise

The SUSE® Build Service* Advantage



- Reduces production problems
- Consolidates IT skills across disparate systems
- Delivers critical updates in hours – not days or weeks

* SUSE Build Service is the internal entity of the Open® Build Service

Processes involved

Enterprise Class Product

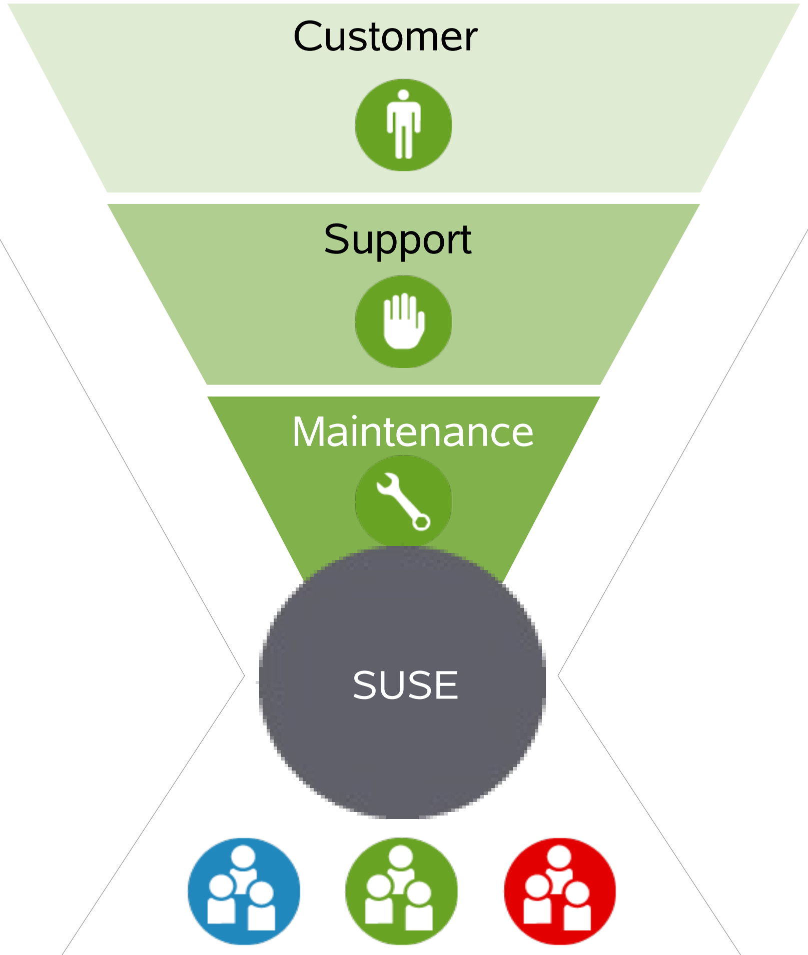
Certifications

Stable Interfaces

Installable Product

Package/Solution

Code/Feature



Customer

Support

Maintenance

SUSE

Community: OSS Teams, IHVs, ISVs, ...

Lifecycle Management

Delivery and Operation

Q+A

Flaw Remidiation

Bugtracking

Buildservice Approval Process

Packaging Process

Community Contacts

How to access SUSE code ?

Securing the supply chain

- SUSE download
  - The product is delivered via download as DVD iso images (shared & scalable infrastructure for The Attachmate Group)
  - Download requires a SUSE / Novell registered account
  - Website access and connections are encrypted (Customer Center)

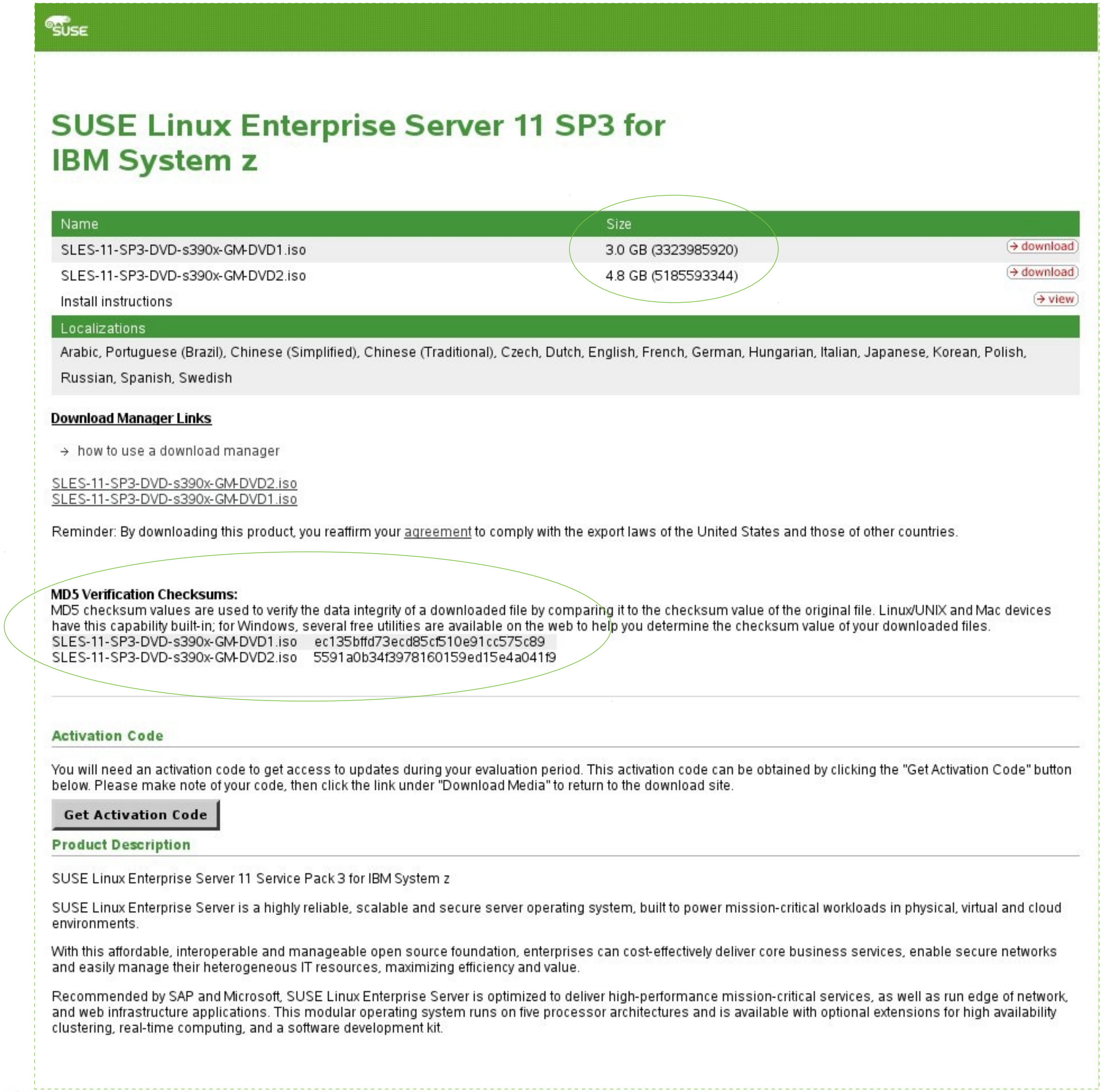
- Different installation source options
  - CD, DVD, or directory (mounted iso image)
  - From a server: nfs, ftp, smb, http
  - Repositories provide signed content files and packages

- Alternatives
  - SLES Starter System: download images, use with z/VM
  - Clone golden image

Download

Qualified DVD images (name, size, checksum)

https://www.suse.com/security/download-verification.html



SUSE Linux Enterprise Server 11 SP3 for IBM System z

Name	Size	
SLES-11-SP3-DVD-s390x-GM-DVD1.iso	3.0 GB (3323985920)	download
SLES-11-SP3-DVD-s390x-GM-DVD2.iso	4.8 GB (5185593344)	download
Install instructions		view

Localizations
Arabic, Portuguese (Brazil), Chinese (Simplified), Chinese (Traditional), Czech, Dutch, English, French, German, Hungarian, Italian, Japanese, Korean, Polish, Russian, Spanish, Swedish

Download Manager Links

→ how to use a download manager

SLES-11-SP3-DVD-s390x-GM-DVD2.iso
SLES-11-SP3-DVD-s390x-GM-DVD1.iso

Reminder: By downloading this product, you reaffirm your agreement to comply with the export laws of the United States and those of other countries.

MD5 Verification Checksums:
MD5 checksum values are used to verify the data integrity of a downloaded file by comparing it to the checksum value of the original file. Linux/UNIX and Mac devices have this capability built-in; for Windows, several free utilities are available on the web to help you determine the checksum value of your downloaded files.

SLES-11-SP3-DVD-s390x-GM-DVD1.iso	ec135bffd73ecd85cf510e91cc575c89
SLES-11-SP3-DVD-s390x-GM-DVD2.iso	5591a0b34f3978160159ed15e4a041f9

Activation Code

You will need an activation code to get access to updates during your evaluation period. This activation code can be obtained by clicking the "Get Activation Code" button below. Please make note of your code, then click the link under "Download Media" to return to the download site.

Get Activation Code

Product Description

SUSE Linux Enterprise Server 11 Service Pack 3 for IBM System z

SUSE Linux Enterprise Server is a highly reliable, scalable and secure server operating system, built to power mission-critical workloads in physical, virtual and cloud environments.

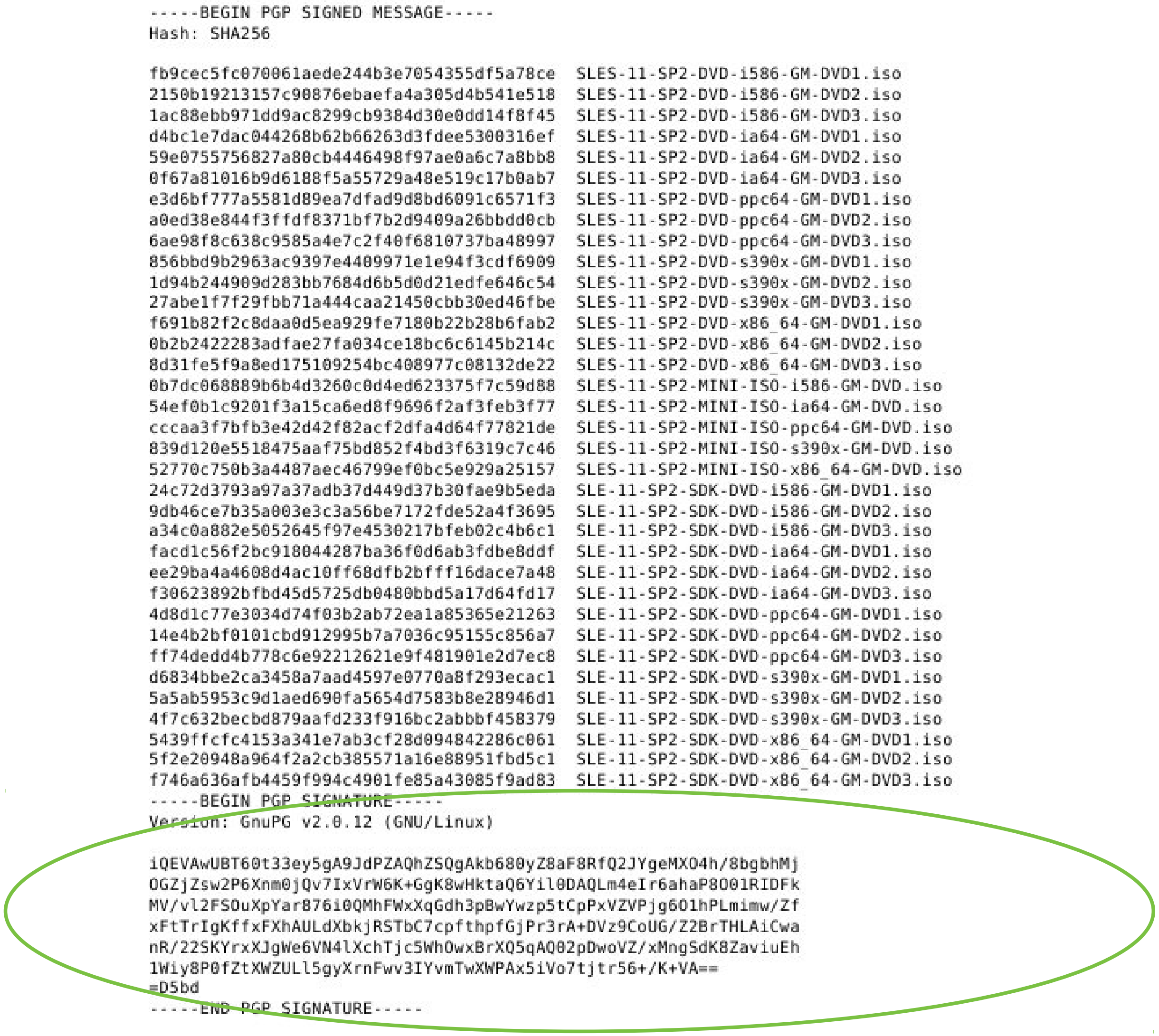
With this affordable, interoperable and manageable open source foundation, enterprises can cost-effectively deliver core business services, enable secure networks and easily manage their heterogeneous IT resources, maximizing efficiency and value.

Recommended by SAP and Microsoft, SUSE Linux Enterprise Server is optimized to deliver high-performance mission-critical services, as well as run edge of network, and web infrastructure applications. This modular operating system runs on five processor architectures and is available with optional extensions for high availability clustering, real-time computing, and a software development kit.

Download

Qualified DVD images (name, size, checksum)

https://www.suse.com/security/download-verification.html



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

fb9cec5fc070061aede244b3e7054355df5a78ce  SLES-11-SP2-DVD-i586-GM-DVD1.iso
2150b19213157c90876ebaefa4a305d4b541e518  SLES-11-SP2-DVD-i586-GM-DVD2.iso
1ac88ebb971dd9ac8299cb9384d30e0dd14f8f45  SLES-11-SP2-DVD-i586-GM-DVD3.iso
d4bc1e7dac044268b62b66263d3fdee5300316ef  SLES-11-SP2-DVD-ia64-GM-DVD1.iso
59e0755756827a80cb4446498f97ae0a6c7a8bb8  SLES-11-SP2-DVD-ia64-GM-DVD2.iso
0f67a81016b9d6188f5a55729a48e519c17b0ab7  SLES-11-SP2-DVD-ia64-GM-DVD3.iso
e3d6bf777a5581d89ea7dfad9d8bd6091c6571f3  SLES-11-SP2-DVD-ppc64-GM-DVD1.iso
a0ed38e844f3ffdf8371bf7b2d9409a26bbdd0cb  SLES-11-SP2-DVD-ppc64-GM-DVD2.iso
6ae98f8c638c9585a4e7c2f40f6810737ba48997  SLES-11-SP2-DVD-ppc64-GM-DVD3.iso
856bbd9b2963ac9397e4409971e1e94f3cdf6909  SLES-11-SP2-DVD-s390x-GM-DVD1.iso
1d94b244909d283bb7684d6b5d0d21edfe646c54  SLES-11-SP2-DVD-s390x-GM-DVD2.iso
27abe1f7f29fbb71a444caa21450cbb30ed46fbe  SLES-11-SP2-DVD-s390x-GM-DVD3.iso
f691b82f2c8daa0d5ea929fe7180b22b28b6fab2  SLES-11-SP2-DVD-x86_64-GM-DVD1.iso
0b2b2422283adfae27fa034ce18bc6c6145b214c  SLES-11-SP2-DVD-x86_64-GM-DVD2.iso
8d31fe5f9a8ed175109254bc408977c08132de22  SLES-11-SP2-DVD-x86_64-GM-DVD3.iso
0b7dc068889b6b4d3260c0d4ed623375f7c59d88  SLES-11-SP2-MINI-ISO-i586-GM-DVD.iso
54ef0b1c9201f3a15ca6ed8f9696f2af3feb3f77  SLES-11-SP2-MINI-ISO-ia64-GM-DVD.iso
cccaa3f7bfb3e42d42f82acf2dfa4d64f77821de  SLES-11-SP2-MINI-ISO-ppc64-GM-DVD.iso
839d120e5518475aaf75bd852f4bd3f6319c7c46  SLES-11-SP2-MINI-ISO-s390x-GM-DVD.iso
52770c750b3a4487aec46799ef0bc5e929a25157  SLES-11-SP2-MINI-ISO-x86_64-GM-DVD.iso
24c72d3793a97a37adb37d449d37b30fae9b5eda  SLE-11-SP2-SDK-DVD-i586-GM-DVD1.iso
9db46ce7b35a003e3c3a56be7172fde52a4f3695  SLE-11-SP2-SDK-DVD-i586-GM-DVD2.iso
a34c0a882e5052645f97e4530217bfeb02c4b6c1  SLE-11-SP2-SDK-DVD-i586-GM-DVD3.iso
facd1c56f2bc918044287ba36f0d6ab3fdbe8ddf  SLE-11-SP2-SDK-DVD-ia64-GM-DVD1.iso
ee29ba4a4608d4ac10ff68dfb2bfff16dace7a48  SLE-11-SP2-SDK-DVD-ia64-GM-DVD2.iso
f30623892bfbd45d5725db0480bbd5a17d64fd17  SLE-11-SP2-SDK-DVD-ia64-GM-DVD3.iso
4d8d1c77e3034d74f03b2ab72ea1a85365e21263  SLE-11-SP2-SDK-DVD-ppc64-GM-DVD1.iso
14e4b2bf0101cbd912995b7a7036c95155c856a7  SLE-11-SP2-SDK-DVD-ppc64-GM-DVD2.iso
ff74dedd4b778c6e92212621e9f481901e2d7ec8  SLE-11-SP2-SDK-DVD-ppc64-GM-DVD3.iso
d6834bbe2ca3458a7aad4597e0770a8f293ecac1  SLE-11-SP2-SDK-DVD-s390x-GM-DVD1.iso
5a5ab5953c9d1aed690fa5654d7583b8e28946d1  SLE-11-SP2-SDK-DVD-s390x-GM-DVD2.iso
4f7c632becbd879aafd233f916bc2abbbf458379  SLE-11-SP2-SDK-DVD-s390x-GM-DVD3.iso
5439ffcfc4153a341e7ab3cf28d094842286c061  SLE-11-SP2-SDK-DVD-x86_64-GM-DVD1.iso
5f2e20948a964f2a2cb385571a16e88951fbd5c1  SLE-11-SP2-SDK-DVD-x86_64-GM-DVD2.iso
f746a636afb4459f994c4901fe85a43085f9ad83  SLE-11-SP2-SDK-DVD-x86_64-GM-DVD3.iso
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.12 (GNU/Linux)

iQEVAwUBT60t33ey5gA9JdPZAQhZSQgAkb680yZ8aF8RfQ2JYgeMXO4h/8bgbhMj
OGZjZsw2P6Xnm0jQv7IxVrW6K+GgK8wHktaQ6Yil0DAQLm4eIr6ahaP8O01RIDFk
MV/vl2FSOuXpYar876i0QMhFWxXqGdh3pBwYwzp5tCpPxVZVPjg6O1hPLmimw/Zf
xFtTrIgKffxFXhAULdXbkjRSTbC7cpfthpfGjPr3rA+DVz9CoUG/Z2BrTHLAiCwa
nR/22SKYrxXJgWe6VN4lXchTjc5WhOwxBrXQ5qAQ02pDwoVZ/xMngSdK8ZaviuEh
1Wiy8P0fZtXWZULl5gyXrnFwv3IYvmTwXWPAx5iVo7tjtr56+/K+VA==
=D5bd
-----END PGP SIGNATURE-----
```

SUSE® Linux Enterprise 11

Systems Management Today

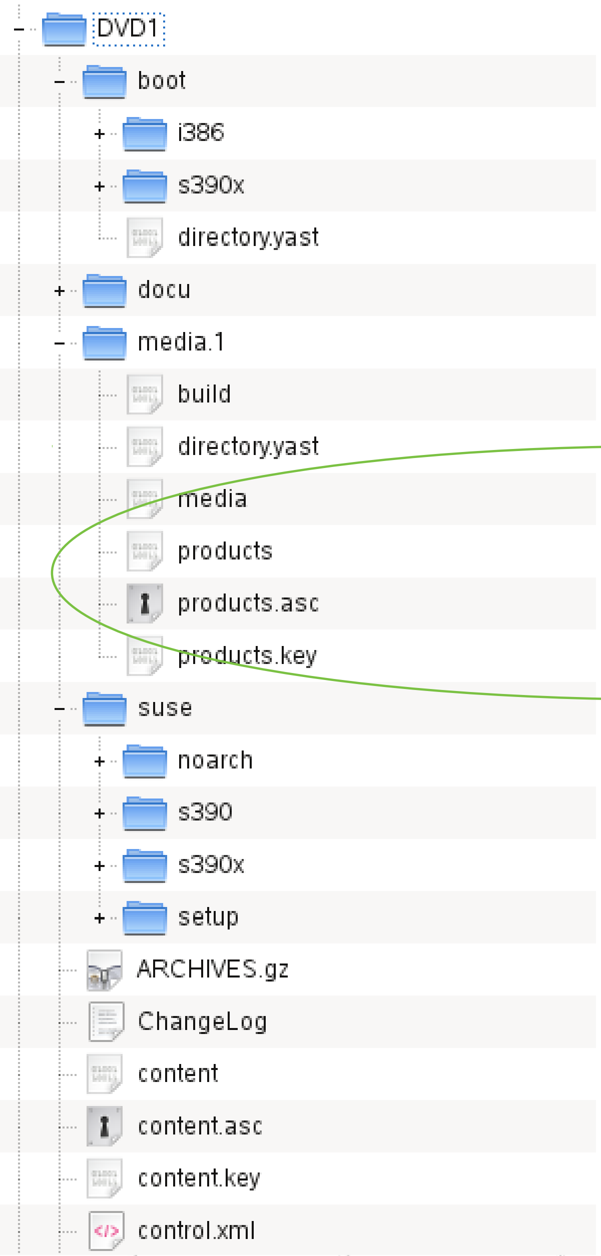
- YaST – unique, highly integrated local management tool
  - Ease of use, effective learning curve; reduces training efforts
  - Automation via AutoYaST for data center mass deployments
- Fastest open source update stack (ZYpp)
  - Reduce management time, effort and cost
  - Improve reliability and availability by reducing down times
  - ZYpp handles multiple installed package versions (e.g. Kernel)
- Build in Installation Server
  - Easy setup, allows for internal high speed repository serving
  - Allows to speed up and automated release and SP migrations
  - Can be combined with SMT to serve multiple SUSE products

Repositories

How to handle software packages

- Structure
  - CD / DVD iso images provide hashes
  - Code repositories and subdirectories are secured by signed content files
  - /repo directories provide product and package meta data
  - /rpm directories contain packages (rpm), their content is signed, and package has unique ids

Installation Repository Tree



```
- DVD1
  - boot
    + i386
    + s390x
      directory.yast
  + docu
  - media.1
      build
      directory.yast
      media
      products
      products.asc
      products.key
  - suse
    + noarch
    + s390
    + s390x
    + setup
    ARCHIVES.gz
    ChangeLog
    content
    content.asc
    content.key
    control.xml
```

- i386 ← i386 rescue system to export media from a x86 workstation
- s390x ← s390x first boot / ipl kernel and ram disk
- docu ← SUSE manuals in different languages
- media.1 ← media description
- products ← product description
- products.asc ← product ascii key
- suse ← package (rpm) repository
- noarch ← architecture independent packages (scripts, etc)
- s390 ← s390 rpm (32bit)
- s390x ← s390x rpm (64bit and 32bit)
- setup ← “patterns”

Zypper

Resolving dependencies and managing software installations

- Zypper (**z**md & **y**um & **p**ackage & **p**atch management)
  - Software management and command line interface to libzypp
  - Manage, refresh and list channels: e.g. zypper lr -u
  - Resolve dependencies across all attached channels
  - Manage patterns (predefines groups of packages)
  - Install & uninstall packages
  - Check of signed content files and subdirectory pathes
  - Logging
  - ...

  - Consult zypper manual page for more details
  - Check for size of /var/cache/zypp, set keeppackages=0 depending on needs (eg. Clean up packgage download cache after updating packages)

The Quartermaster

Knowing where files are to be placed

- Red Hat Package Manager (rpm)
  - Source code packages to build applications (w/ spec file & change log)
  - Executables, configuration files and documentation included in rpm to easy deployment and removal of applications
  - Meta data management by rpm
    - rpm database
    - file locations
    - requirements and dependencies tracking
    - Install, Update and delete
    - Changes and check sum tracking
    - Key management (signed packages, authentication)
    - … (for more options please see manual page of rpm)

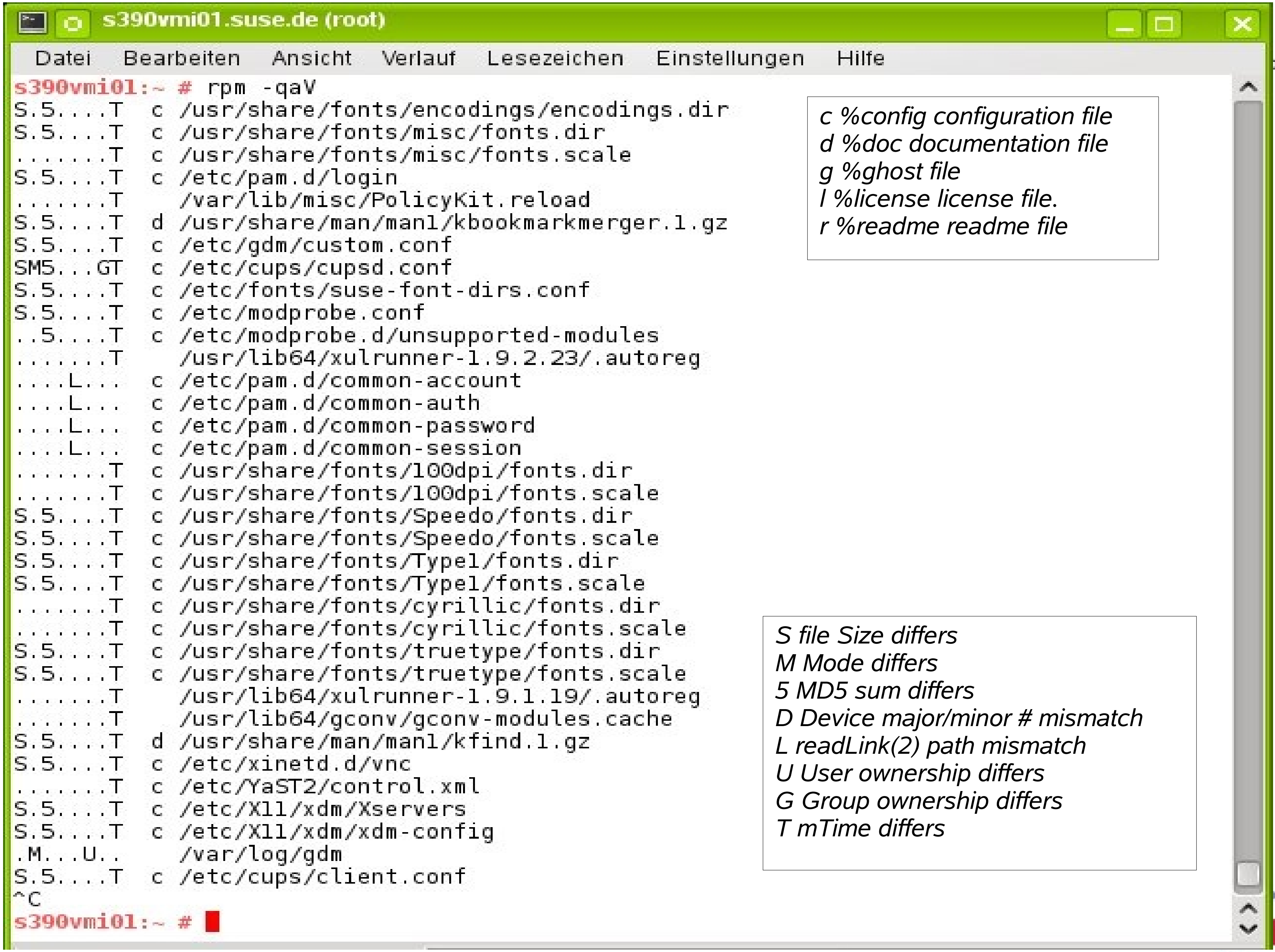
rpm -q gpg-pubkeys-*

List all registered keys

- gpg-pubkey-307e3d54-4be01a65
  - SuSE Package Signing Key <build@suse.de>
- gpg-pubkey-3d25d3d9-36e12d04
  - SuSE Security Team <security@suse.de>
- gpg-pubkey-9c800aca-4be01999
  - SuSE Package Signing Key <build@suse.de>
- gpg-pubkey-b37b98a9-4be01a1a
  - SUSE PTF Signing Key <support@suse.com>

rpm -qaV

List all changes to package files



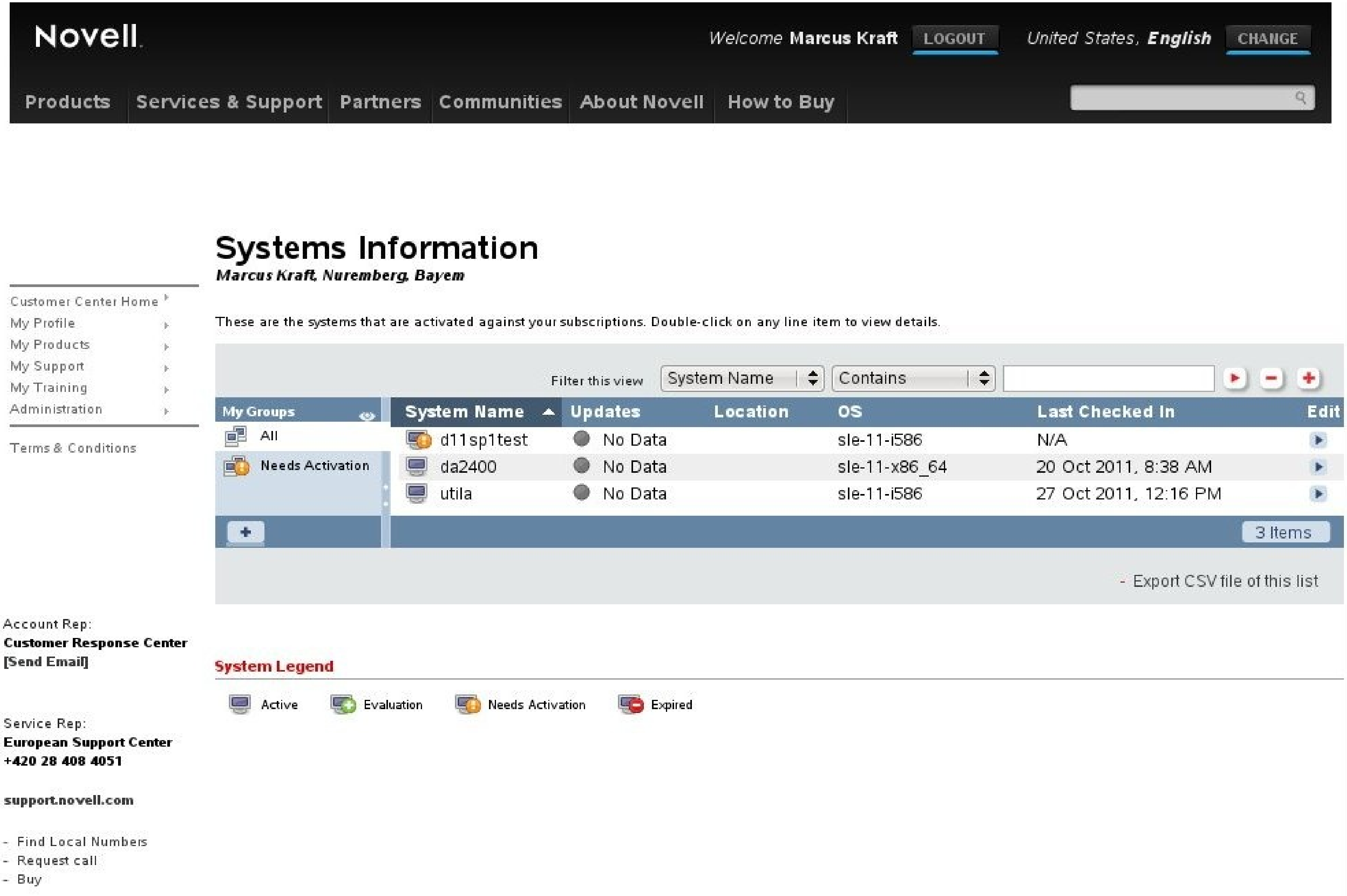
```
s390vmi01:~ # rpm -qaV
S.5....T  c /usr/share/fonts/encodings/encodings.dir
S.5....T  c /usr/share/fonts/misc/fonts.dir
.......T  c /usr/share/fonts/misc/fonts.scale
S.5....T  c /etc/pam.d/login
.......T    /var/lib/misc/PolicyKit.reload
S.5....T  d /usr/share/man/man1/kbookmarkmerger.1.gz
S.5....T  c /etc/gdm/custom.conf
SM5...GT  c /etc/cups/cupsd.conf
S.5....T  c /etc/fonts/suse-font-dirs.conf
S.5....T  c /etc/modprobe.conf
..5....T  c /etc/modprobe.d/unsupported-modules
.......T    /usr/lib64/xulrunner-1.9.2.23/.autoreg
....L...  c /etc/pam.d/common-account
....L...  c /etc/pam.d/common-auth
....L...  c /etc/pam.d/common-password
....L...  c /etc/pam.d/common-session
.......T  c /usr/share/fonts/100dpi/fonts.dir
.......T  c /usr/share/fonts/100dpi/fonts.scale
S.5....T  c /usr/share/fonts/Speedo/fonts.dir
S.5....T  c /usr/share/fonts/Speedo/fonts.scale
S.5....T  c /usr/share/fonts/Type1/fonts.dir
S.5....T  c /usr/share/fonts/Type1/fonts.scale
.......T  c /usr/share/fonts/cyrillic/fonts.dir
.......T  c /usr/share/fonts/cyrillic/fonts.scale
S.5....T  c /usr/share/fonts/truetype/fonts.dir
S.5....T  c /usr/share/fonts/truetype/fonts.scale
.......T    /usr/lib64/xulrunner-1.9.1.19/.autoreg
.......T    /usr/lib64/gconv/gconv-modules.cache
S.5....T  d /usr/share/man/man1/kfind.1.gz
S.5....T  c /etc/xinetd.d/vnc
.......T  c /etc/YaST2/control.xml
S.5....T  c /etc/X11/xdm/Xservers
S.5....T  c /etc/X11/xdm/xdm-config
.M...U..    /var/log/gdm
S.5....T  c /etc/cups/client.conf
^C
s390vmi01:~ #
```

c %config configuration file
d %doc documentation file
g %ghost file
l %license license file.
r %readme readme file

S file Size differs
M Mode differs
5 MD5 sum differs
D Device major/minor # mismatch
L readLink(2) path mismatch
U User ownership differs
G Group ownership differs
T mTime differs

Software Lifecycle Management

Customer Center



Systems Information

Marcus Kraft, Nuremberg, Bayern

These are the systems that are activated against your subscriptions. Double-click on any line item to view details.

Filter this view: System Name | Contains

System Name	Updates	Location	OS	Last Checked In	Edit
d11sp1test	● No Data		sle-11-i586	N/A	▸
da2400	● No Data		sle-11-x86_64	20 Oct 2011, 8:38 AM	▸
utila	● No Data		sle-11-i586	27 Oct 2011, 12:16 PM	▸

3 Items

- Export CSV file of this list

System Legend

Active Evaluation Needs Activation Expired

Account Rep:
Customer Response Center
[Send Email]

Service Rep:
European Support Center
+420 28 408 4051

support.novell.com

- Find Local Numbers
- Request call
- Buy

Critical Patches

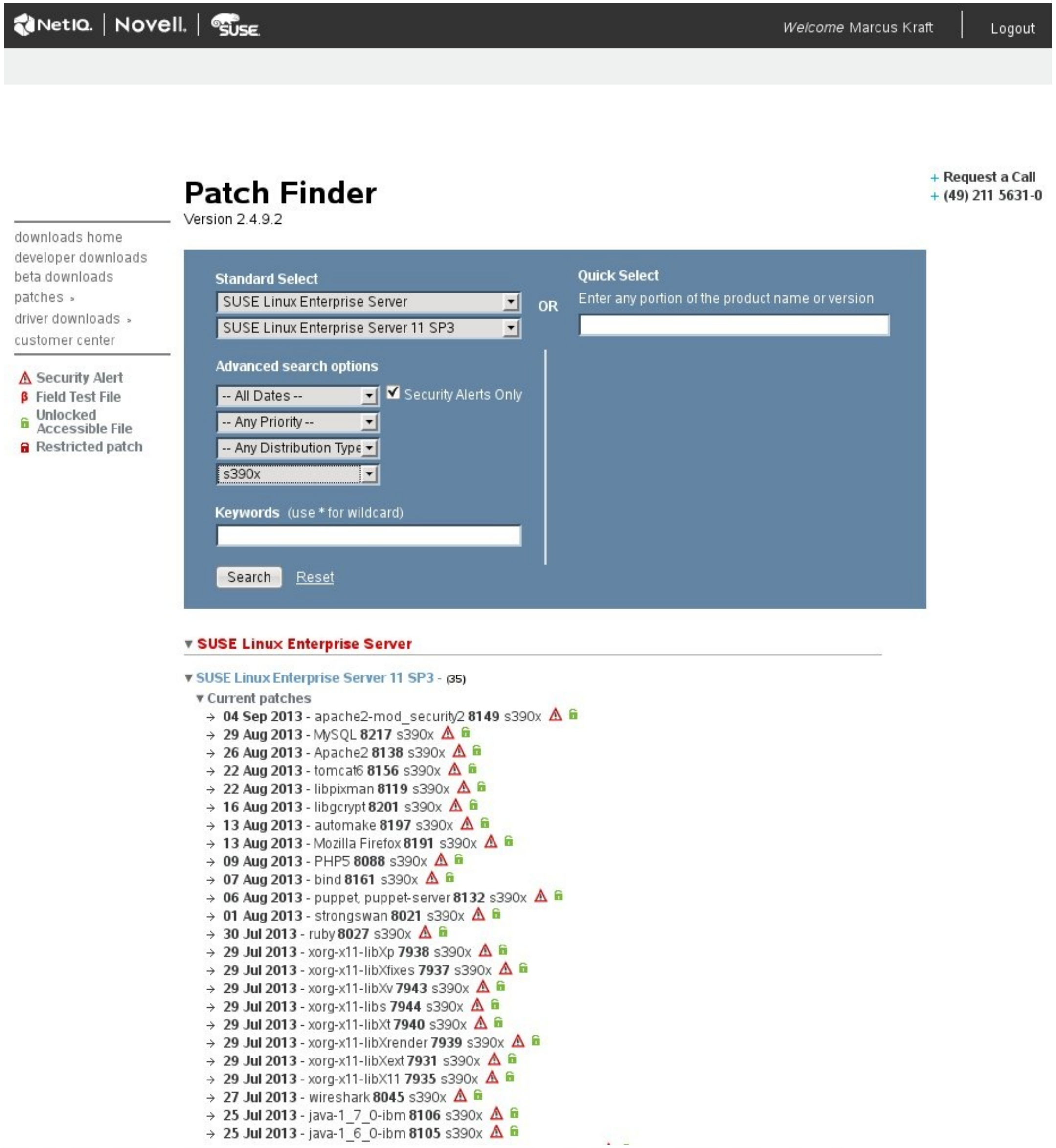
How to get informed ?

- Automated email alert for critical fixes
  - SUSE customer center
- Check SUSE update advisory
  - https://www.suse.com/support/update/

- Example: kernel update
  - https://download.novell.com/Download?buildid=MzkPKLmG54I~
  - Referenceshttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0160

Patch Finder

Product specific search for critical updates



NetIQ | Novell | SUSE — *Welcome* Marcus Kraft | Logout

Patch Finder

Version 2.4.9.2

+ Request a Call
+ (49) 211 5631-0

- downloads home
- developer downloads
- beta downloads
- patches »
- driver downloads »
- customer center

⚠ Security Alert
β Field Test File
🔓 Unlocked Accessible File
🔒 Restricted patch

Standard Select

SUSE Linux Enterprise Server ▾
SUSE Linux Enterprise Server 11 SP3 ▾

OR

Quick Select

Enter any portion of the product name or version

Advanced search options

-- All Dates -- ▾ ☑ Security Alerts Only
-- Any Priority -- ▾
-- Any Distribution Type ▾
s390x ▾

Keywords (use * for wildcard)

Search | Reset

▼ **SUSE Linux Enterprise Server**

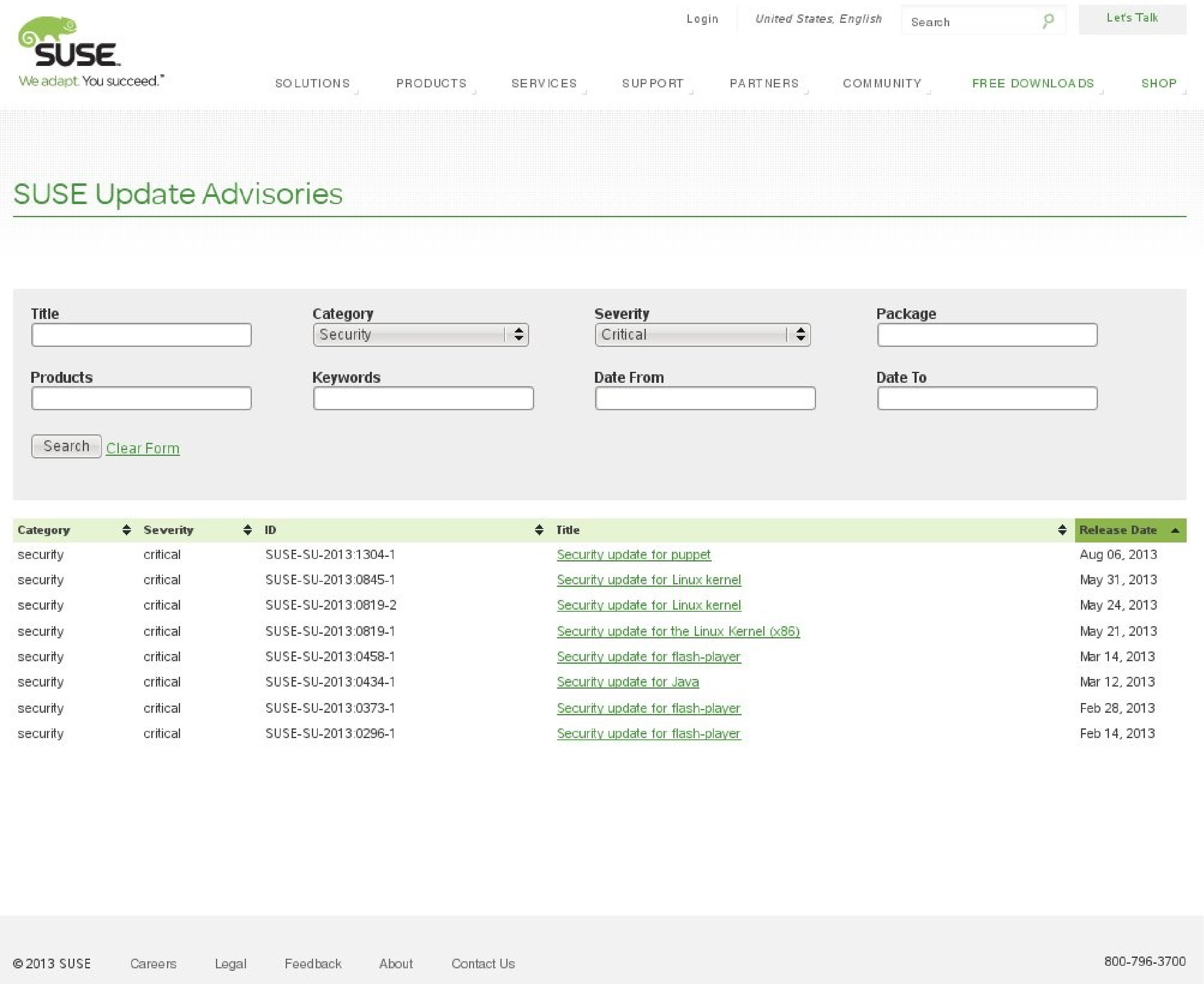
▼ SUSE Linux Enterprise Server 11 SP3 - (35)

▼ Current patches

- → **04 Sep 2013** - apache2-mod_security2 **8149** s390x ⚠ 🔓
- → **29 Aug 2013** - MySQL **8217** s390x ⚠ 🔓
- → **26 Aug 2013** - Apache2 **8138** s390x ⚠ 🔓
- → **22 Aug 2013** - tomcat6 **8156** s390x ⚠ 🔓
- → **22 Aug 2013** - libpixman **8119** s390x ⚠ 🔓
- → **16 Aug 2013** - libgcrypt **8201** s390x ⚠ 🔓
- → **13 Aug 2013** - automake **8197** s390x ⚠ 🔓
- → **13 Aug 2013** - Mozilla Firefox **8191** s390x ⚠ 🔓
- → **09 Aug 2013** - PHP5 **8088** s390x ⚠ 🔓
- → **07 Aug 2013** - bind **8161** s390x ⚠ 🔓
- → **06 Aug 2013** - puppet, puppet-server **8132** s390x ⚠ 🔓
- → **01 Aug 2013** - strongswan **8021** s390x ⚠ 🔓
- → **30 Jul 2013** - ruby **8027** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXp **7938** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXfixes **7937** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXv **7943** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libs **7944** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXt **7940** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXrender **7939** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libXext **7931** s390x ⚠ 🔓
- → **29 Jul 2013** - xorg-x11-libX11 **7935** s390x ⚠ 🔓
- → **27 Jul 2013** - wireshark **8045** s390x ⚠ 🔓
- → **25 Jul 2013** - java-1_7_0-ibm **8106** s390x ⚠ 🔓
- → **25 Jul 2013** - java-1_6_0-ibm **8105** s390x ⚠ 🔓

Security Updates

Multiple criteria search engine https://www.suse.com/support/update/



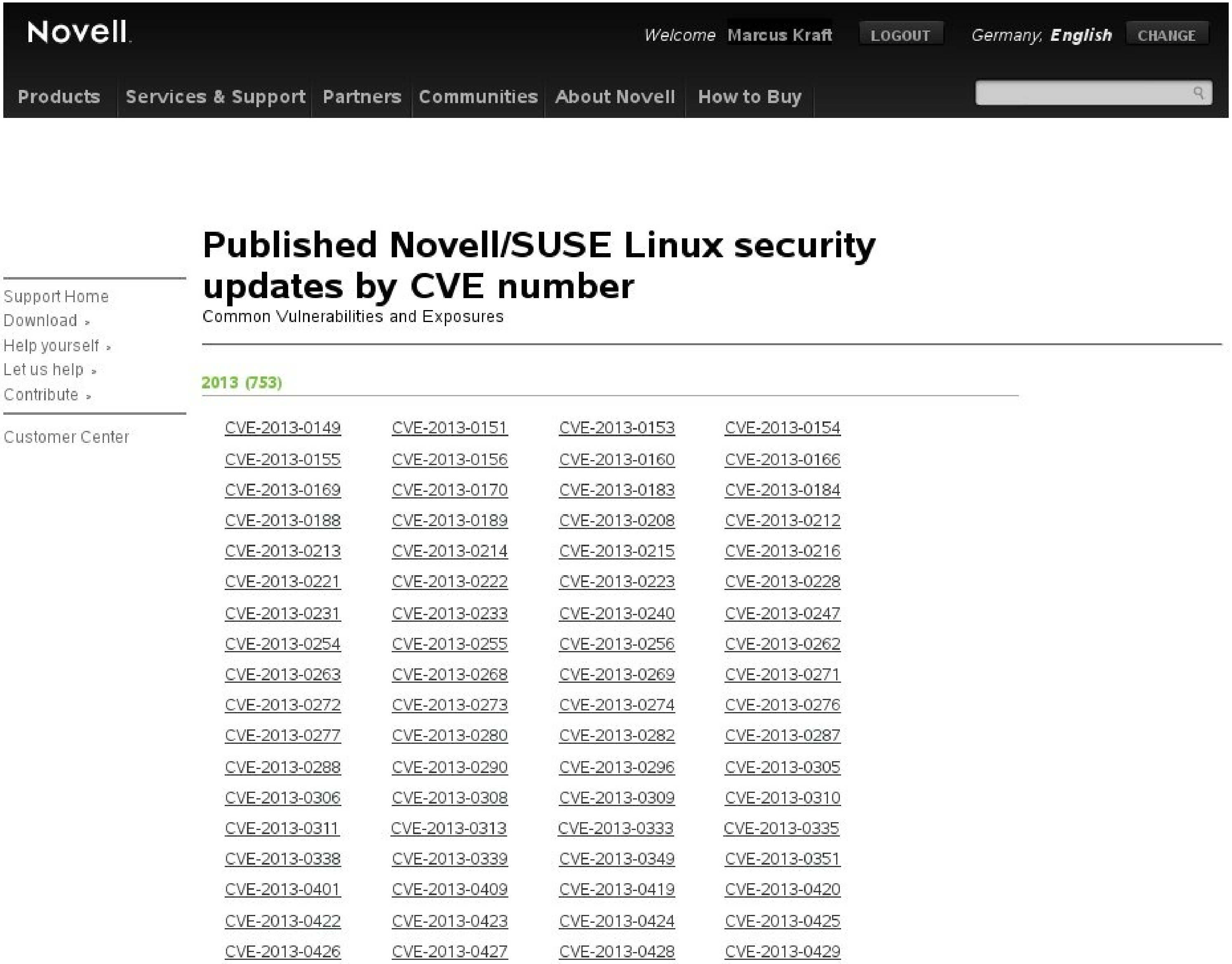
SUSE Update Advisories

Title	Category	Severity	Package
	Security	Critical	
Products	Keywords	Date From	Date To

Category	Severity	ID	Title	Release Date
security	critical	SUSE-SU-2013:1304-1	Security update for puppet	Aug 06, 2013
security	critical	SUSE-SU-2013:0845-1	Security update for Linux kernel	May 31, 2013
security	critical	SUSE-SU-2013:0819-2	Security update for Linux kernel	May 24, 2013
security	critical	SUSE-SU-2013:0819-1	Security update for the Linux Kernel (x86)	May 21, 2013
security	critical	SUSE-SU-2013:0458-1	Security update for flash-player	Mar 14, 2013
security	critical	SUSE-SU-2013:0434-1	Security update for Java	Mar 12, 2013
security	critical	SUSE-SU-2013:0373-1	Security update for flash-player	Feb 28, 2013
security	critical	SUSE-SU-2013:0296-1	Security update for flash-player	Feb 14, 2013

Security Updates

by CVE number



Published Novell/SUSE Linux security updates by CVE number

Common Vulnerabilities and Exposures

2013 (753)

CVE-2013-0149 CVE-2013-0151 CVE-2013-0153 CVE-2013-0154
CVE-2013-0155 CVE-2013-0156 CVE-2013-0160 CVE-2013-0166
CVE-2013-0169 CVE-2013-0170 CVE-2013-0183 CVE-2013-0184
CVE-2013-0188 CVE-2013-0189 CVE-2013-0208 CVE-2013-0212
CVE-2013-0213 CVE-2013-0214 CVE-2013-0215 CVE-2013-0216
CVE-2013-0221 CVE-2013-0222 CVE-2013-0223 CVE-2013-0228
CVE-2013-0231 CVE-2013-0233 CVE-2013-0240 CVE-2013-0247
CVE-2013-0254 CVE-2013-0255 CVE-2013-0256 CVE-2013-0262
CVE-2013-0263 CVE-2013-0268 CVE-2013-0269 CVE-2013-0271
CVE-2013-0272 CVE-2013-0273 CVE-2013-0274 CVE-2013-0276
CVE-2013-0277 CVE-2013-0280 CVE-2013-0282 CVE-2013-0287
CVE-2013-0288 CVE-2013-0290 CVE-2013-0296 CVE-2013-0305
CVE-2013-0306 CVE-2013-0308 CVE-2013-0309 CVE-2013-0310
CVE-2013-0311 CVE-2013-0313 CVE-2013-0333 CVE-2013-0335
CVE-2013-0338 CVE-2013-0339 CVE-2013-0349 CVE-2013-0351
CVE-2013-0401 CVE-2013-0409 CVE-2013-0419 CVE-2013-0420
CVE-2013-0422 CVE-2013-0423 CVE-2013-0424 CVE-2013-0425
CVE-2013-0426 CVE-2013-0427 CVE-2013-0428 CVE-2013-0429

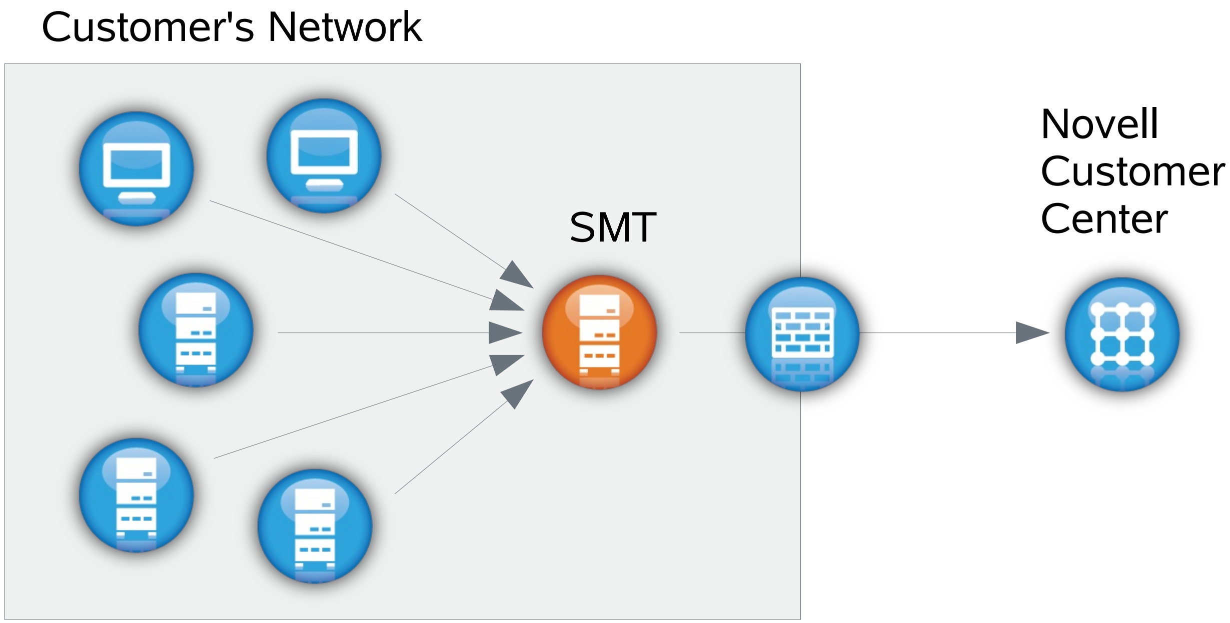
z BladeCenter Extension

Subscription Management Tool
Overview

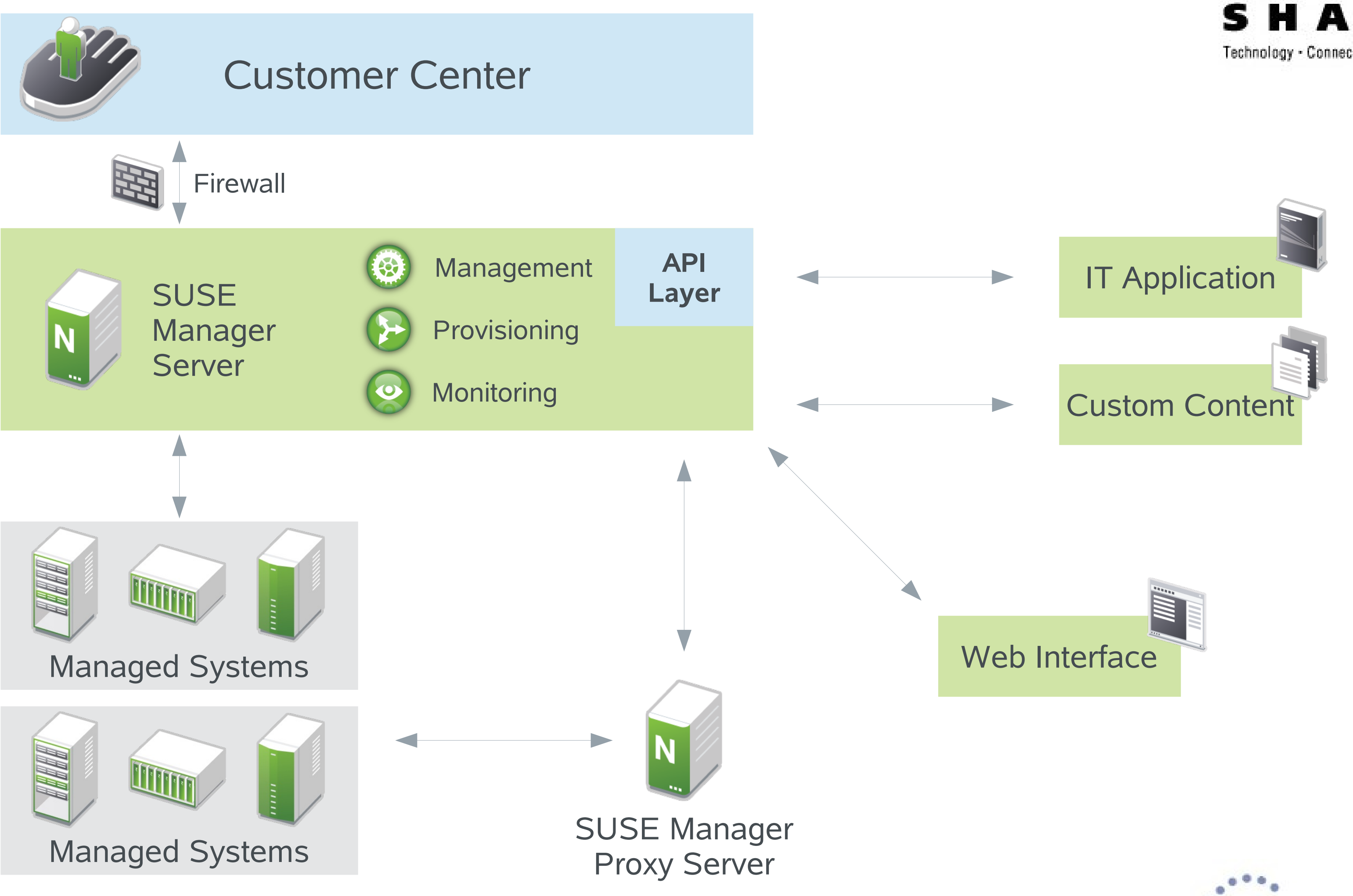
SMT is a proxy and auditing tool that mirrors the Novell® Customer Center update channels and tightly integrates with it.

It allows you to accurately register and manage an entire SUSE® Linux Enterprise deployment and subscriptions.

It allows for retrieving and staging of updates to support the deployment process workflow.



How Does SUSE Manager Work?



Tools

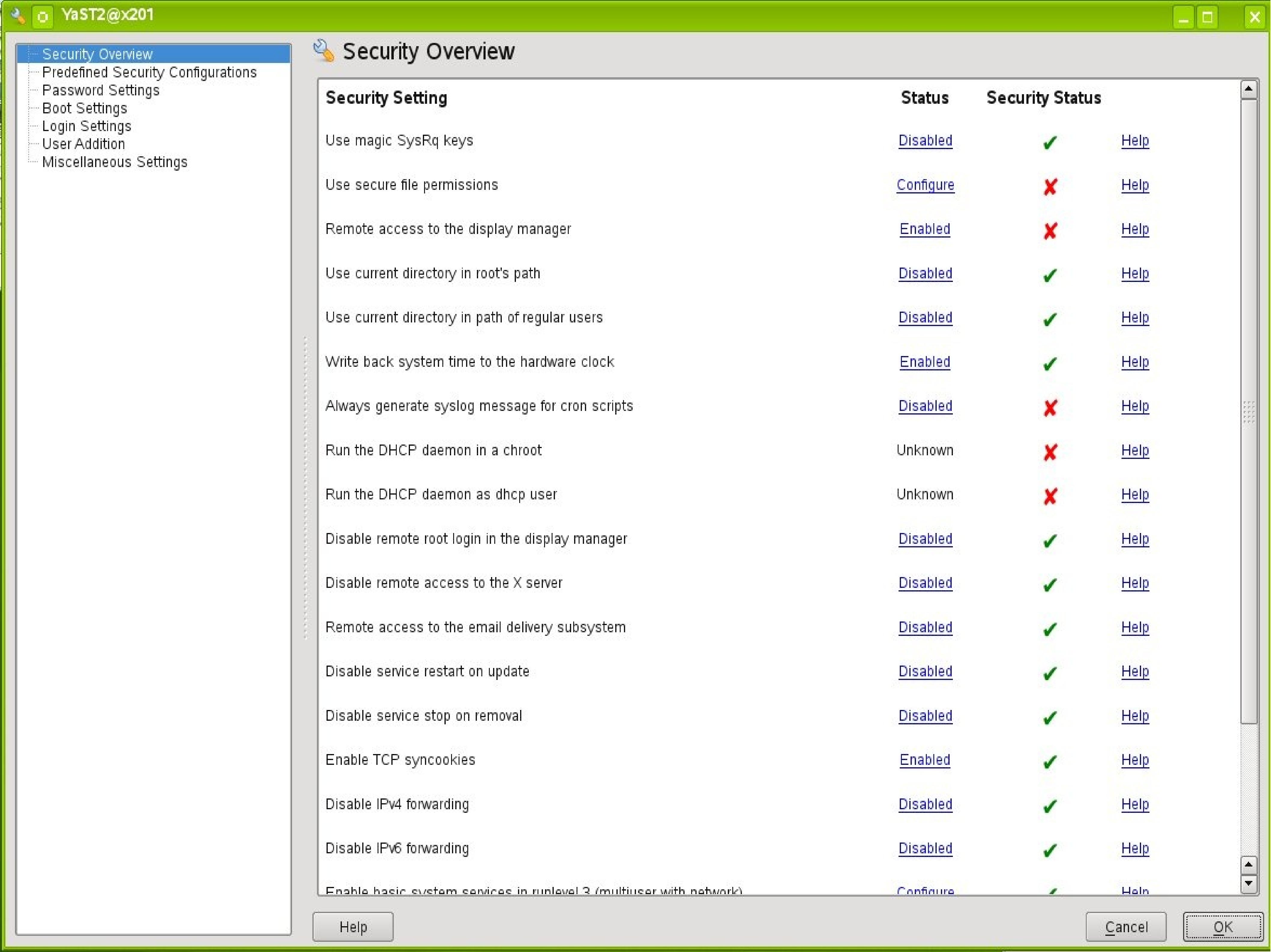
More Security Contributors

- System Hardening → “YaST Security Center”
- Application confinement with AppArmor
- Basic Enablement for “SE Linux”
- Check integrity of systems on file level with AIDE
- Protect systems and data using encryption on three levels: “Full Disk” – Volume – Filesystem (eCryptFS)
- Filesystem POSIX capabilities to allow more finegrained control of access to files and running executables
- Certifications
  - Carrier Grade Linux 4.0 registration: validated for telecommunication
  - IPv6 (refresh)

SUSE® Linux Enterprise Server

Configuration Concepts

- Services default to “off” with very few exceptions: sshd, rpcbind
- Configuration templates for advanced configurations
- Administrative tools need root authentication
- Cryptographic integrity protection of packages and meta information



Security Overview

Security Setting	Status	Security Status	
Use magic SysRq keys	Disabled	✓	Help
Use secure file permissions	Configure	✗	Help
Remote access to the display manager	Enabled	✗	Help
Use current directory in root's path	Disabled	✓	Help
Use current directory in path of regular users	Disabled	✓	Help
Write back system time to the hardware clock	Enabled	✓	Help
Always generate syslog message for cron scripts	Disabled	✗	Help
Run the DHCP daemon in a chroot	Unknown	✗	Help
Run the DHCP daemon as dhcp user	Unknown	✗	Help
Disable remote root login in the display manager	Disabled	✓	Help
Disable remote access to the X server	Disabled	✓	Help
Remote access to the email delivery subsystem	Disabled	✓	Help
Disable service restart on update	Disabled	✓	Help
Disable service stop on removal	Disabled	✓	Help
Enable TCP syncookies	Enabled	✓	Help
Disable IPv4 forwarding	Disabled	✓	Help
Disable IPv6 forwarding	Disabled	✓	Help
Enable basic system services in runlevel 3 (multiuser with network)	Configure	✓	Help

What it Does in the Background

Run another YaSTmodule

Change settings in files in /etc/sysconfig

Modify configuration files directly

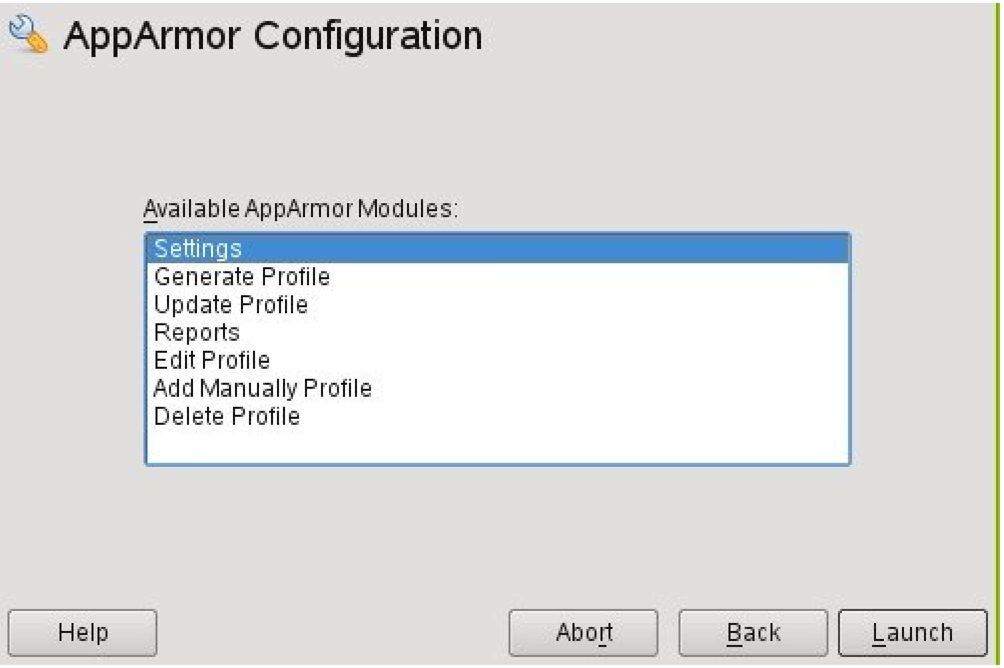
AppArmor Security

- Creates firewall around any Linux program (custom, open source, third party)
- Prevents the exploitation of unknown or undiscovered application vulnerabilities
- Easy to use GUI tools with static analysis and learning-based profile development
- Default policies included
- Create custom policy in hours, not days

AppArmor: usr.sbin.vsftpd

/etc/apparmor/profiles/extras/

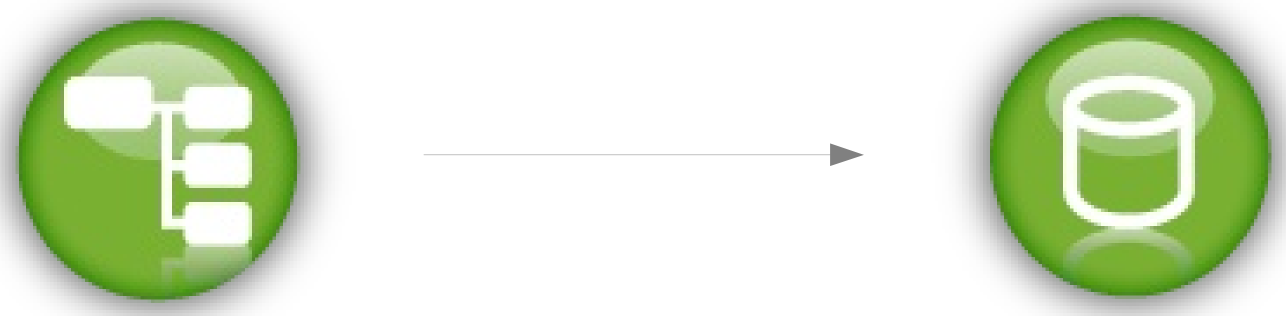
```
#include <tunables/global>

/usr/sbin/vsftpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/authentication>

  /dev/urandom               r,
  /etc/fstab                 r,
  /etc/hosts.allow           r,
  /etc/hosts.deny            r,
  /etc/mtab                  r,
  /etc/shells                r,
  /etc/vsftpd.*              r,
  /etc/vsftpd/*              r,
  /usr/sbin/vsftpd           rmix,
  /var/log/vsftpd.log        w,
  /var/log/xferlog           w,
  # anon chroots
  /                          r,
  /pub                       r,
  /pub/**                    r,
  @{HOMEDIRS}                r,
  @{HOME}/**                 rwl,
}
```



AIDE

Advance Intrusion Detection Environemt

- Description & Function
  - AIDE checks configurable attributes of files / file system
  - Stores result in a (remote) database
  - Allows to compare results of different runs and identify changes



SUSE® Linux Enterprise Server

Encryption Technology

- Ssh for remote login, file transfers, remote X sessions
- Storage encryption
  - Ecryptfs
  - dm-crypt
  - cryptoloop for block-layer encryption
- File and E-Mail encryption and signing:
  - GPG (PGP)
- VPN
  - Openvpn
  - strongswan
  - stunnel (SSL/TLS encapsulation)
- Crypto libraries:
  - openssl (most used) – hardware accelerated on z
  - libgcrypt (gpg), mcrypt

cgroups - Resource Control

Consider a large university server with various users - students, professors, system tasks etc. The resource planning for this server could be along the following lines:

CPUs

Top cpuset (20%)

/ \

CPUSet1 CPUSet2

| |

(Profs) (Students)

60% 20%

Memory

Professors = 50%

Students = 30%

System = 20%

Disk I/O

Professors = 50%

Students = 30%

System = 20%

Network I/O

WWW browsing = 20%

/ \

Prof (15%) Students (5%)

Network File System (60%)

Others (20%)

Source: /usr/src/linux/Documentation/cgroups/cgroups.txt

Device Subsystem

Isolation

A system administrator can provide a list of devices that can be accessed by processes under cgroup

- Allow/Deny Rule
- Allow/Deny : READ/WRITE/MKNOD

Limits access to device or file system on a device to only tasks in specified cgroup

Source: http://jp.linuxfoundation.org/jp_uploads/seminar20081119/CgroupMemcgMaster.pdf

SLES for System z

SUSE® Linux Enterprise Server for System z 11 SP3

- zEC12 + zBX = IBM zEnterprise exploitation continued
  - **zBC12, z/VM 6.3,** zBX HX5 support (blade center extension)
  - z9 EC, z10 EC, z196 EC, z9 BC, z10 BC, z114 BC support
  - Java 7 and supportive kernel enhancements
  - Flash Express SC Memory support (/dev/scm)
  - GCC 4.7 for applications targeting zEC12 processor

- Improved RAS tools and System z specific support
  - 2 stage dump & network storage sharing with compression
  - Robust disk mirroring for large pools of DASDs (MD RAID10)
  - Enhanced DASD statistics for PAV & HPF
  - IUCV terminal server client & server setup support
  - s390-tools update

Support for crypto hardware zEC12 Crypto Express4S

Fate 314097 / [LTC 79958]

http://www-03.ibm.com/systems/z/advantages/security/zec12cryptography.html
http://www-03.ibm.com/systems/z/hardware/zenterprise/zec12_specs.html → Crypto Express 4S
Device Drivers, Features, and Commands on SUSE Linux Enterprise Server 11 SP3
http://public.dhe.ibm.com/software/dw/linux390/docu/les3dd03.pdf → Chap 34, p319

- **Description:** z90crypt device driver supports the Crypto Express 4 (CEX4) adapter card, which represents the newest-generation cryptographic feature and is designed to complement the cryptographic capabilities of the CPACF.

- **Customer benefit**

technical	business
• New modes for DES, 3DES, AES	• Enhanced security

SLES	10	11
GA	-	-
SP1+2	-	-
SP3	-	**yes**
SP4	-	n/a

Crypto CPACF exploitation - libica part 2

Fate 314078 / [LTC 73703]
weblink
doculink

- **Description:** Extends the libica library with new modes of operation for DES, 3DES and AES. These modes of operation (CBC-CS, CCM, GCM, CMAC) are supported by Message Security Assist (CPACF) extension 4, which can be used with z196 and later System z mainframes.

- **Customer benefit**

technical	business
• New modes for DES, 3DES, AES • z196 and zEC12 crypto function support	• Enhanced security

SLES	10	11
GA	-	-
SP1+2	-	-
SP3	-	**yes**
SP4	-	n/a

Fill entropy with hwrandom for z10

Fate 310591 / [LTC -]

- **Description:** z10 processor and successors have a pseudo random number generator built in, that can be accessed at /dev/hwrng if active. However, with z90crypt device driver and crypto express cards /dev/random delivers hardware generated random numbers at high rate.

- **Customer benefit**

technical	business
• Use /dev/random as a source of random numbers generated by hardware at a high rate • Avoids stalling of processes querying for randomness	• Better scalability for workloads with lots of processes requiring randomness to execute or proceed

SLES	10	11
GA	-	-
SP1	-	-
SP2+3	-	yes
SP4	-	yes

DS8000 Disk Encryption

Fate 307004 / [LTC 201740]

http://www.ibm.com/developerworks/linux/linux390/s390-tools-1.8.1.html -> dasdview

Device Drivers, Features, and Commands as available with SUSE Linux Enterprise Server 11 p.350

- **Hardware support:** enhances s390-tools to be able to display if the disk storage has its disk encrypted or not.

- **Customer benefit**

technical	business
• Retrieve info on encryption status of device	• Secure data storage

SLES	10	11
GA	-	yes
SP1	-	yes
SP2+3	yes	yes
SP4	yes	yes

Resources

Further Information

Security Focus

The SUSE® Security Team handles all security vulnerabilities in cooperation with the security community, other vendors and upstream developers.

- Contact info, encryption keys, announcements:
  - Email: security@suse.com, security@suse.de
  - http://www.suse.com/security
  - https://www.suse.com/security/download-verification.html
- Common Criteria Support package
  - http://ftp.suse.com/pub/projects/security/CommonCriteria

SUSE to Go

Mobile Enablement App

ADownload from the
iTunes App Store or Google Play
or point your device to:
www.suse.com/susetogo

SUSE® Linux Enterprise

Documentation and Release Notes

- Product Pages
  - http://www.suse.com/products/server/
  - http://www.suse.com/products/sles-for-sap/
  - http://www.suse.com/products/highavailability/
  - http://www.suse.com/products/realtime/
- Unix to Linux Migration
  - http://www.suse.com/solutions/enterprise-linux-servers/unixtolinux.html
- Documentation
  - http://www.suse.com/documentation/
- Release Notes
  - http://www.suse.com/releasenotes/

We adapt. You succeed.

Corporate Headquarters
Maxfeldstrasse 5
90409 Nuremberg
Germany

+49 911 740 53 0 (Worldwide)
www.suse.com

Join us on:
www.opensuse.org

Unpublished Work of SUSE. All Rights Reserved.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.