# Running Fedora Linux Workstations at Scale

## Managing enterprise Linux mobile endpoints

Jonathan Billings
<jbilling@redhat.com>

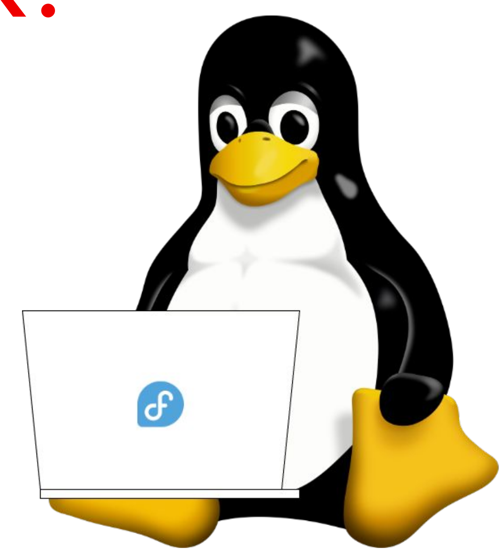
# Introduction: Jonathan Billings

- Full time Linux sysadmin since 1999
- Worked at several U.S. universities managing Linux workstations
- Long time Fedora user (and Red Hat Linux before that)
- Now working at Red Hat, in IT
- Manages the Red Hat's internal IT "Corporate Standard Base (CSB)" version of Fedora Workstation

## Topics

- Why Fedora Linux?
- Managing Linux workstations and laptops at scale
- What kind of things can be managed?
- Final thoughts

# Why Fedora Linux?



# Why Fedora?

- The Fedora Project builds a Linux Distribution that introduces the latest technologies while maintaining a good security profile
- Red Hat (my job) sponsors Fedora and a lot of employees participate in the Fedora Community
- Many employees would be running Fedora even if we didn't support it
- It's software is upstream to Red Hat Enterprise Linux, so we can test it before it hits our products

# Why Fedora?

- Great on laptops
  - Latest kernel and userland is absolutely essential for supporting cutting edge laptop technology
  - GNOME Desktop works well on the laptop form-factor
  - Secure Boot support
  - Fingerprint reader support
  - TPM support

# Why not RHEL or CentOS Stream?

- CentOS Stream is a fantastic OS and is rapidly approaching the level of support that would work well for laptops, but our managed linux desktop project started when it wasn't ready yet
- Red Hat's focus for bug fixes is not laptops, so any fixes do take some time to appear in RHEL
- EPEL (Fedora packages on RHEL/CentOS) is a subset of the packages available for Fedora

# Managing Linux workstations and laptops at scale

# What does Managing Systems at scale mean?

- Managing a lot of computers with a small group of people
- Cattle vs. Pets
- Configuration as Code
- Assessing risk at scale

# What does Managing Systems at scale mean?

- Windows and MacOS have many commercial and open source products for Mobile Device management
  - Microsoft has Group Policy, Active Directory and Entra
  - Apple has Apple Business Manager
  - Many products that can manage these OSs
- Most of these tools don't really support Linux in a meaningful way
- These are the typical scenarios:
  - Just no support at all for Linux
  - Assumes Linux is just a server
  - Just sends a shell script to run on remote side

# What does Managing **Linux** Systems at scale mean?

- Use configuration management system
  - Puppet, Chef, Ansible, SaltStack, Cfengine, etc.
  - Managed through an IT administrative server/network
- Every system was known and tracked
  - Some sort of Asset database
  - Configuration Management consumed asset data
- Managed installed packages and tracking updates
- Manage and update software configuration
- Capturing logs and metrics about systems

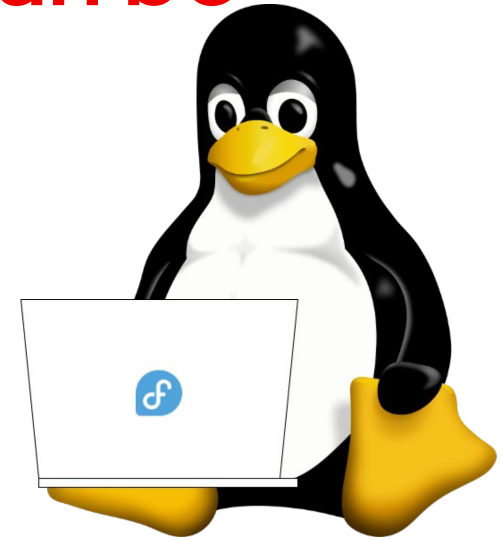
# How is configuration applied to managed systems?

- Pull:  Configured system "pulls" configuration from a central server or cluster of administrative servers
  - Software such as Puppet, Chef, SaltStack, Ansible-pull
  - Must provide an API endpoint (such as HTTPS) that is always reachable
- Push: Administrative service "pushes" the configuration to managed systems
  - Software such as Ansible Automation and SaltStack
  - Administrative systems connect to the managed system (such as through SSH)

# Traditional Configuration Management assumes certain things

- Computer is most likely a server or a cloud VM
- Computer is always running, or can be spun up on demand
- Network is probably stable and always on
- It won't be interrupted by a power event (poweroff, sleep)
- Can always reach identity providers (AD, Kerberos, LDAP, etc.)
- The user(s) of the computer doesn't have physical access to the system

# What kind of things can be managed?



# Managing Linux

- Linux Workstations are just Linux, many of the same tools used to manage Linux servers can be used on workstations
  - Packages
  - Files
  - Services
  - Run commands

# Managing the Linux Desktop

- Provisioning Fedora desktop systems
- System-wide configuration
  - dconf
  - browser settings
  - software repositories
  - user capabilities
- Remote support

# Provisioning Fedora Desktop systems - Kickstart

- Fedora Workstation uses Anaconda to install
- Use Kickstart, which is a simple text configuration file, which lets you automate:
  - partitioning
  - initial package setup
  - initial system systems like time zone, keyboard mappings
  - post-install script
- Add a kickstart file to a Fedora Linux ISO using the mkksiso command
- Use Lorax or Image Builder to generate a "Live Image" file, use that instead of installing packages in the kickstart

# Provisioning Fedora Desktop systems - Recommendations

- Encrypt disks. Laptops have a tendency to walk off, best to have disk encrypted
  - Create a backup password for decrypting disks
  - Anaconda kickstart has syntax for creating an escrow file that can be saved and decrypted by IT
- Use good computer naming conventions
  - Make it easy for you to identify who has what computer
  - Makes looking through logs easier if collected centrally
- Automate post-install setup of devices

# System-wide configuration - dconf

- Simple key-based settings used by GNOME and other software

```
$ dconf read /org/gnome/desktop/screensaver/picture-uri
'file:///usr/share/backgrounds/fedora-workstation/zen_dark.jpg'
```

- Examine dconf settings with "dconf" command

```
$ dconf dump /org/gnome/desktop/screensaver/
[/]
lock-delay=uint32 0
lock-enabled=true
picture-uri=file:///usr/share/backgrounds/fedora-workstation/zen_dark.jpg
```

# System-wide configuration - dconf

- Files can be placed in /etc/dconf/db/local.d/ to set defaults

```
$ cat /etc/dconf/db/local.d/00-mysettings
[org/gnome/desktop/screensaver]
picture-uri=file:///usr/share/backgrounds/My_Custom_Background.jpg
```

- Dconf settings can be locked by placing files in /etc/dconf/db/local.d/locks

```
$ cat /etc/dconf/db/local.d/locks/00-mysettings-lock
# Lock desktop background
/org/gnome/desktop/screensaver/picture-uri
```

# System-wide configuration - dconf

- The GNOME Display Manager (gdm) also uses dconf
- Settings are placed in /etc/dconf/db/gdm.d/, in the "/org/gnome/login-screen" dconf schema
- You can set a login banner, which is text that will appear during the graphical login screen
- You can also set the logo that appears at the bottom of the login screen
- I also set the power settings so the login screen never sleeps

# System-wide configuration - browser settings

- Firefox has a default settings directory, you can drop a javascript (.js) file in /etc/firefox/defaults/pref/, for example:

```
// browser startup page
pref("browser.startup.homepage",
"data:text/plain,browser.startup.homepage=https://mycompany.fedora/startpage/");
```

- These settings are just what you'll get by default on a new firefox profile
- Good for setting things like startup page, setting a default spellchecker dictionary, setting up any proxies or network settings

# System-wide configuration - browser settings

- Firefox has a policy language, you can drop a JSON file in /etc/firefox/policies
- This file can define settings for all sessions, even firefox profiles that have already been created
- The list of policy settings is available in the Mozilla github: https://mozilla.github.io/policy-templates/
  For example:

```
{ "policies": {
    "DisplayBookmarksToolbar": true
  }
}
```

# System-wide configuration - browser settings

- You can set the default browser extensions, and even make them mandatory

```
{ "policies": {
    "Extensions": {
      "Install": ["https://addons.mozilla.org/firefox/downloads/somefile.xpi",
"//path/to/xpi"],
      "Uninstall": ["bad_addon_id@mozilla.org"],
      "Locked":  ["addon_id@mozilla.org"]
    }
  }
}
```

# System-wide configuration - browser settings

- You can set customization to browser extensions too*

```
{ "policies":
  { "3rdparty":
    { "Extensions": {
      "uBlock0@raymondhill.net": {"adminSettings": {
         "selectedFilterLists":
["ublock-privacy","ublock-badware","ublock-filters","user-filters"]
}}}}}}
```

- Each browser extension has its own policy, which may or may not be well documented. For example, uBlock Origin is well documented: [https://github.com/gorhill/uBlock/wiki/Deploying-uBlock-Origin](https://github.com/gorhill/uBlock/wiki/Deploying-uBlock-Origin)

* Pretend this is valid JSON, it's hard to fit in a slide

# System-wide configuration - browser settings

- Google Chrome also has the ability to set system-wide settings
- Other chromium-based browsers too (i.e. Brave, Vivaldi, etc.)
- Put JSON files in `/etc/opt/chrome/policies/managed/`

```
{
    "PromotionalTabsEnabled": false,
    "MetricsReportingEnabled": false,
    "SafeBrowsingExtendedReportingEnabled": false,
    "UrlKeyedAnonymizedDataCollectionEnabled":
false,
    "PrivacySandboxPromptEnabled": false,
    "PrivacySandboxAdMeasurementEnabled": false,
    "PrivacySandboxAdTopicsEnabled": false,
    "PrivacySandboxSiteEnabledAdsEnabled": false,
    "CreateThemesSettings": 2,
    "DevToolsGenAiSettings": 2
    "GenAILocalFoundationalM                1,
    "HelpMeWriteSettings":
    "TabOrganizerSettings":
}
```

# System-wide configuration - browser settings

- Google Chrome can also set the default browser extensions similarly, but syntactically distinct from Firefox

```
{ "ExtensionSettings": {
    "ddkjiahejlhfcafbddmgiahcphecmpfh": {
    "installation_mode": "normal_installed",
    "update_url": "https://clients2.google.com/service/update2/crx" }
  }
}
```

- You need to know the extension's signature, in this case it is uBlock Origin Lite
- Google can also set up extension settings in the same file, which looks just like Firefox's 3rdparty browser policy
- [https://chromeenterprise.google/policies/](https://chromeenterprise.google/policies/)

# System-wide configuration - software repositories

- Set up custom DNF package repositories in /etc/yum.repos.d/, for example:

```
[internal-packages-testing]
name = MyCompany Repository for Fedora Linux $releasever (Testing)
baseurl = https://repos.mycompany.com/fedora/$releasever/
gpgkey = https://repos.mycompany.com/fedora/RPM-GPG-KEY-fedora
enabled = 1
gpgcheck = 1
skip_if_unavailable = 1
timeout = 5
```

# System-wide configuration - software repositories

- But what if you don't want to publish a public DNF repo?
  - There is a 'username' and 'password' repo setting, which will let you password-protect your DNF repos.  It basically signs into a web page that uses standard HTTP authentication
  - You can make the repos only available while on a VPN or mesh network. Most modern VPNs require two-factor authentication which would prevent automation from accessing repositories
  - We store packages in an AWS S3 bucket, exported to the internet via CloudFront, using a Lambda function for DNF authentication

# System-wide configuration - user capabilities

- User authentication
  - Local password: Need to be able to prevent login ability for auditing, security, and HR reasons
  - Enterprise authentication: What happens if there is no network connection?
    - Use SSSD's ability to cache an enterprise authentication, add "cache_credentials = True" in /etc/sssd/sssd.conf for your domain.
    - During setup, have user authenticate once so it is cached
    - Creates a hash of the password, will be updated if user logs in or unlocks the screen while attached to the internal network

# System-wide configuration - user capabilities

- sudo
  - By default, allows members of the 'wheel' group sudo abilities
  - Drop configuration files in /etc/sudoers.d/ for additional setup
  - Useful for running tools that don't integrate with PolicyKit
  - Not as useful for running graphical applications

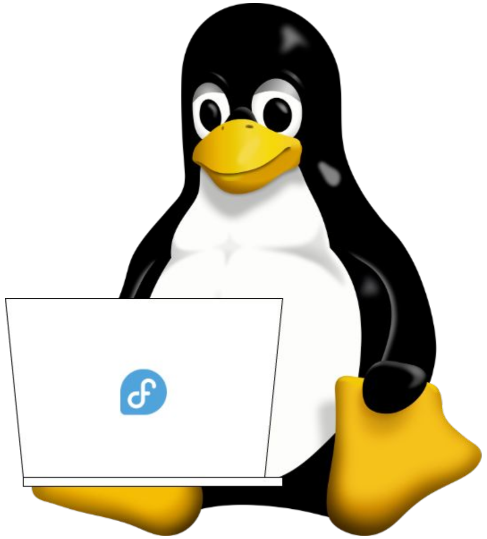
# System-wide configuration - user capabilities

- PolicyKit
  - Can define whether user can perform actions like restarting system services, update software, launch virtual machines, etc.
  - Can also restrict actions to local users, prohibiting a user over SSH from performing the same action
  - Many Fedora services use PolicyKit, for example, Software updates, NetworkManager, firewalld, systemd, etc.
  - Local rules go into /etc/polkit-1/rules.d/, packaged rules are in /usr/share/polkit-1/rules.d/

# System-wide configuration - Remote Support

- Commercial solutions
  - Red Hat uses BeyondTrust for Remote Support (Latest version works with Wayland!)
  - RustDesk: Rust-based remote desktop software
  - Teamviewer, AnyDesk, LogMeIn123, etc, (I've never used, have no opinion)
- Open Source
  - OpenSSH: As long as you limit to only over a VPN or private network
  - VNC/RDP/etc: Do not run over an unencrypted network. Only tunnel over SSH. Do not expose to the internet

# Managing Linux Workstations



# Managing Linux Workstations

## Traditional Workstation Management

- Every device on managed network
- Everyone came in to office to work
- Static or assigned IPs
- Desktops systems more common
- Every system was known and tracked

Ref: https://commons.wikimedia.org/wiki/File:Computer_lab_showing_desktop_PCs_warwick.jpg

# Why traditional Linux administration doesn't work anymore

- People are working remotely
  - Working while travelling
  - Pandemic caused many WFH mandates
  - Remote work jobs are much more common
  - Desktops replaced with Laptops
- How do you manage remote systems?
- How do you track assets?
- How can you trust the network anymore?

# How Linux Workstations now appear to IT

- IT no longer own the whole network path to workstations
- Home and remote work systems are behind a NAT
- Global workplace and global hours
- Most devices are laptops
  - Do not remain in one place
  - Laptop hardware is not server hardware, driver issues, shorter support lifetime, weird devices attached

# Configuration Management of Highly Mobile Workstations (aka laptops)

- Pull-based Configuration Management
  - If Pull server is on internal network, can't be reached when not on internal network or VPN
  - If Pull server is on external network, it's exposed to attacks
- Push-based Configuration Management
  - Remote devices are unreachable, either because they're off or behind a private network
  - Exposing SSH on workstations to the internet is a bad idea
  - VPNs can't always be active, or activated through automation

# Configuration Management of Highly Mobile Workstations (aka laptops)

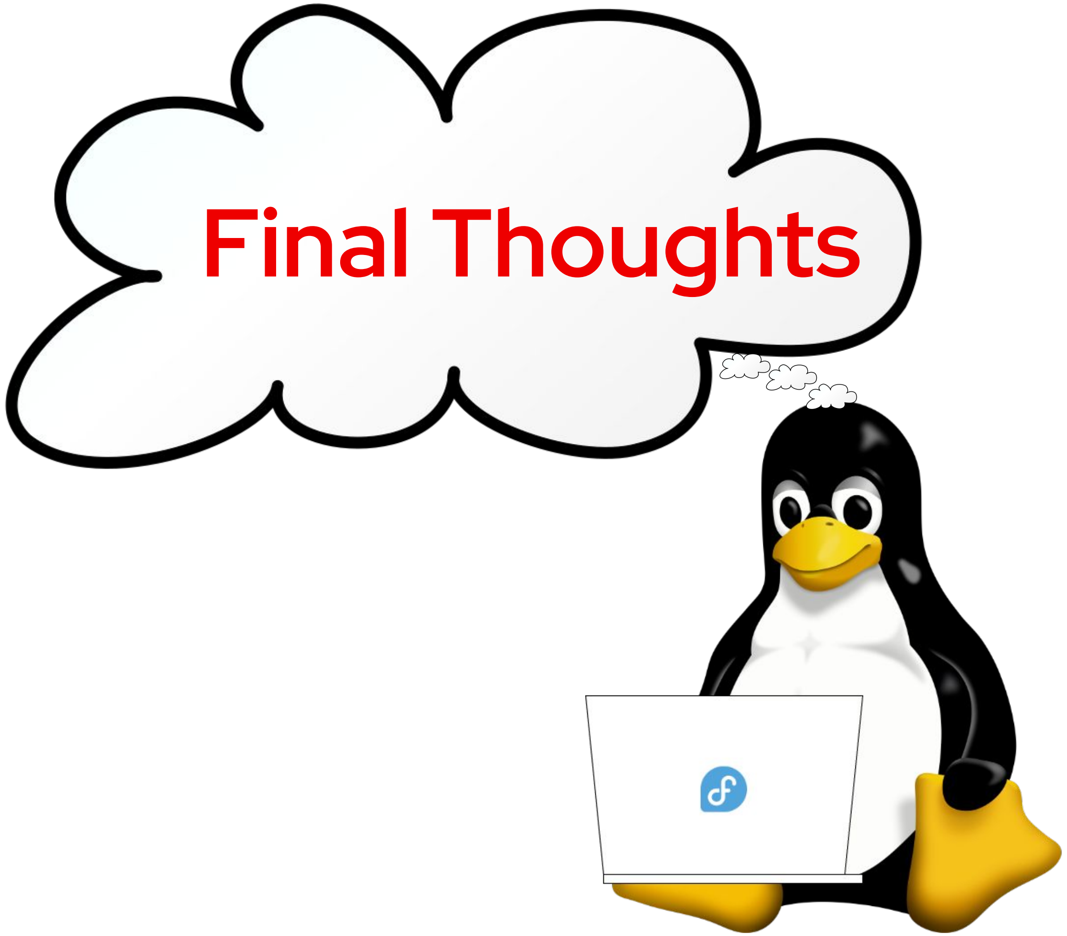
- Other issues with managing remote laptops
  - Users like to suspend or reboot at the least convenient time
  - User likes to tinker with the system and disables management services
  - User plugs weird devices into the computer, causing it to misbehave
  - Laptop hardware gets frequent firmware updates, breaking things
  - Laptop hardware support in LTS Linux Operating systems is sometimes slow
  - Walking a user through reinstalling the OS remotely

# How we (mostly) solved these issues

- We ended up using Ansible for configuration management
  - But why? You can't easily SSH into the systems!
  - But you can build all your Ansible playbooks and roles into an RPM, and deploy the RPM through locked down Yum repositories
- Learn to love Splunk
  - Securing Splunk's API endpoint is Splunk's job, not mine
  - Configured Ansible to use Splunk callback to log plays
  - Send systemd journal to splunk
- Osquery: Monitor packages, scan for known vulnerabilities and malware

Ansible Logo: https://en.m.wikipedia.org/wiki/File:Ansible_logo.svg
Splunk Logo: https://www.splunk.com/en_us/newsroom/media-kit.html
osquery Logo: https://github.com/osquery/osquery

# Final Thoughts



# Final Thoughts

- Linux Desktop management at scale still requires tying together a lot of pieces, there is no comprehensive solution
- Don't be afraid of using commercial tools, if they provide a solution and can offer support. I will always promote open source tools, so when evaluating a commercial product, see how they use open source software.
- Linux users are an unruly bunch, don't be surprised if they don't want to be managed. It's best to come from the perspective of making their life easier rather than laying down the law

# Final Thoughts

- Things I'd love to try
  - Headscale, Netbird, or Nebula VPN: have all systems on a private mesh.
  - systemd-homed: Have encrypted home directories automatically set up.
  - (For Lenovo Thinkpad users) Lenovo Cloud Deploy of a Linux desktop image
  - rpm-ostree or bootc-based workstation distributions
  - Systemd Factory Reset - resets to a "Factory default"
  - Btrfs snapshot support integrated into the managed desktop environment
  -

# Q&A

Thank You!

Slides will be available after the talk!

Contact me:

Email: jbilling@redhat.com

Mastodon: floss.social/@jsbillings