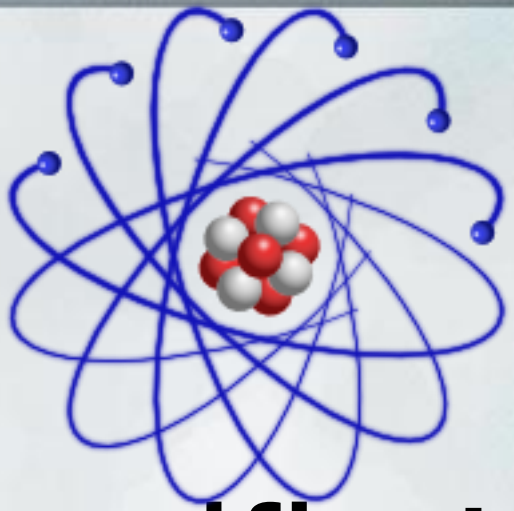


Scientific Linux Infrastructure Changes

Connie Sieh
csieh@fnal.gov
Pat Riehecky
riehecky@fnal.gov

Hepix Fall 2012

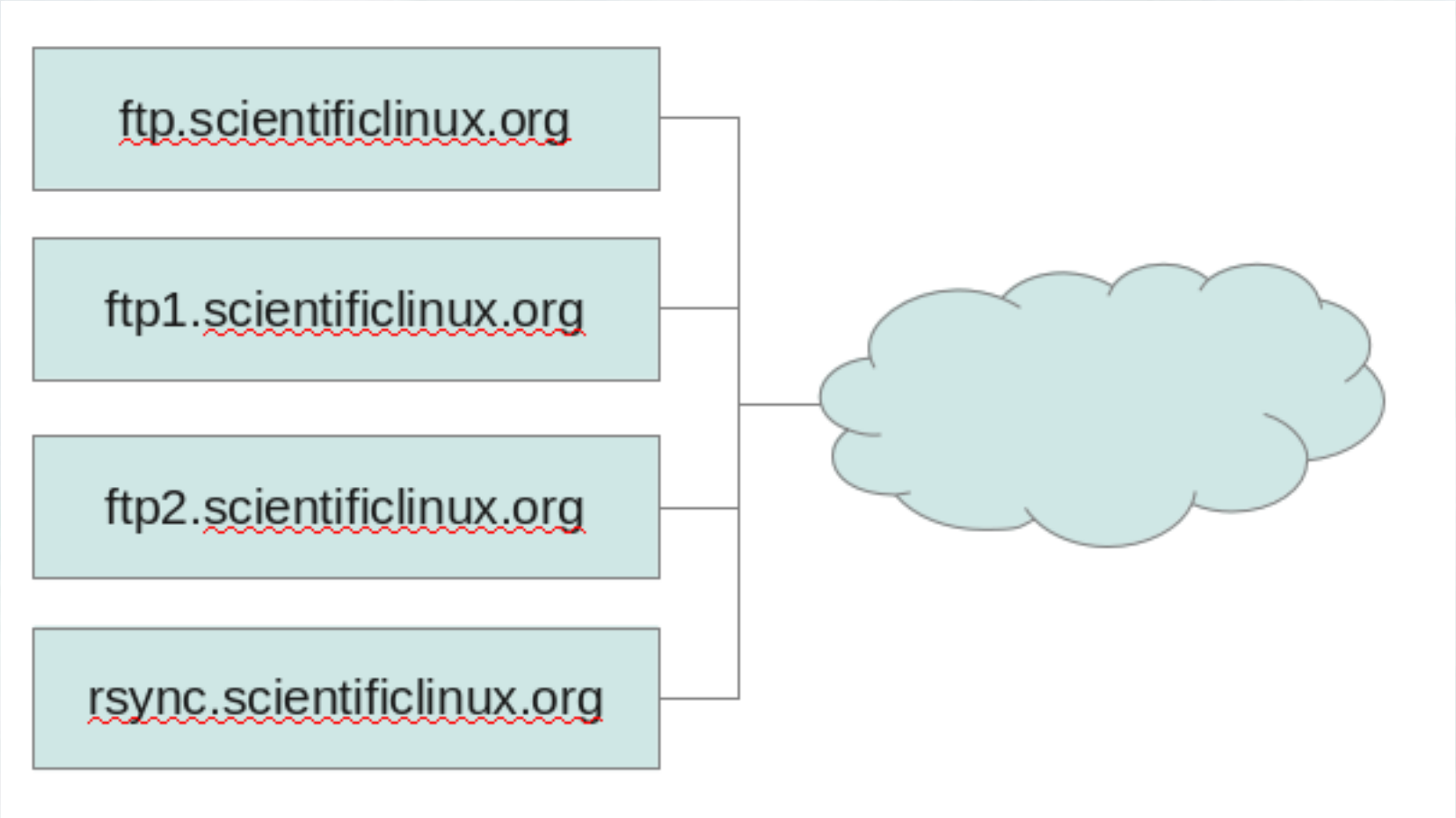
Oct 15, 2012

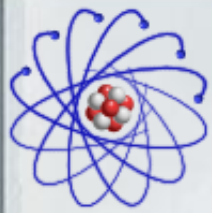
Scientific Linux

- Presentation Overview
  - Distribution Server updates
  - Evaluating Webserver Infrastructure
  - Listserv changes
  - Errata publish changes
  - Packages DB

Scientific Linux
Distribution Servers

- Current model



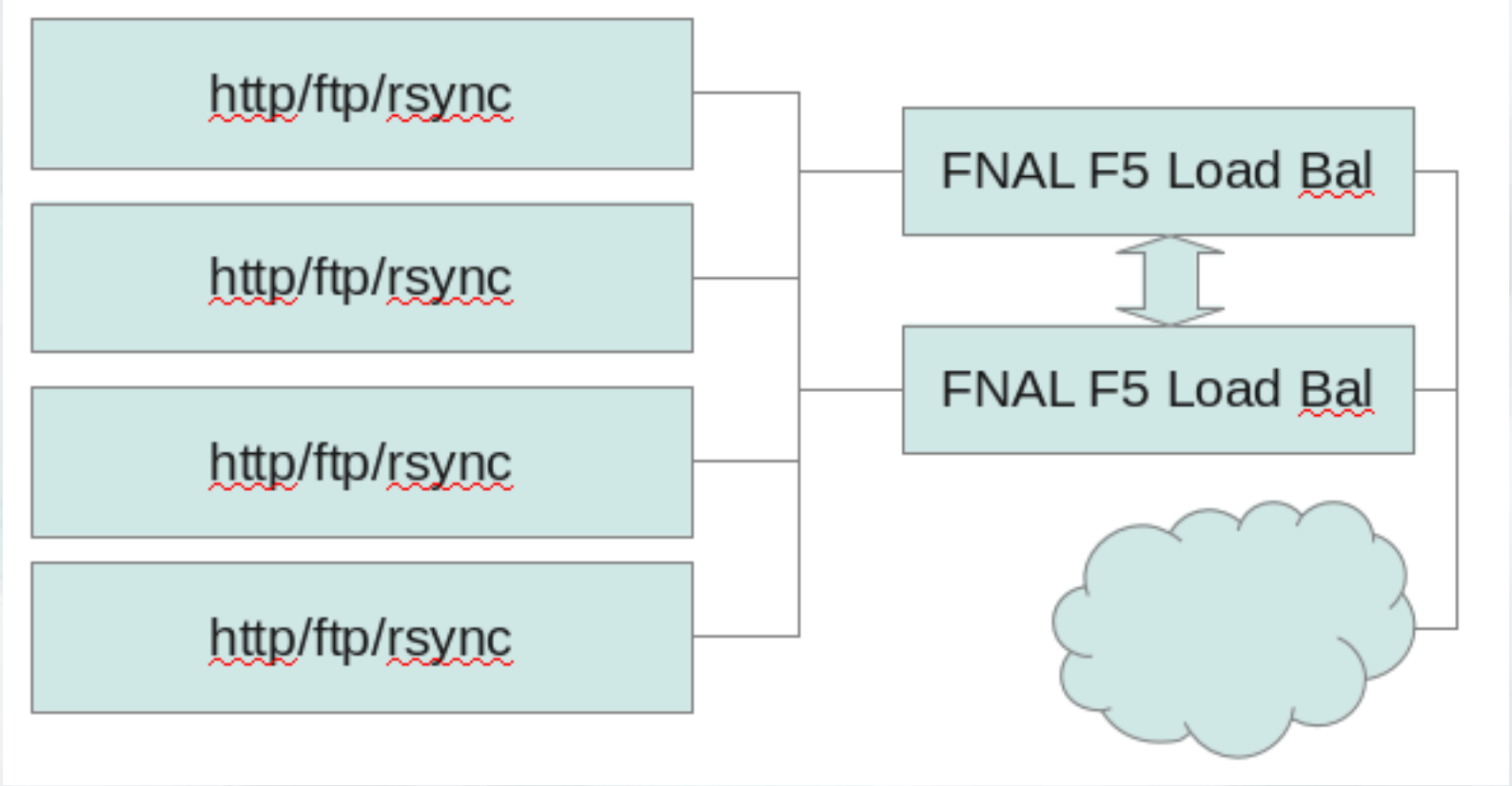


Scientific Linux
Distribution Servers

- Current 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

Scientific Linux
Distribution Servers

- New Plan

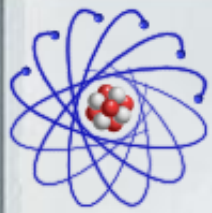


Scientific Linux
Distribution Servers

- New 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 we expect to have systems in multiple data centers
  - Plans are in motion
    - new systems are on-site and being installed

Scientific Linux
Distribution Servers

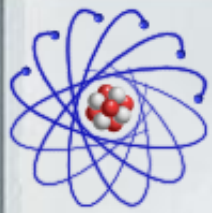
- Still under investigation
  - Caching
    - The actual distribution files are kept on an NFS share and provided to each distribution server.
      - This may be a large performance bottleneck as files must always be fetched from the share.
  - Load testing plan
    - We serve about 9000 requests per hour from IP addresses all over the world.



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

Distribution Servers

- Load testing
  - Plan to get help from FNAL users for load generation
  - Distributed testing requires coordinated effort
    - Tests need to happen when we can monitor them
    - Tests need to happen when we can troubleshoot problems
    - Tests need to stop happening when we are done testing
  - Expect to use 'ab' for HTTP testing
    - What tools for ftp or rsync?

Scientific Linux

Evaluating Webserver Infrastructure

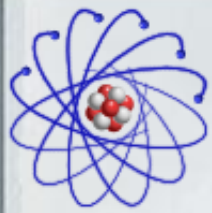
- Our current plone instance at www.scientificlinux.org is beginning to show its age
  - Somewhat frequent outages
  - Difficult to automate posts
  - No redundancy
  - Organic growth of content

- Looking for new content management software that will
  - Let us automate posts
  - Generate automatic content
  - Allow authentication with KCA certs from FNAL
  - Be 'clusterable' for redundancy

Scientific Linux
listserv changes

- The list of invalid subscribers is growing
  - About 100 invalid subscribers on scientific-linux-users
  - About 300 invalid subscribers on scientific-linux-errata

- We've been testing automated unsubscription on internal lists for 4 months
  - Only removing people who constantly bounce emails
  - No unexpected removals
  - We will not institute 'bans' on bad addresses. Users are free to re-subscribe instantly.
  - Exact conditions for unsubscription are still being determined
  - Changes will be announced in detail before they go into effect



Scientific Linux

Errata Publishing changes

- A complete Django application has replaced the PHP/MySQL proof of concept tool.
  - Application by Bonnie King
- Moved to Django for
  - Greater simplicity in customization
  - Ease of adding functionality
  - Easier long term maintenance
  - Greater familiarity with Python
  - Easy web admin interface
  - Easy to build user web pages
  - Automated database design
  - Integrated ORM (Object Relationship Model)
  - Large community plugin base

Scientific Linux

Errata Publishing changes

- This should result in greater consistency for errata announcements
- We now have a database for tracking some information about what was released when
- Can query this database for aspects of 'updateinfo'
  - Package -> Errata ID -> Description

- This is the first step towards a unified packages database

Scientific Linux

Errata Publishing changes

```
]# 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

Errata Publishing changes

- Sample internal only pages

hello, riehecky! SL RSS SLF RSS

RHSA_ID	Received Date	Urgency	Package	Published SL
RHSA-2012:1350-01	2012-10-09	Critical	firefox	YES
RHSA-2012:1351-01	2012-10-09	Critical	thunderbird	YES
RHSA-2012:1326-01	2012-10-03	Moderate	freeradius	YES
RHSA-2012:1323-01	2012-10-02	Important	kernel	YES
RHSA-2012:1327-01	2012-10-02	Moderate	freeradius2	YES
RHSA-2012:1304-01	2012-09-25	Moderate	kernel	YES
RHSA-2012:1269-01	2012-09-19	Moderate	qpid	YES
RHSA-2012:1288-01	2012-09-18	Moderate	libxml2	YES
RHSA-2012:1283-01	2012-09-17	Important	openjpeg	YES

RHSA-2012:1350-01: firefox

Published in SL: Oct. 10, 2012
Published in SLF: NO
fix publish dates
add/remove RPMs

Urgency: Critical
Date Received: Oct. 9, 2012

CVEs:
CVE-2012-1956
CVE-2012-3982
CVE-2012-3986
CVE-2012-3988
CVE-2012-3991
CVE-2012-3994
CVE-2012-3993
CVE-2012-4184
CVE-2012-3992
CVE-2012-3995
CVE-2012-4179
CVE-2012-4180
CVE-2012-4181
CVE-2012-4182
CVE-2012-4183
CVE-2012-4185
CVE-2012-4186
CVE-2012-4187
CVE-2012-4188
CVE-2012-3990

Bugzillas:
851912, 863614, 863618, 863619, 863621, 863622, 863623, 863624, 863625, 863626, 863628,

ss back to list

SL BODY

SLF body
original email from Red Hat

Security ERRATA Critical: firefox on SL5.x, SL6.x i386/x86_64

```
Synopsis:          Critical: firefox security and bug fix update
Issue Date:        2012-10-09
CVE Numbers:       CVE-2012-1956
                   CVE-2012-3982
                   CVE-2012-3986
                   CVE-2012-3988
                   CVE-2012-3991
                   CVE-2012-3994
                   CVE-2012-3993
                   CVE-2012-4184
                   CVE-2012-3992
                   CVE-2012-3995
                   CVE-2012-4179
                   CVE-2012-4180
                   CVE-2012-4181
                   CVE-2012-4182
                   CVE-2012-4183
                   CVE-2012-4185
                   CVE-2012-4186
                   CVE-2012-4187
                   CVE-2012-4188
                   CVE-2012-3990
--

Mozilla Firefox is an open source web browser. XULRunner provides the XUL
Runtime environment for Mozilla Firefox.

Several flaws were found in the processing of malformed web content. A web
page containing malicious content could cause Firefox to crash or,
potentially, execute arbitrary code with the privileges of the user running
Firefox. (CVE-2012-3982, CVE-2012-3988, CVE-2012-3990, CVE-2012-3995,
CVE-2012-4179, CVE-2012-4180, CVE-2012-4181, CVE-2012-4182, CVE-2012-4183,
CVE-2012-4185, CVE-2012-4186, CVE-2012-4187, CVE-2012-4188)
```

Scientific Linux

PackagesDB

- Full inventory of all packages in SL
  - When was it released?
  - When was it updated?
  - Was it ever removed?
    - Why?
  - What sort of package is it?
    - Security? Fastbug?
    - Who says? Upstream or SL?
  - This is the real datasource for updateinfo
    - (once it exists)
  - Track all security updates, fastbugs, releases
    - Should allow us to build a very comprehensive set of release notes.
  - Internal use

Scientific Linux
PackagesDB

- Data source challenges
  - Historical release dates for fastbugs are not always accurate
  - Description information for non-security errata has restrictions on use
  - SL-created packages don't have an explicit history we can query

Scientific Linux

Discussion / Questions

- Discussion
- Other Questions?