Anatomy of Fedora Kiosk Mode

FOSS.MY 2008
Kuala Lumpur, Malaysia

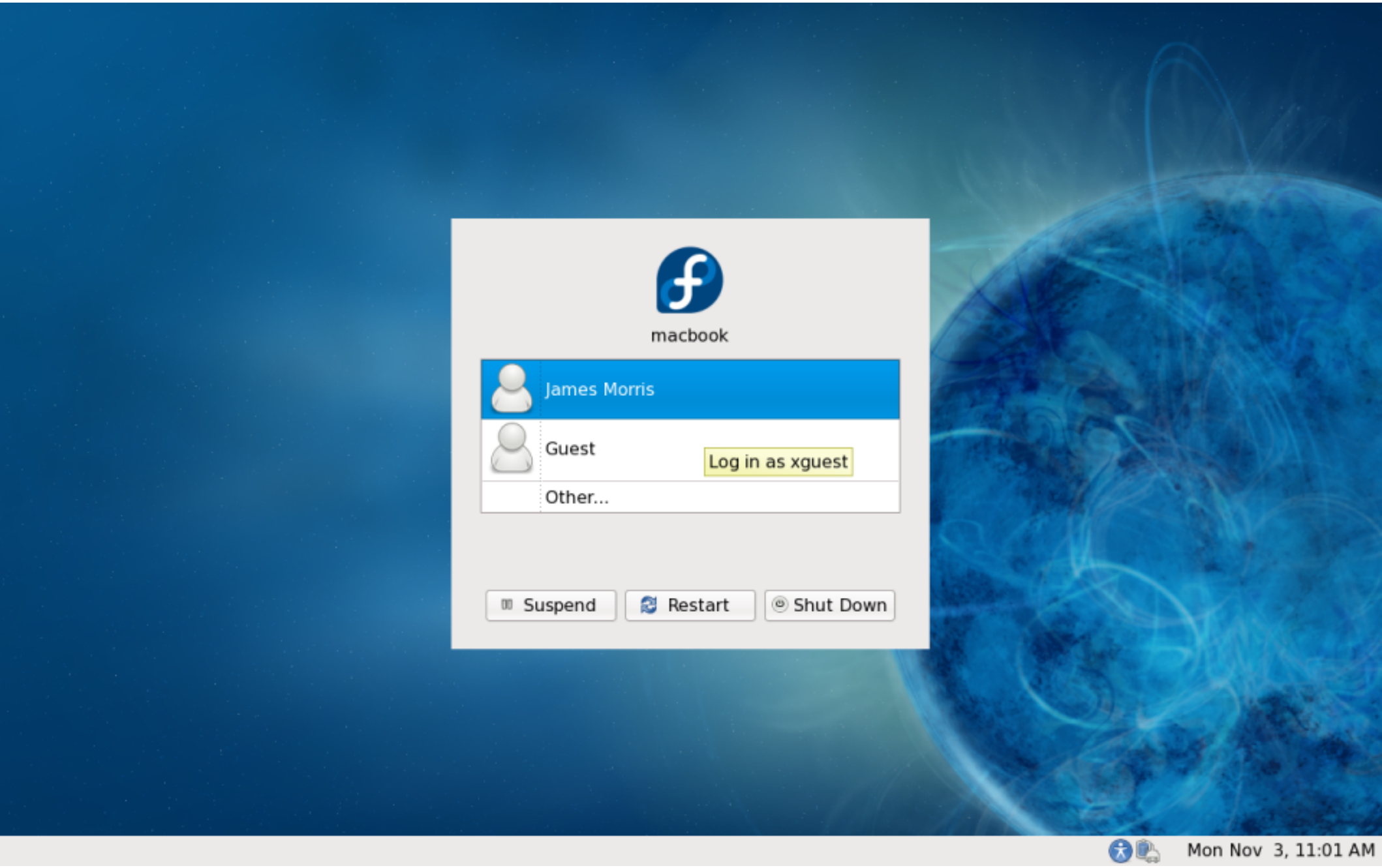
James Morris
jmorris@namei.org

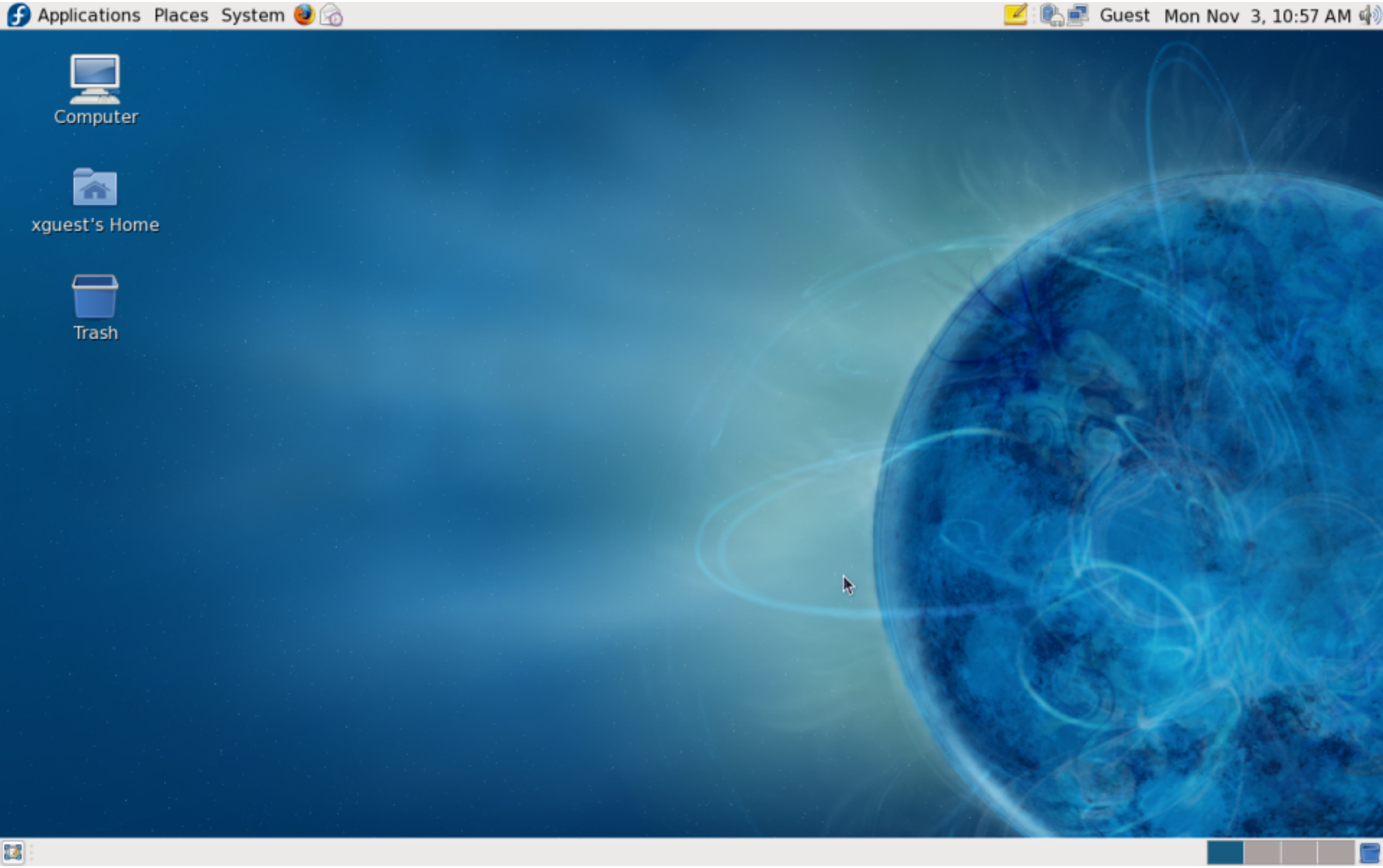
Overview

- Kiosk Mode
  - Anonymous desktop user
  - Access desktop apps and browser
  - Useful for libraries, conferences, product demos, protecting laptop from small children etc.

Installation and Configuration

```
$ sudo yum install xguest
```


macbook
James Morris
Guest
Log in as xguest
Other...
Suspend
Restart
Shut Down
Mon Nov 3, 11:01 AM


Applications
Places
System
Guest
Mon Nov 3, 10:57 AM
Computer
xguest's Home
Trash

Demo

Components

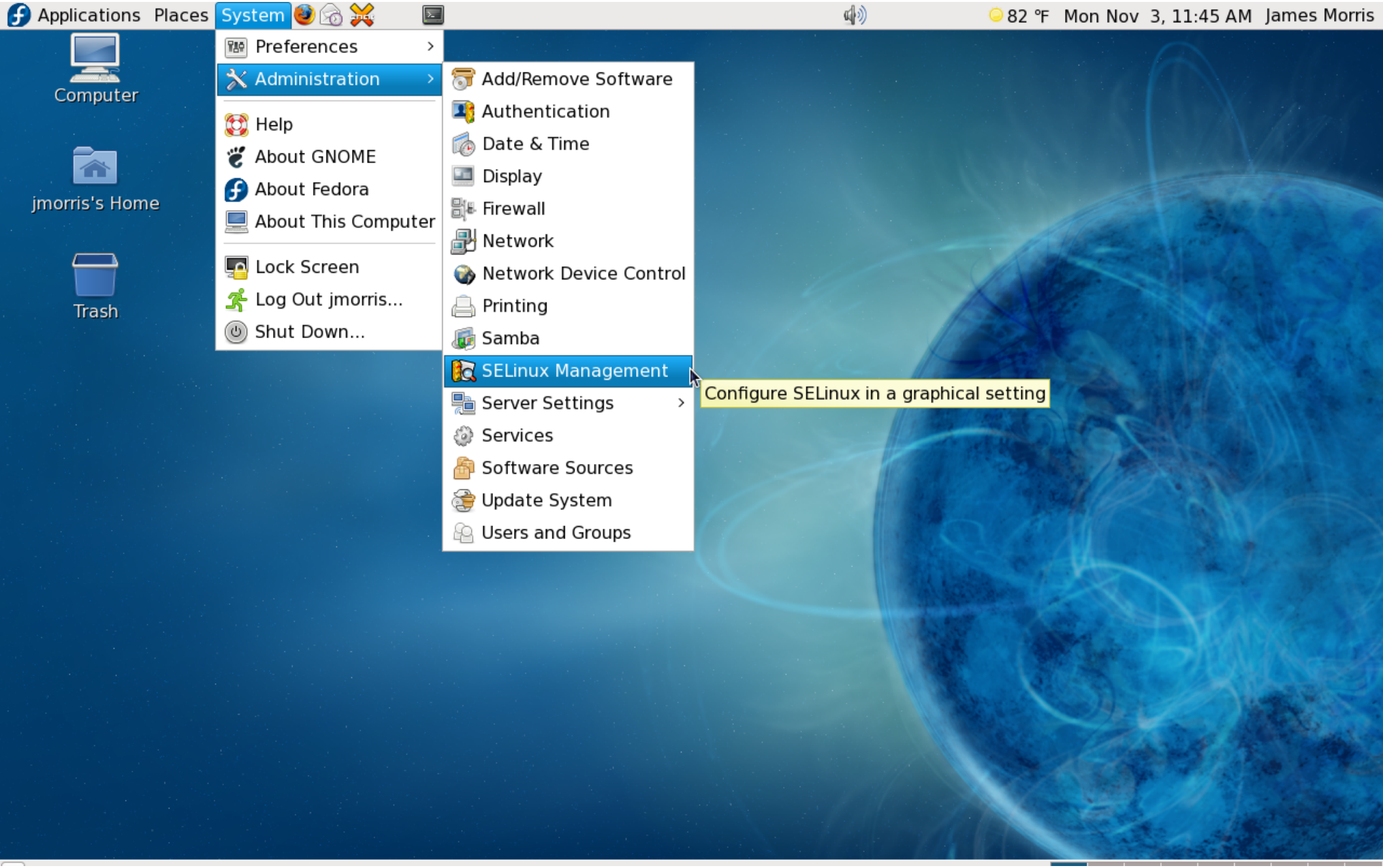
- SELinux
- Linux Namespaces
- Pluggable Authentication Modules
- Sabayon

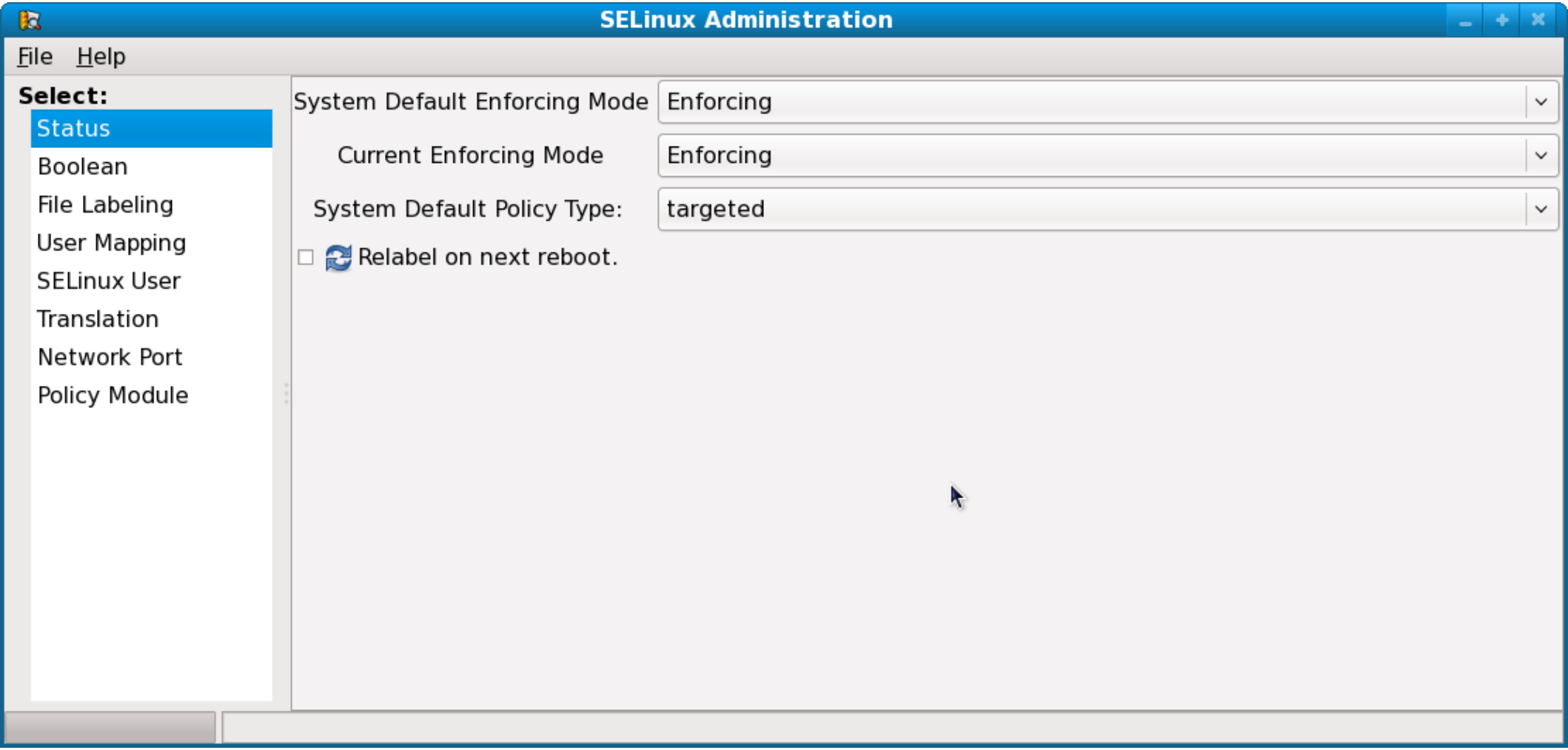
SELinux Overview

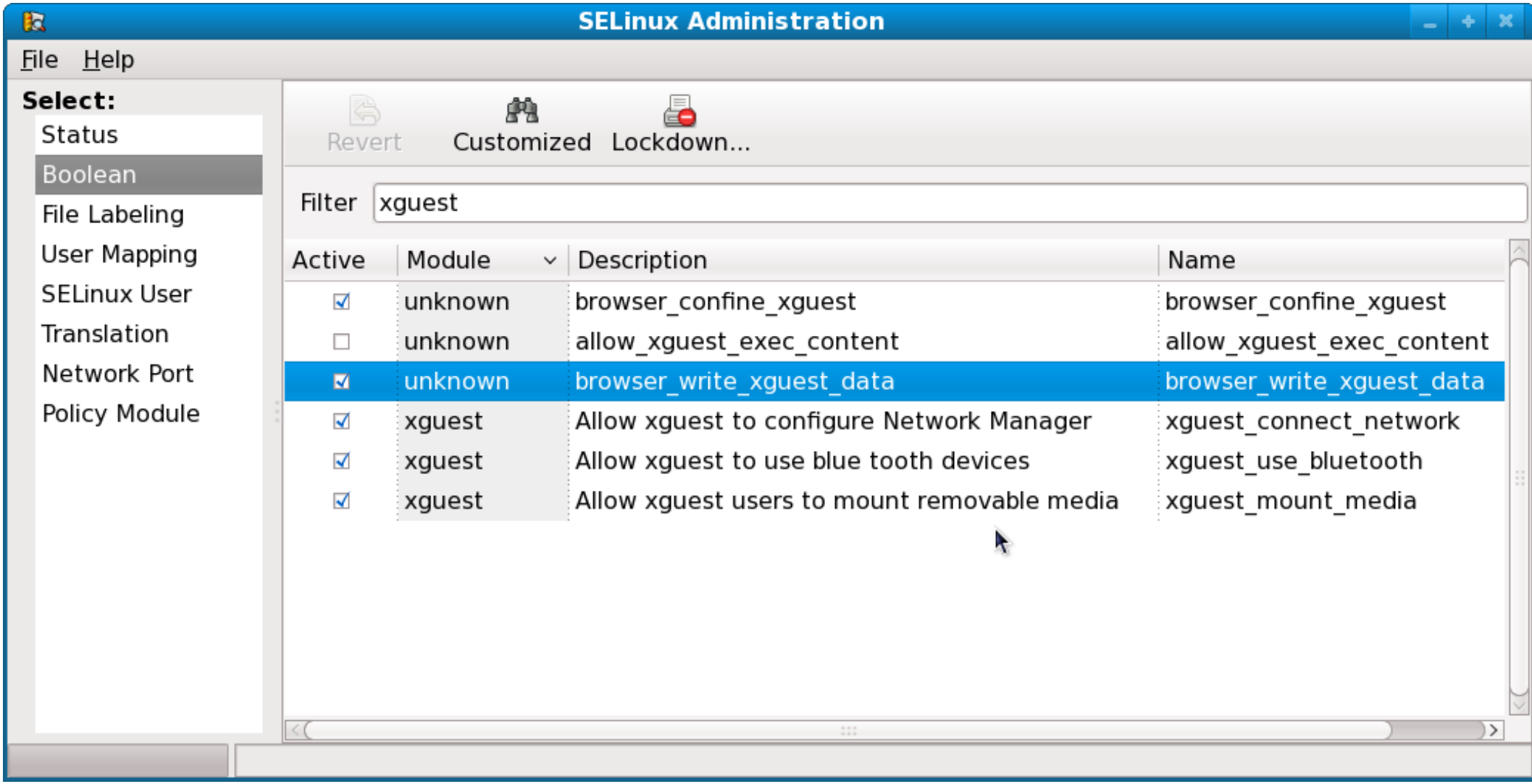
- Mandatory Access Control (MAC)
- Fine-grained and flexible security policy
- Separation of mechanism and policy
- Protects integrity of base system
- Mitigates software vulnerabilities
- Typically protects system from external threats

SELinux Policy for Kiosk Mode

- Protect system from user
- Allow only what is required:
  - GDM login only
  - Run desktop applications
  - Access network via browser
- Admin can tweak via GUI


Applications
Places
System
82 °F
Mon Nov 3, 11:45 AM
James Morris
Computer
jmorris's Home
Trash
Preferences
Administration
Help
About GNOME
About Fedora
About This Computer
Lock Screen
Log Out jmorris...
Shut Down...
Add/Remove Software
Authentication
Date & Time
Display
Firewall
Network
Network Device Control
Printing
Samba
SELinux Management
Server Settings
Services
Software Sources
Update System
Users and Groups
Configure SELinux in a graphical setting


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Translation
Network Port
Policy Module
System Default Enforcing Mode
Enforcing
Current Enforcing Mode
Enforcing
System Default Policy Type:
targeted
Relabel on next reboot.


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Translation
Network Port
Policy Module
Revert
Customized
Lockdown...
Filter
xguest
Active
Module
Description
Name
unknown
browser_confine_xguest
browser_confine_xguest
unknown
allow_xguest_exec_content
allow_xguest_exec_content
unknown
browser_write_xguest_data
browser_write_xguest_data
xguest
Allow xguest to configure Network Manager
xguest_connect_network
xguest
Allow xguest to use blue tooth devices
xguest_use_bluetooth
xguest
Allow xguest users to mount removable media
xguest_mount_media

Linux Namespaces

- Introduced by Al Viro, based on Plan 9 ideas
- Per-user view of filesystems
- Private by default, shared via bind mounts
- Adapted for DoD multilevel security
- ... and for Kiosk mode:
  - Private /tmp and /home
  - Remaining filesystems shared

Pluggable Authentication Modules

- Flexible authentication of applications
- Kiosk mode uses PAM for:
  - Ensuring SELinux is in enforcing mode
  - Ensuring that only one xguest session runs
  - Setting up the Linux namespaces

PAM Configuration

```
# egrep '(namespace|selinux)' /etc/pam.d/gdm
auth       [success=done ignore=ignore
 default=bad] pam_selinux_permit.so
session    required     pam_selinux.so close
session    required     pam_selinux.so open
session    required     pam_namespace.so
```

pam_sepermit

```
# grep xguest /etc/security/sepermit.conf

xguest:exclusive
```

pam_namespace

```
# cat /etc/security/namespace.conf

    pam_namespace:

    # xguest begin
    # Inserted by the xguest package.
    /tmp     tmpfs    tmpfs    ~xguest
    /var/tmp          tmpfs    tmpfs    ~xguest
    $HOME             tmpfs    tmpfs    ~xguest
```

Sabayon

- Not the Linux distro!
- GUI tool for managing desktop profiles, mandatory GConf keys etc.

- As used by Kiosk mode:
  - Installs fresh desktop in private $HOME for each session
  - Desktop state is wiped on logout when namespaces are deleted

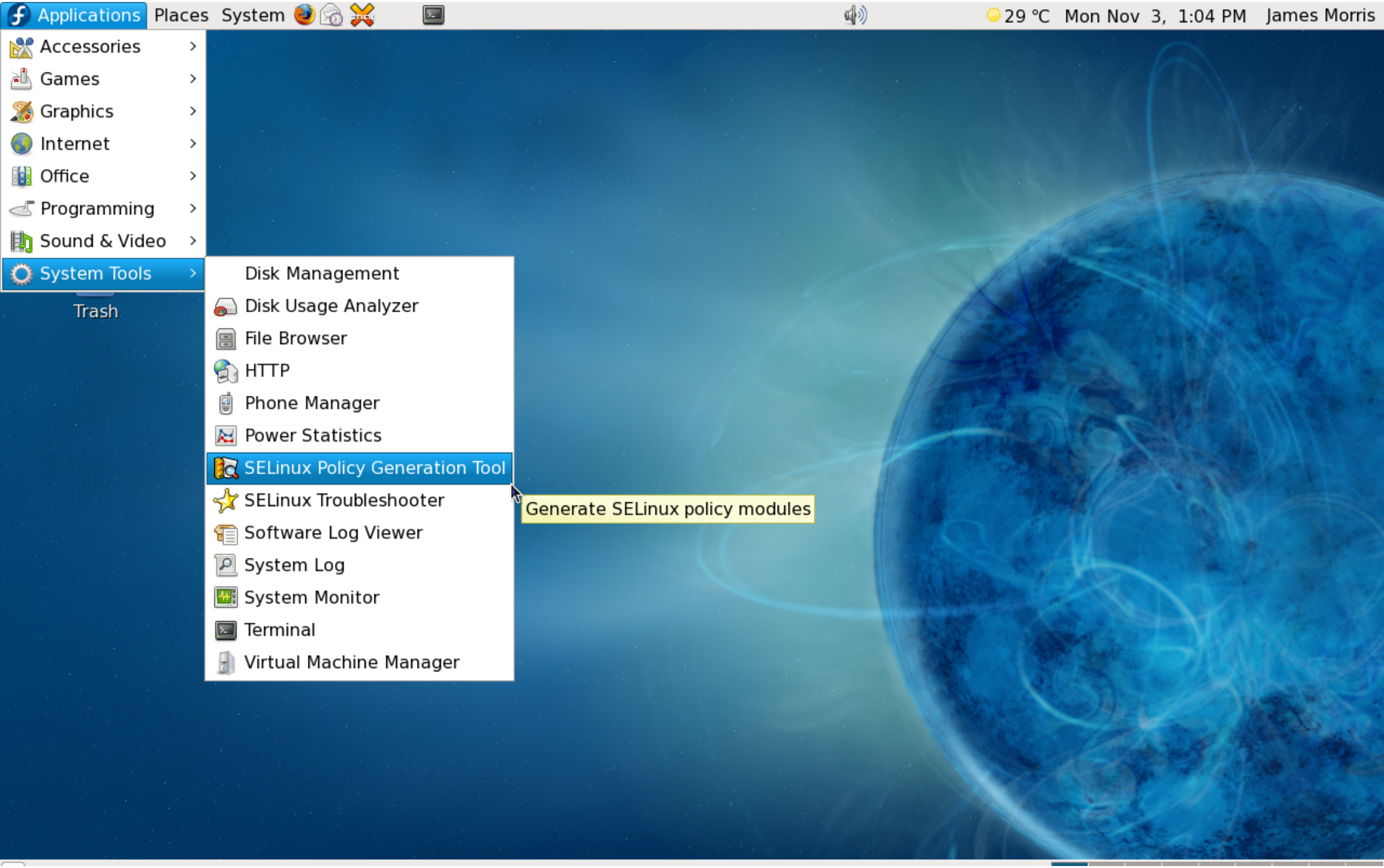
Walkthrough Summary

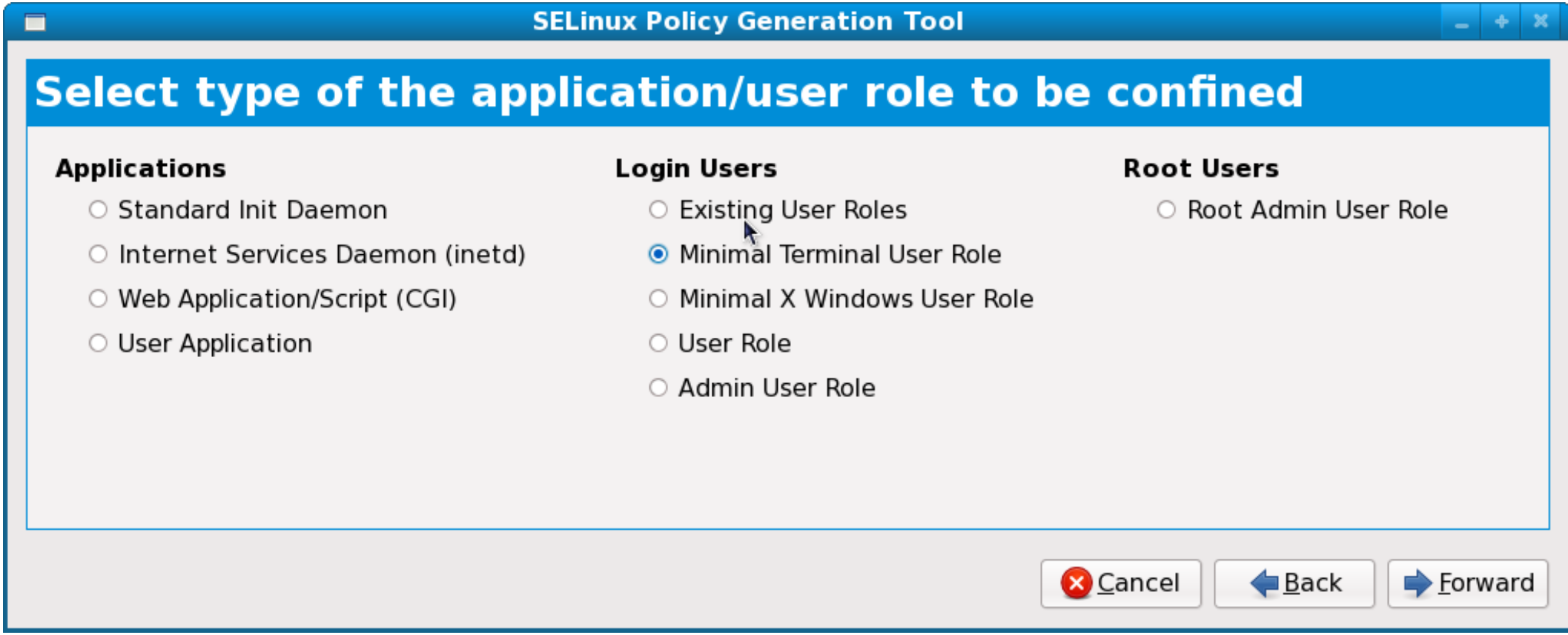
- Guest login via GDM
- PAM
  - ensures SELinux is in enforcing mode
  - ensures single session
  - configures private filesystem namespaces
- Sabayon installs fresh GNOME desktop
- SELinux isolates user with MAC security policy
- All state is destroyed on logout

Investigating Further...

- Other confined accounts:
  - guest (local terminal session)
  - staff (limited root account)

- Customization
  - Extend or develop your own confined account with GUI tool, e.g. allow developers to compile and run code


Applications
Places
System
29 °C
Mon Nov 3, 1:04 PM
James Morris
Accessories
Games
Graphics
Internet
Office
Programming
Sound & Video
System Tools
Trash
Disk Management
Disk Usage Analyzer
File Browser
HTTP
Phone Manager
Power Statistics
SELinux Policy Generation Tool
SELinux Troubleshooter
Software Log Viewer
System Log
System Monitor
Terminal
Virtual Machine Manager
Generate SELinux policy modules


SELinux Policy Generation Tool
Select type of the application/user role to be confined
Applications
Standard Init Daemon
Internet Services Daemon (inetd)
Web Application/Script (CGI)
User Application
Login Users
Existing User Roles
Minimal Terminal User Role
Minimal X Windows User Role
User Role
Admin User Role
Root Users
Root Admin User Role
Cancel
Back
Forward

Related and Future Work

- Other MAC security applications:
  - Confining desktop applications:
    - Browser plugins (already in Fedora)
    - Isolated tabs (Google Chrome + SELinux)
    - OpenOffice macros (some blocked by Kiosk mode)
  - Storage
  - Virtualization (sVirt)
  - Networking
  - Grid Computing
  - Cloud Computing

Conclusions

- Demonstrates:
  - Application of flexible MAC security for general use
  - Combining technologies to make something unexpected
  - Importance of flexible, generalized and open design
- **FOSS innovation!**

Resources

- Google knows about:
  - Dan Walsh’s blog
  - SELinux project
  - Linux mount namespaces
  - Gnome Sabayon
  - Linux PAM