

Update On Scientific Linux

Connie Sieh

csieh@fnal.gov

Pat Riehecky

riehecky@fnal.gov

Hepix Spring 2013



Scientific Linux



- Presentation Overview
 - The last six months
 - What we are currently working on
 - What we see in the future
 - Topics for conversation



Scientific Linux

Past Six Months

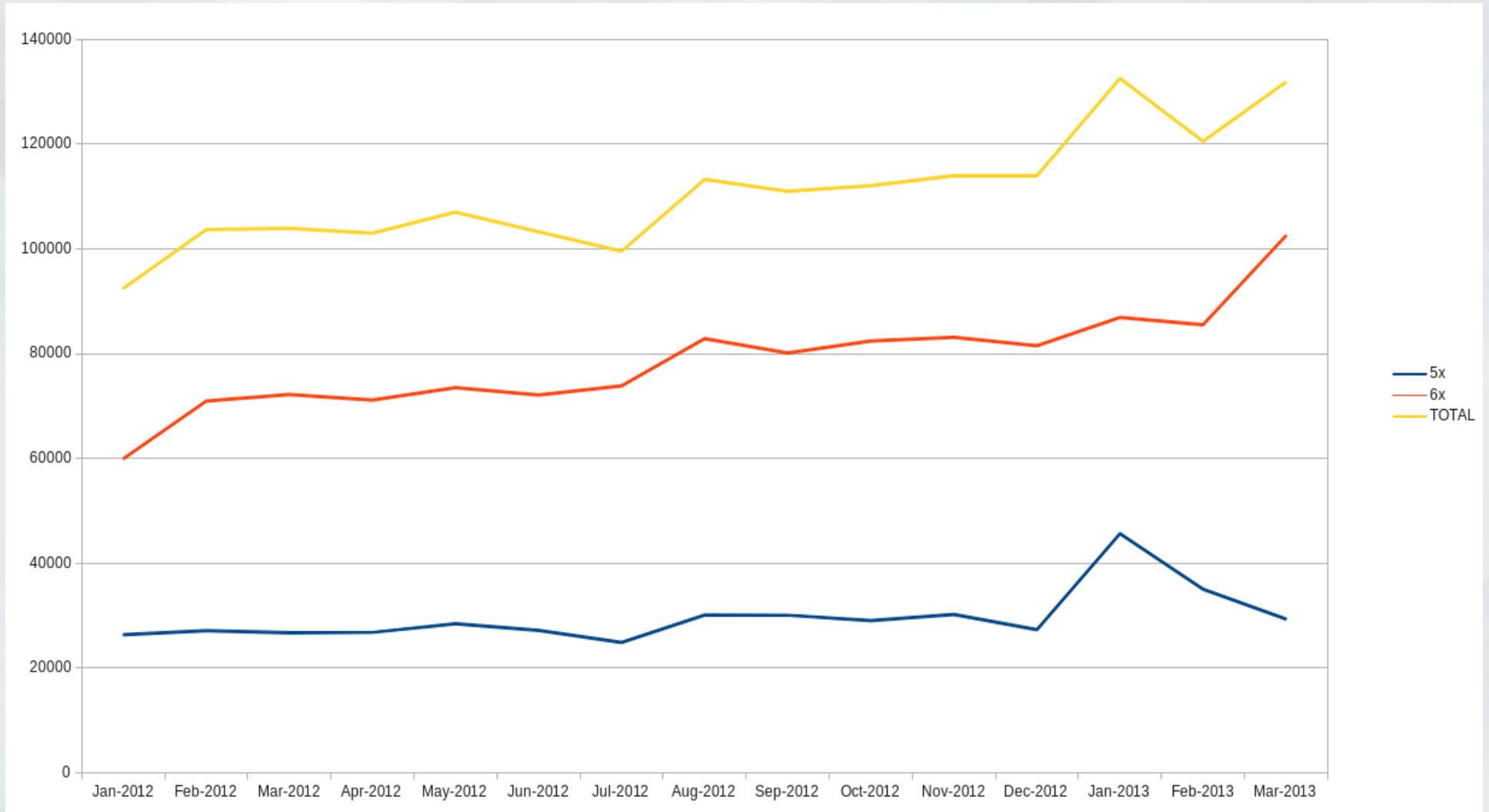


- The following statistics were gathered from ftp.scientificlinux.org log files
 - These numbers are a minimum.
 - We know that the real numbers are higher.
 - The values we have are based on yum downloads of security errata
 - We currently have 80 public mirrors.
 - These statistics do not represent any of the mirror sites.
 - Vertical axis represents “number of unique ip addresses”
 - Horizontal axis is time



Scientific Linux

Past 14 Months





Scientific Linux

Past Six Months



- SL 5.9 released February 2013
 - We decided to treat it more like SL 6
 - Doesn't automatically integrate fastbugs or security errata into the main tree
 - Packages will be available as always, but in the security/fastbugs repo where they belong
 - Defaults to 5x yum conf, formerly yum-conf-59
 - Ndiswrapper removed as does not compile , available via elrepo
 - Closed source Java 6 now at “End of Life” so not included in SL 5.9



Scientific Linux

Past Six Months



- SL 6.4 released – March 2013
 - yum-conf-6x is now the default
 - openafs kernel module changed
 - created addons repo
 - created external_products repo
 - updateinfo.xml support



Scientific Linux

Past Six Months



- SL Live 6.4 expected release – April 2013
 - Web site is at www.livecd.ethz.ch
 - For i386 and x86_64
 - CD, DVD, mini-CD
 - Uses anaconda to install to a hard drive
 - Liveusb-creator makes it trivial to create a LiveUSB from the CD/DVD images.
 - LiveCD-tools makes it easier for people to create their own LiveCD
 - tools moved from main tree to addons



Scientific Linux

Past Six Months



- OpenAFS and SL 6.3/SL 6.4
 - There is an issue with the AFS cache
 - Read/Write may fail, hang, or be very slow.
 - If your cache is on EXT4 and was in use on a previous kernel (before 2.6.32-279.el6) and your system is 32-bit. If you update to a kernel \geq 2.6.32-279.el6 you **may** be affected.
 - See <https://lwn.net/Articles/544520/> for a good detailed description



Scientific Linux



Past Six Months

OpenAFS and SL 6.3/SL 6.4

- Problem resolved in this manner:
 - kmod-openafs is now a noarch
 - It depends on current kmod-openafs-<version> and one version back , this provides yum downgrade support
 - for 6.4 it depends on kmod-openafs-279(SL 6.3) and kmod-openafs-358(SL 6.4)
 - A tweaked /sbin/weak-modules
 - » only lets the 6.3 kmod load in 6.3 series kernels same with 6.4
 - Added /etc/init.d/afs purgecache to clean bad caches. --ONLY RUN THIS WHEN YOU KNOW YOU NEED IT
 - Thanks to Stephan Wiesand of DESY for this work



Scientific Linux

Past Six Months



- SL 6.4 addons repo
 - live-creator was moved from SL main tree
 - Urs live cd tools
 - pssh
 - parallel OpenSSH client with good reporting
 - python-rpmpatch
 - script to automate patching rpms
 - python-Updateinfo
 - tools to create updateinfo.xml
 - revisor was moved from SL main tree
 - compose tool for SL
 - zfs
 - via GE



Scientific Linux

Past six months



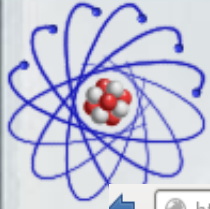
- SL 6.4 external_products repo
 - Red Hat Developer Toolset 1.0 and 1.1
 - Newer compilers
 - Installed in parallel with existing compilers
 - Power users can have the latest gcc/g++
 - Invoked via 'scl' (software collection)
 - see
https://access.redhat.com/site/documentation/enUS/Red_Hat_Developer_Toolset/1/html/User_Guide/index.html



Scientific Linux



- SL updateinfo.xml is available now for SL 6.4
 - This provides metadata for yum-plugin-security
 - Provides for easy CVE search
 - Provides a description of the update, typically with reasons for applying the update
 - Allows filtering based on severity
 - Currently only security errata
 - See example on next slide
 - Metadata nicely formatted via http interface



Scientific Linux



Browser navigation bar showing the URL: http://ftp.scientificlinux.org/linux/scientific/6x/x86_64/updates/security/repdata/updateinfo.xml. Includes search engines (Google) and a list of bookmarks: Most Visited, Scientific Linux, FEF Mediawiki, RH Errata, Koji, SLF Unpublished..., SL Unpublished ..., and Kitten Cam : Too ...

Updates for:
Scientific Linux 6

Update Information

Update ID	Title	Released	Severity
SLSA-2013:0751-1	Critical: java-1.7.0-openjdk security update	2013-04-17	critical
SLSA-2013:0753-1	Moderate: icedtea-web security update	2013-04-17	moderate
SLSA-2013:0748-1	Moderate: krb5 security update	2013-04-16	moderate
SLSA-2013:0742-1	Low: 389-ds-base security update	2013-04-15	low
SLSA-2013:0737-1	Moderate: subversion security update	2013-04-12	moderate
SLSA-2013:0714-1	Moderate: stunnel security update	2013-04-08	moderate
SLSA-2013:0696-1	Critical: firefox security update	2013-04-02	critical
SLSA-2013:0697-1	Important: thunderbird security update	2013-04-02	important
SLSA-2013:0689-1	Important: bind security update	2013-03-29	important
SLSA-2013:0685-1	Moderate: perl security update	2013-03-27	moderate
SLSA-2013:0687-1	Moderate: pixman security update	2013-03-27	moderate
SLSA-2013:0668-1	Moderate: boost security update	2013-03-21	moderate
SLSA-2013:0669-1	Moderate: qt security update	2013-03-21	moderate
SLSA-2013:0663-1	Moderate: sssd security update	2013-03-19	moderate
SLSA-2013:0656-1	Moderate: krb5 security update	2013-03-18	moderate
SLSA-2013:0567-1	Important: kernel security update	2013-03-14	important
SLSA-2013:0630-1	Important: kernel security update	2013-03-14	important
SLSA-2013:0646-1	Moderate: pidgin security update	2013-03-14	moderate
SLSA-2013:0623-1	Critical: tomcat6 security update	2013-03-12	critical



Scientific Linux



```
]# yum info-sec
```

Security ERRATA Important: openjpeg on SL6.x i386/x86_64

Update ID : SLSA-2012:1283-01

Release: Scientific Linux

Type : security

Status : final

Issued : 2012-09-17

Bugs : 842918 - openjpeg: heap-based buffer overflow

CVEs : CVE-2012-3535

Description : OpenJPEG is an open source library for reading and writing image
: files in JPEG 2000 format. It was found that OpenJPEG failed to
: sanity-check an image header field before using it. A remote attacker
: could provide a specially-crafted image file that could cause an
: application linked against OpenJPEG to crash or, possibly, execute
: arbitrary code. (CVE-2012-3535). All running applications
: using OpenJPEG must be restarted for the update to take effect.

Severity : important



Scientific Linux

The Past Six Months



- Security updates continually released for all supported versions
 - SL 6.4 security repo now supports updateinfo.xml
- Fastbugs updates consistently released weekly for latest versions of SL 5 and SL 6



Scientific Linux

The Past Six Months



- Security updates continually released for all supported versions
 - SL 6.4 security repo now supports updateinfo.xml
- Fastbugs updates consistently released weekly for latest versions of SL 5 and SL 6

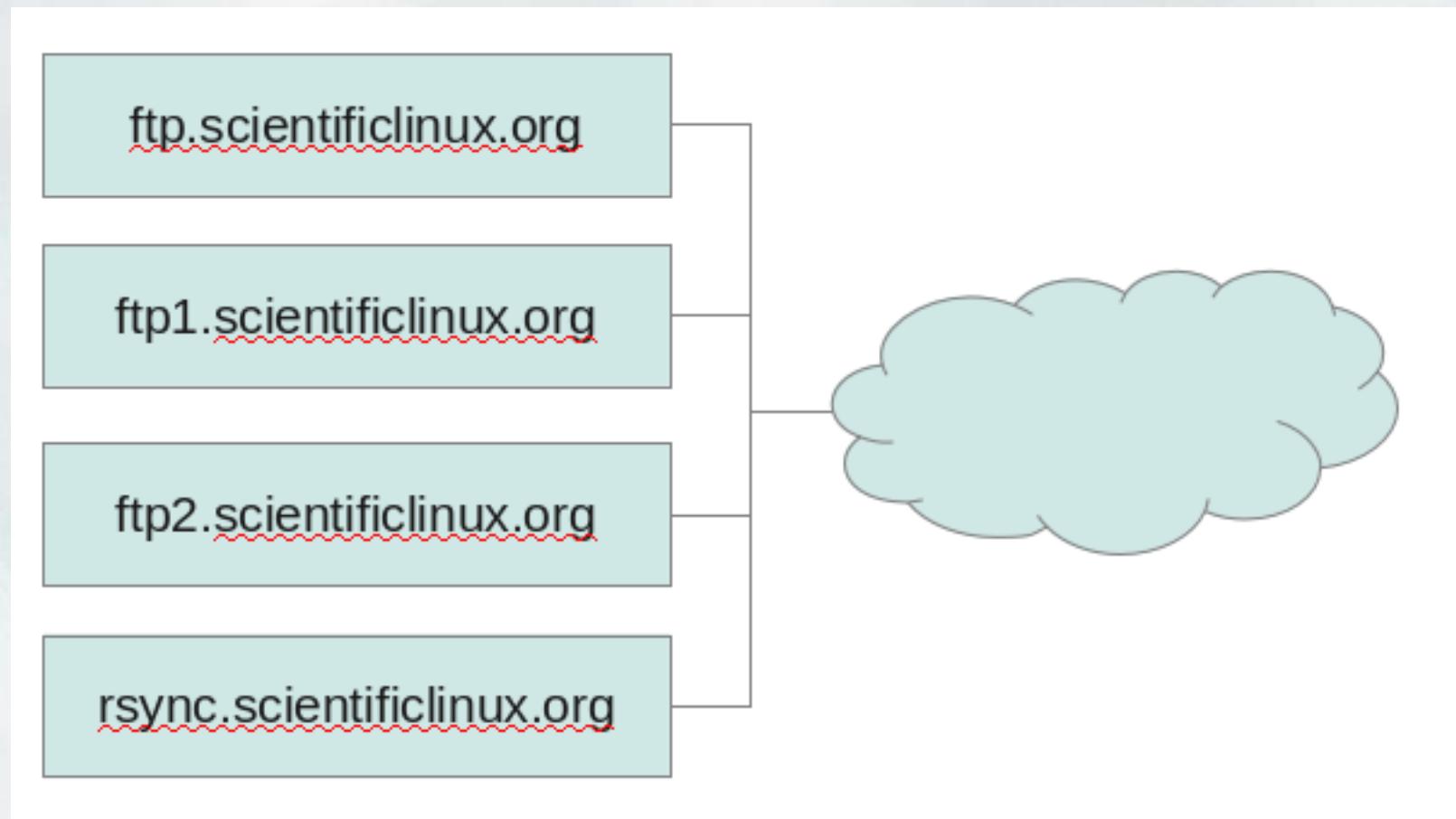


Scientific Linux

Distribution Servers



- Old model





Scientific Linux

Distribution Servers



- Old shortcomings
 - Some systems are overloaded while others are underutilized
 - Single system outages significantly impact the user community
 - Adding new systems requires changes to yum repos or removing existing systems
 - Existing systems are getting old
 - 1 x 1GB ethernet interface used

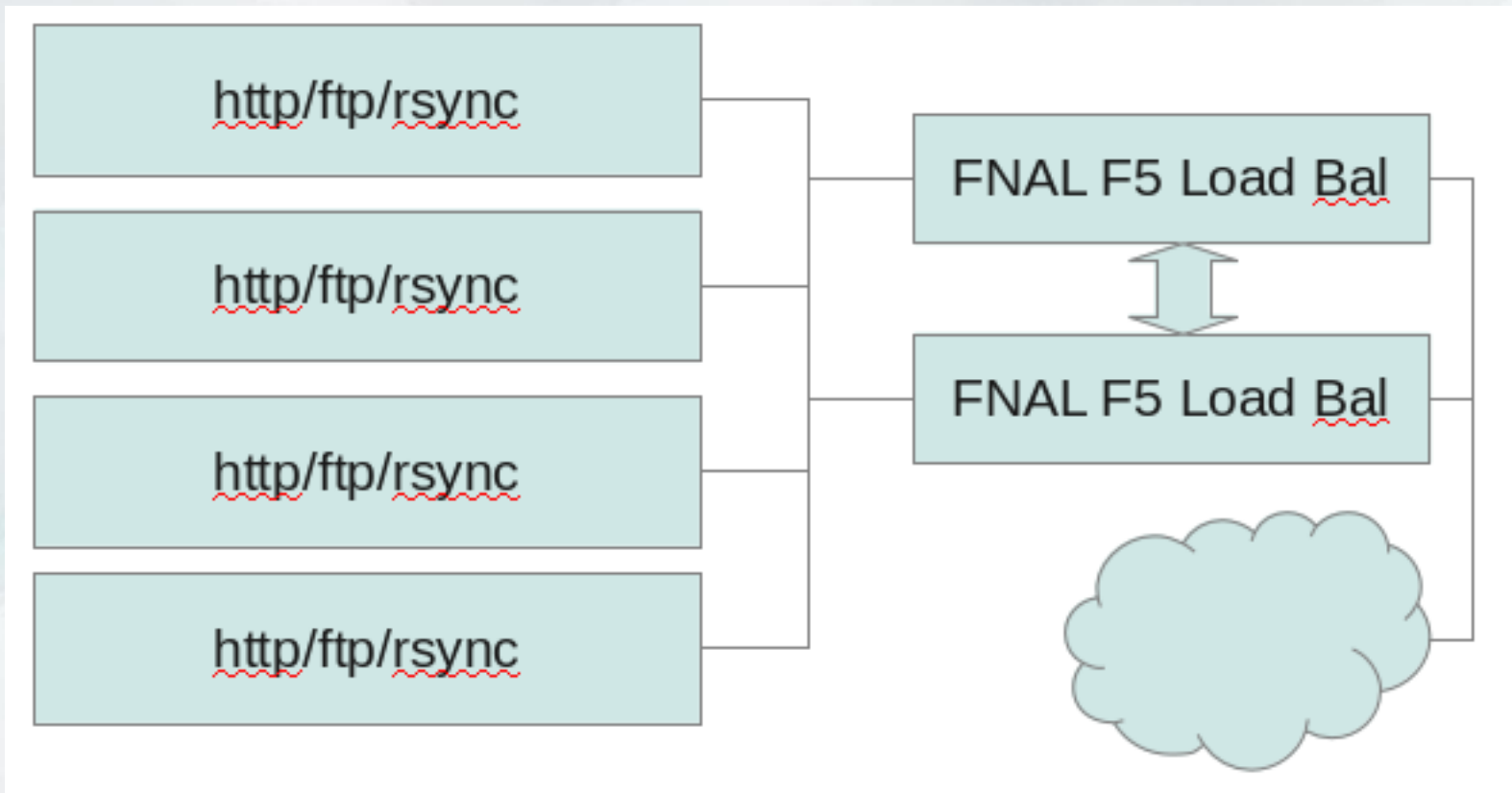


Scientific Linux

Distribution Servers



- New model





Scientific Linux

Distribution Servers



New model added benefits

- Systems should be equally utilized, no one system will carry all the weight
- Single system outages should be transparent
- Additional systems can be added or removed without interfering with the community
- More physically distributed
 - Currently the distribution servers are in one room
 - With the new plan the systems are in multiple data centers
- Newer hardware
 - More memory
 - 2 x 1GB ethernet interfaces used
 - 1 BlueArc Backing store , 1 to internet



Scientific Linux

Distribution Servers



- Still under investigation
 - Caching
 - The actual distribution files are kept on an NFS share and provided to each distribution server.
 - This may be a large performance bottleneck as files must always be fetched from the share.
 - Researching mirrorbrain
 - redirects to mirrors based on config settings
 - allows for us to still get statistics
 - offloads to local mirrors



Scientific Linux

Distribution Servers



- Caching
 - Squid
 - Pros
 - Proven track record
 - Lots of local expertise
 - Cons
 - HTTP only, can't accelerate ftp or rsync
 - Requires http source to cache from
 - fscached, does it work?
 - Pros
 - Accelerates all protocols
 - Trivial configuration
 - Cons
 - Technology Preview
 - Not a lot of history, unknown future



Scientific Linux

What we see in the future



- Continue to have security updates for all releases of SL 5 and 6.
- Continue to have fastbug updates for only the latest releases of SL 5 and 6.



Scientific Linux

Discussion topics



- SL 7 – expected 2013
 - Default to 7x rather than 7.0, 7.1, et al.
 - Plan on supporting UEFI Secure Boot via “Fedora Method” as expected to be RHEL 7 method
- Point releases?
 - Yes
 - contains lots of long term maintenance concerns, and possible errata issues
 - No
 - is different than we've done things before
 - Discuss on scientific-linux-devel



Scientific Linux

Discussion / Questions



- Discussion
- Other Questions?



Scientific Linux

References



- <http://www.scientificlinux.org/>
- <http://www.scientificlinux.org/download/mirrors>
- <http://www.livecd.ethz.ch/>
- <https://www.redhat.com/licenses/>
- https://www.redhat.com/licenses/rhel_us_appendix1.pdf
- https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Developer_Toolset/1/pdf/User_Guide/Red_Hat_Developer_Toolset-1-User_Guide-en-US.pdf