

# The Linux Standard Desktop Build @LLNL

Title: Linux Standard Build @LLNL

UCRL: UCRL-PRES-231384

Author: Kevin Simmons

Issued: June 1, 2007

Presented: June 12, 2007, Albuquerque, NM

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.





# Linux Standard Build @LLNL

- What is uLoad?
- How does uLoad work?
- Components



# What is uLoad?

In a word...

The Linux Standard Build, or uLoad, is an institutionally supported standard configuration for the Linux desktop / workstation. Its security configuration is based on the Center for Internet Security (CIS) for National Institute of Standards and Technology (NIST) compliance. It also complies with LLNL security policies and Certification and Accreditation requirements.

It will be used as an OS option when purchasing a standard desktop / notebook hardware. The uLoad integrates with LLNL institutional services such as:

- Active Directory for authentication, authorization, and policy deployment
- Red Hat Network for patching, SW package deployment, and inventory
- LANDesk for inventory and Certification and Accreditation (C&A).



# What is uLoad?

- Red Hat Enterprise Linux 4 – Work Station
- Plus some *extra* packages
- NIST/CIS/LLNL Fortification & Scanning
  - National Institute of Standards and Technology
  - Center for Internet Security
- Integration with Institutional Tools
  - Red Hat Network (RHN) - patching, SW distribution
  - Active Directory - authentication, authorization, policies
  - LANDesk – Inventory, CnA scanning and reporting



# How does uLoad work?

- Network based installation
- Kickstart
  - Easily maintained through web interface
  - Custom profiles possible
  - RHN Satellite servers at LLNL
  - RHN Satellite Proxies support multiple networks
- Launch install from various media
  - DVD/CD/USB currently
  - Working with vendors to offer through EOS



# Components

## Kickstart Server

- Kickstart from RHN Satellite Servers @ LLNL
  - Web-form based kickstart creation
    - No need to build the Software tree, just select from supported channels.
    - Handles GPG Keys, SSL certs, and initial configuration
    - %post is where the magic happens
      - We try to package *everything*



# Components

## Boot media

- Custom boot DVD/CD
  - Networked based http kickstart
    - NOT DHCP (not available at LLNL)
  - Multiple Profiles (RHEL4/5, package selection, arch)
  - Helps with install but is not necessary
    - Any RH Install disk should work
- Working with our HW resellers to install on supported systems for our Electronic Order System



# Components

## Installation Process

- After launch from DVD, only prompted once during process
  - disk partitioning
    - defaults to flexible partitioning scheme, LVM
- Thirty minute install



# Components

Post installation

Firstboot



# firstboot

- Welcome
- Root Password (m)
- GRUB Password
- AD Joiner
- RHN Registration
- Sound Card
- Finish Setup



## Welcome - LLNL Firstboot

There are a few more steps to take before your system is ready to use. The Setup Agent will now guide you through some basic configuration. Please click the "Next" button in the lower right corner to continue.

NOTE: Mandatory items are marked with an (m).

(Use ctrl-alt-keypad+ or keypad- to cycle through possible display resolutions, if needed. Laptops may need to use the Fn key to access the keypad+/-.)



Red Hat **Enterprise Linux**  
**LLNL Standard Build**





# firstboot

Welcome

▸ Root Password (m)

GRUB Password

AD Joiner

RHN Registration

Sound Card

Finish Setup



## Root Password (m)

Please set the root password for the system.

Root Password:

Confirm:

◀ Back

▶ Next



# firstboot

Welcome

Root Password (m)

→ GRUB Password

AD Joiner

RHN Registration

Sound Card

Finish Setup



## GRUB Password

Please set the grub password for the system.

GRUB Password:

Confirm:

◀ Back

▶ Next



# firstboot

Welcome

Root Password (m)

GRUB Password

→ AD Joiner

RHN Registration

LANDesk Integration

Sound Card

Finish Setup

## AD Joiner

You may use this form to use the VAS/VGP software to join this computer to LLNL's Active Directory. This would eliminate the need to define local user accounts (except for root). Enter the information below...

AD Admin Username:

authorized for the container specified below

Computer Name:

Domain (REALM):

Choose from drop-down list or type in.

AD Container:

ex: ou=computers,ou=unix,ou=msg,dc=the-lab,dc=llnl,dc=gov

Join...

Activating this button will launch the AD join process based on the choices from this form. You will be prompted for a password for the username given.

◀ Back

▶ Next



# firstboot

- Welcome
- Root Password (m)
- GRUB Password
- AD Joiner
- RHN Registration
- Sound Card
- Finish Setup

## RHN Registration

You may use this form to register this system to your System Group on [rhn.llnl.gov](http://rhn.llnl.gov).  
\*NOTE: This option is only available from LLNL's unclassified (yellow) networks.

RHN System Group:

ex: DPT\_XXXX (case insensitive)

RHN Admin User:

Enter a valid rhn user authorized for the above group

Register...

Activating this button will launch the RHN registration process based on the choices from this form. Please contact [rhn.llnl.gov](http://rhn.llnl.gov) if assistance is needed.

◀ Back

▶ Next



# firstboot

Welcome

Root Password (m)

GRUB Password

AD Joiner

RHN Registration

▶ LANDesk Integration

Sound Card

Finish Setup

## LANDesk Integration

This module gives you the ability to install either the full LANDesk Linux Agent for use with the Institutional core servers, or, simply the CnA scripts for use with your own LANDesk Linux Agent for your departmental LANDesk servers.

Launch Institutional LANDesk Linux Agent Installer...

Launch Departmental LANDesk LLNL Customizations Installer...

>>Choose the top button for installing the Institutional LANDesk Agent for use with the Institutional LANDesk Core Servers. This option includes the Linux Agent plus the CnA scanning scripts.

>>Choose the bottom button to launch the Departmental LANDesk LLNL Customizations Installer. This includes the CnA scanning scripts for use with YOUR department's LANDesk Linux Agent.

Either installer will prompt you for location information.

◀ Back

▶ Next



# firstboot

Welcome

Root Password (m)

GRUB Password

AD Joiner

RHN Registration

Sound Card

› Finish Setup



## Finish Setup

Your system is now set up and ready to use. Please click the "Next" button in the lower right corner for an important message.



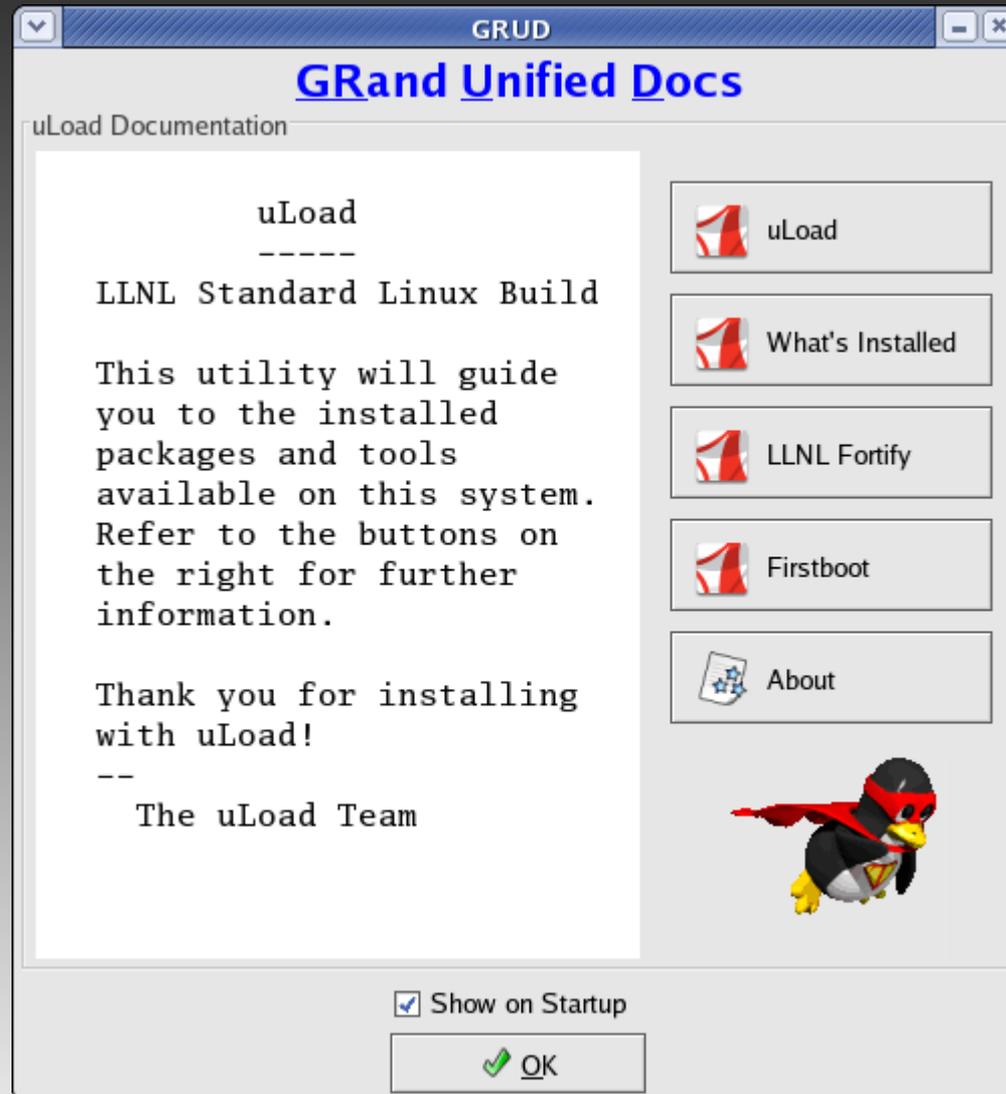
Red Hat **Enterprise Linux**  
**LLNL Standard Build**

Information

 Installation is now complete. Please be sure to maintain all security settings for continued compliance with LLNL policies. For further information, visit the SMSG web site at <http://smsg.llnl.gov/linux>. Please practice safe computing and you go have a fine day.



# firstboot





# Components

## LLNL-FORTIFY

- Based on Center for Internet Security v.1.0.3
- “fortified” after package installs during %post section of kickstart
- LLNL-wrapped scan
- Can be run silently (cron, etc)
  - Management console for interactive use
- Full documentation available upon request.



# Components

LLNL-FORTIFY

-----  
Functions  
-----

option		option	(v1.0.2-4)
-----	---- Scanning -----	-----	---- Restoration -----
ss	normal System Scan	pr	Prepare Restore
ds	Deep System Scan	sr	Show Restore
rs	Result of last Scan	dr	Do Restore (pr first)
-----	---- Fortification -----	-----	---- Cleaning -----
df	Dry-run make Fortified	pc	Prepare Cleaning (purge)
mf	Make Fortified	sc	Show Cleaning
sf	Show Fortification log	dc	Do Cleaning (pc first)
-----	----- Miscellaneous -----	-----	-----
vm	toggle Verbose Menu	on	Operational Notes
q	Quit.		

FORTIFIED on Thu Mar 29 18:08:25 PDT 2007

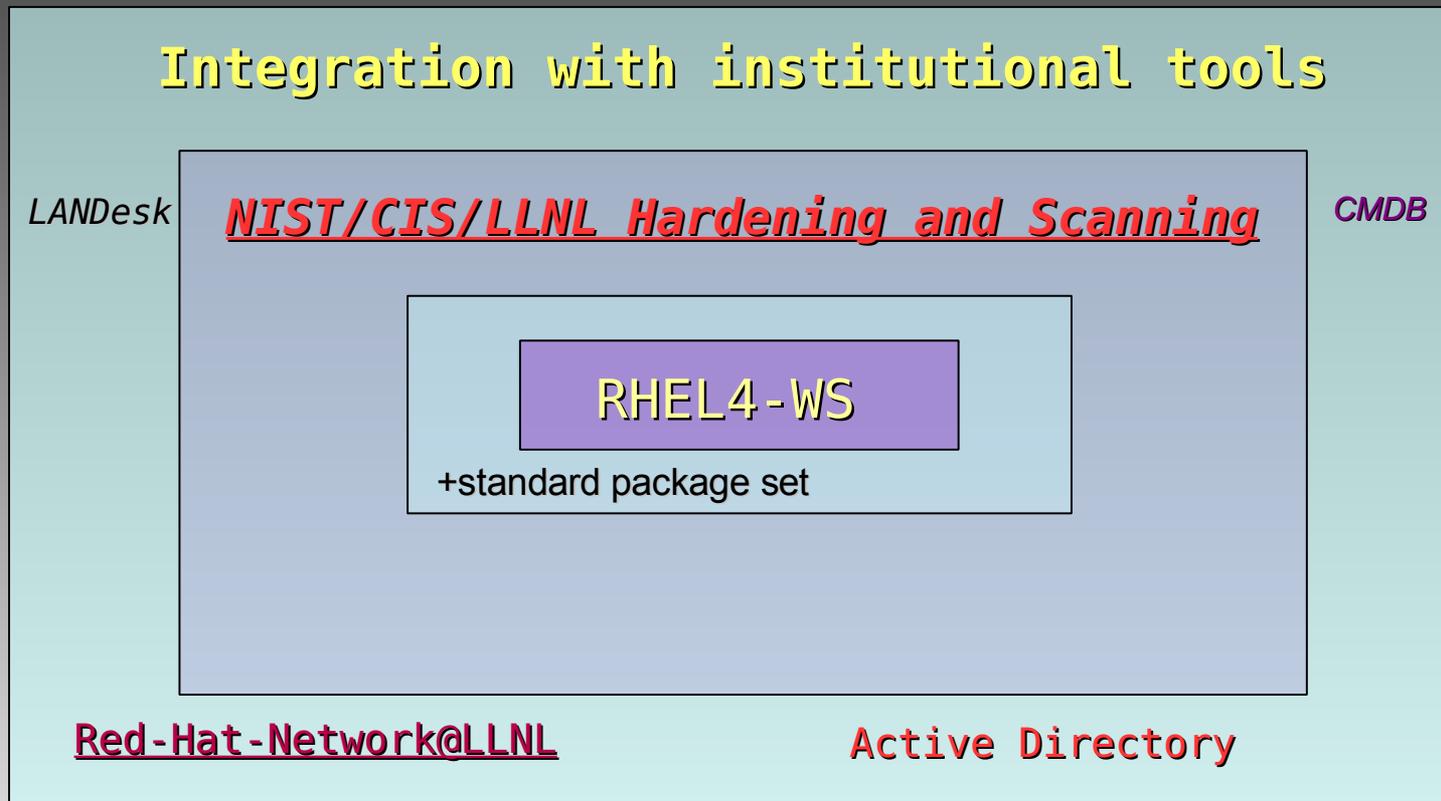
-----

-->



# The result...

## Linux Standard Build



# futures...

- LLNL-FORTIFY scanning result upload to central reporting database
  - optional automatic hardening
- LLNL PKI integration
- RHEL5 support
- Departmental build customizations (possibly)