SUSE

Linux Group Policy

Latest Developments, Use Cases, Integration, and Best Practices

Agenda

Introduction

10 MAY 2023
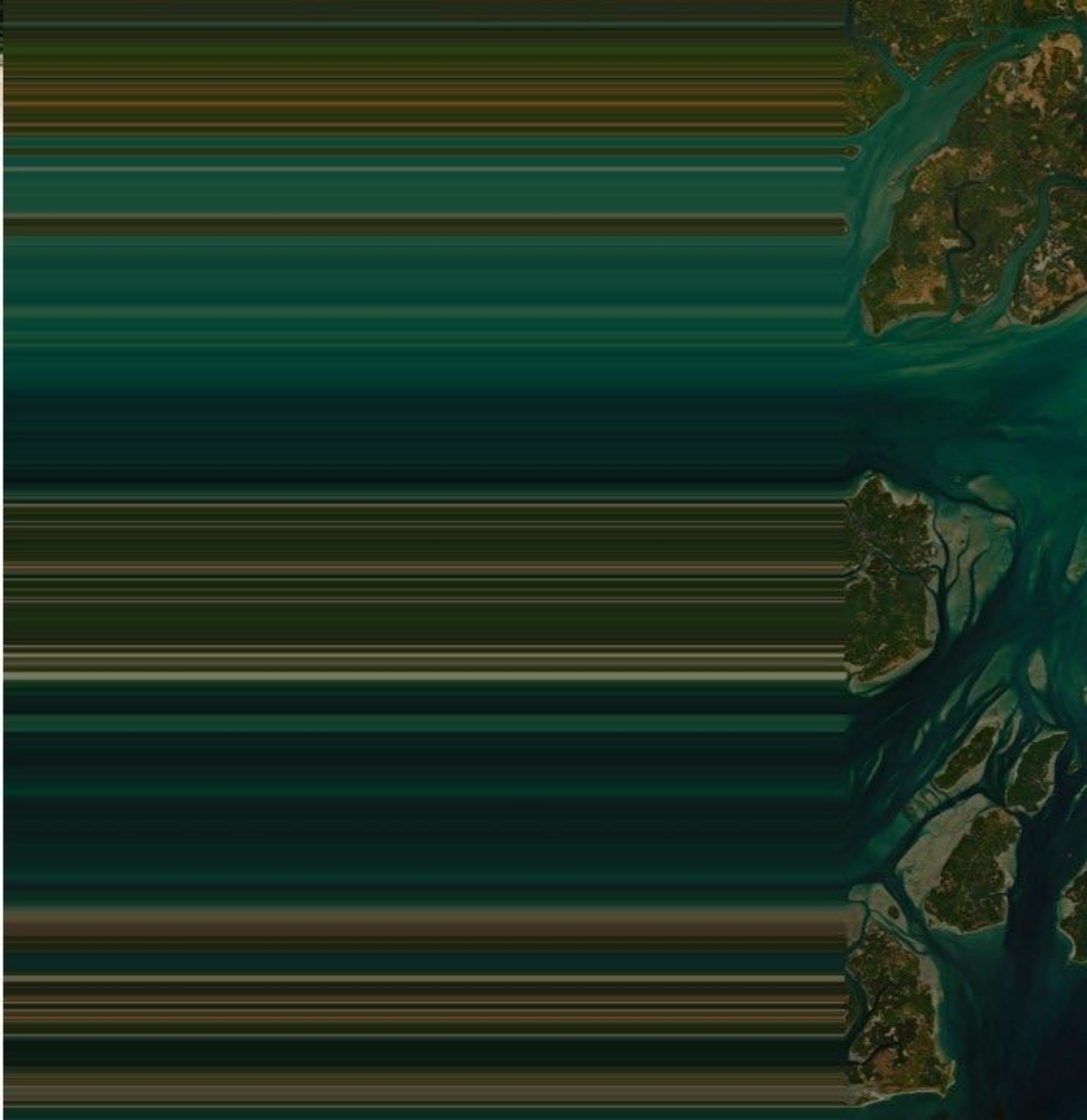
What is Group Policy?
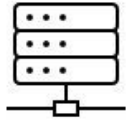
Active Directory

Group Policy

Stored on the SYSVOL
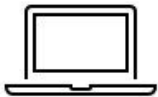
Computer Settings

User Settings

Centralized Management

Group Policy provides a central location for creating, managing, and deploying policies

- Reduces the risk of misconfiguration

- Eliminates policy inconsistencies

What is a Group Policy Object?

Group Policy (Work Order Template)

A => ?
B => ?
C => ?

Group Policy Object (Work Order)

A => 1
B => 2
C => 3

Group Policy on Linux

Samba has provided Group Policy client support since 4.14

- Intended to be like popular proprietary tools (Vintela, Centrify, etc)

- Easier integration into a Windows environment

- Many policies already available, custom policies are supported (documentation explains how to do this)

Current Policies for Linux

A current list of all available policies from Samba 4.18

- Scripts (hourly/daily/weekly/monthly)
- Kerberos and Passwords (for ADDC)
- Startup Scripts
- Sudoers
- Certificate Auto Enrollment
- Browser (Chrome/Chromium/Firefox)
- Firewall (firewalld)
- GNOME Settings (including custom dconf settings)

- Messages (MOTD/Issue)
- smb.conf
- PAM Access
- Files
- OpenSSH
- Symlinks
- Drive Maps (coming in 4.19)

Latest Developments in Linux Group Policy

10 MAY 2023

Latest Developments

— Improved cleanup to prevent tattooing policies

— Many bugs fixed

— Eliminate the libgpo backend

Significant changes were made to generally improve reliability of existing policies and improve documentation.
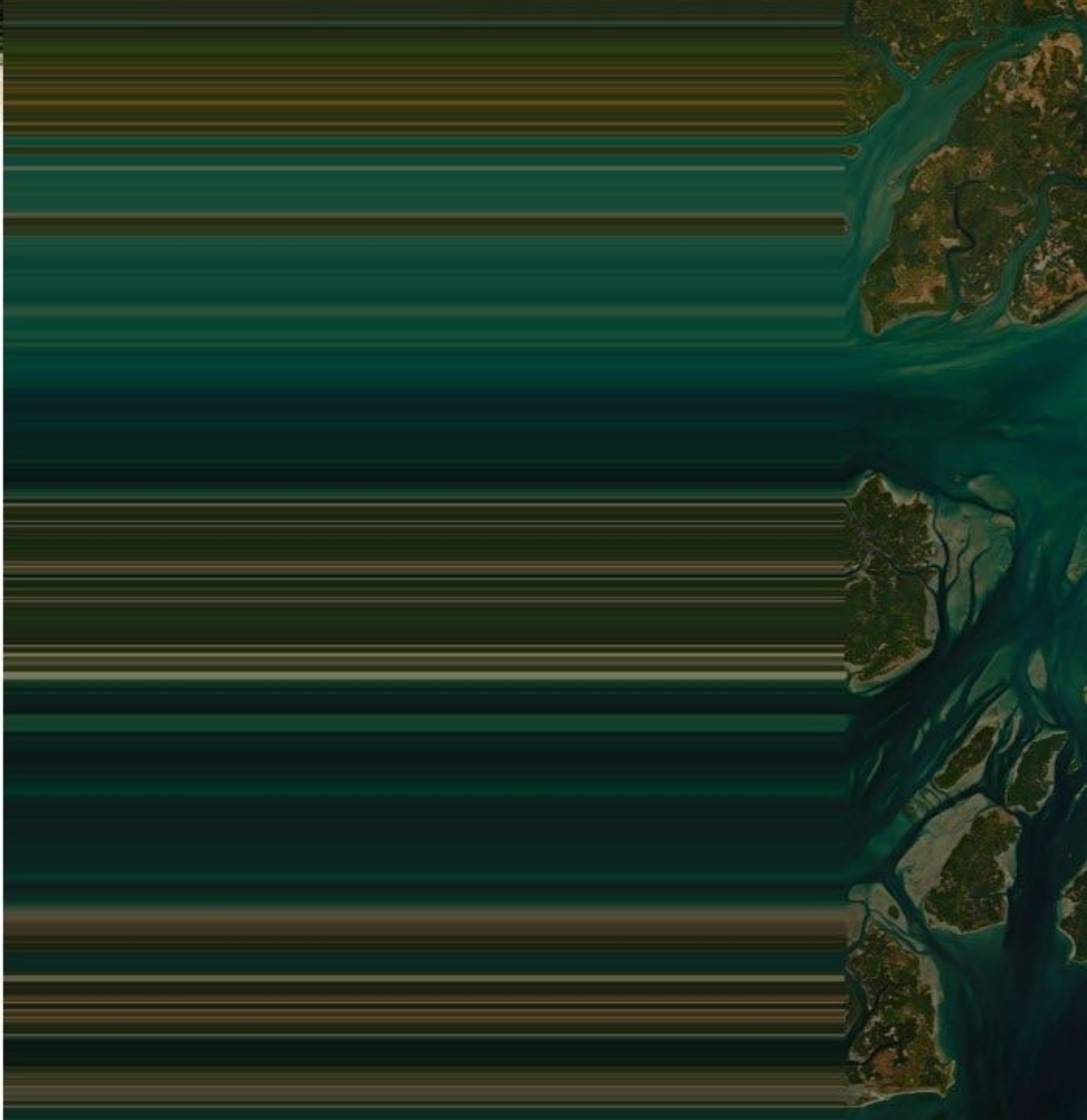
Drive Maps - Client Side Extension

Implementation which applies Group Policy Drive Maps

- Mounts SMB shares via **gio mount**

- Shows up in Nautilus, similar to Windows user experience

- Mounts are persistent

Use Cases for Linux Group Policy

10 MAY 2023

Securing Endpoints

Control who has access to a Linux host

SUDO

Sudo policies control who can access root

SSH Policies

OpenSSH policies control
how users access
the host

Secure Endpoint

Access Policies

PAM
Access policies
control who has
access to a host

Firewall

Firewalld policies lock down
ports on the host
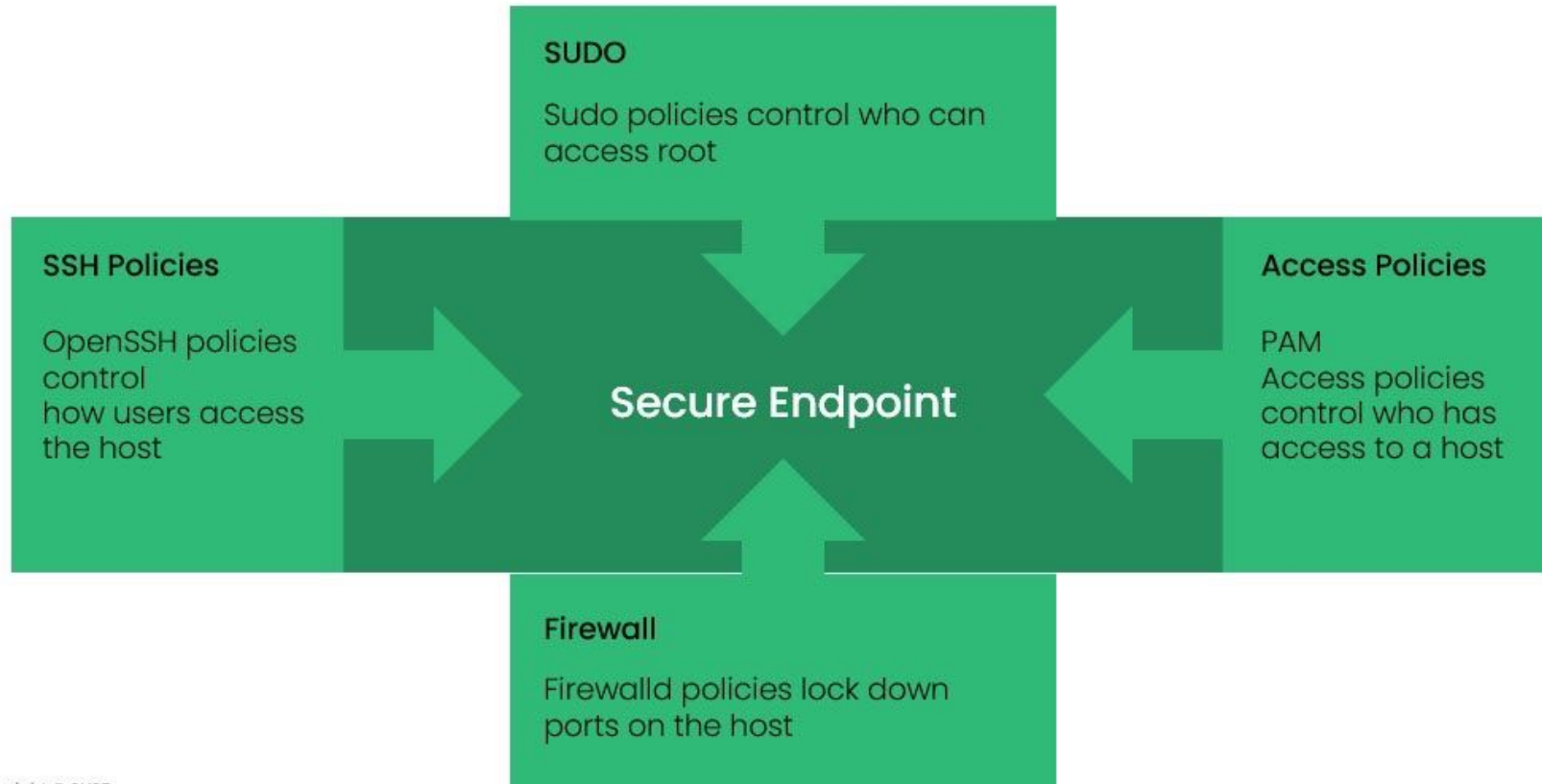
Demo Securing Endpoints

Pre-recorded demo

```
dmulder@localhost:~>
```
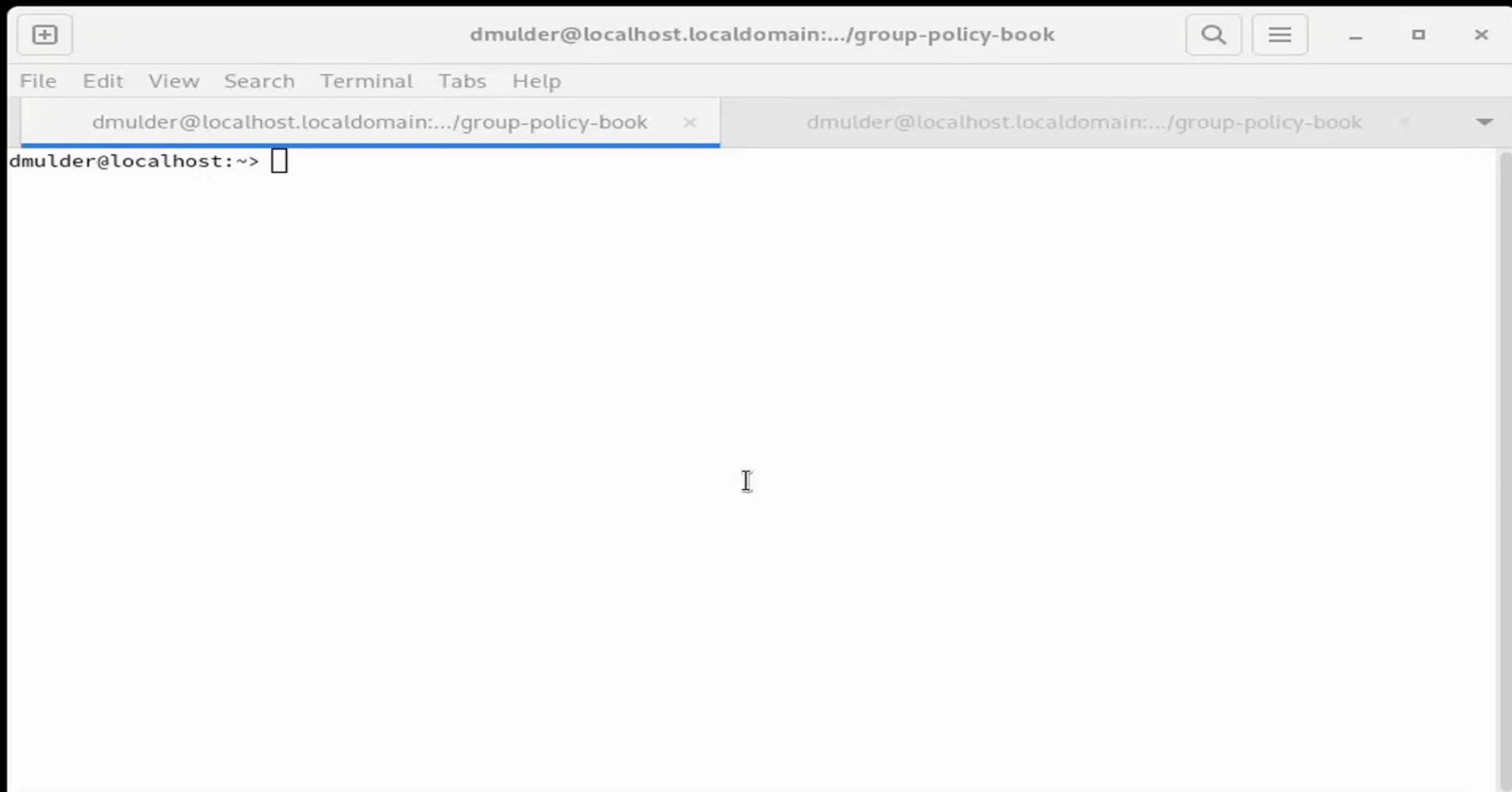
Complex Deployments
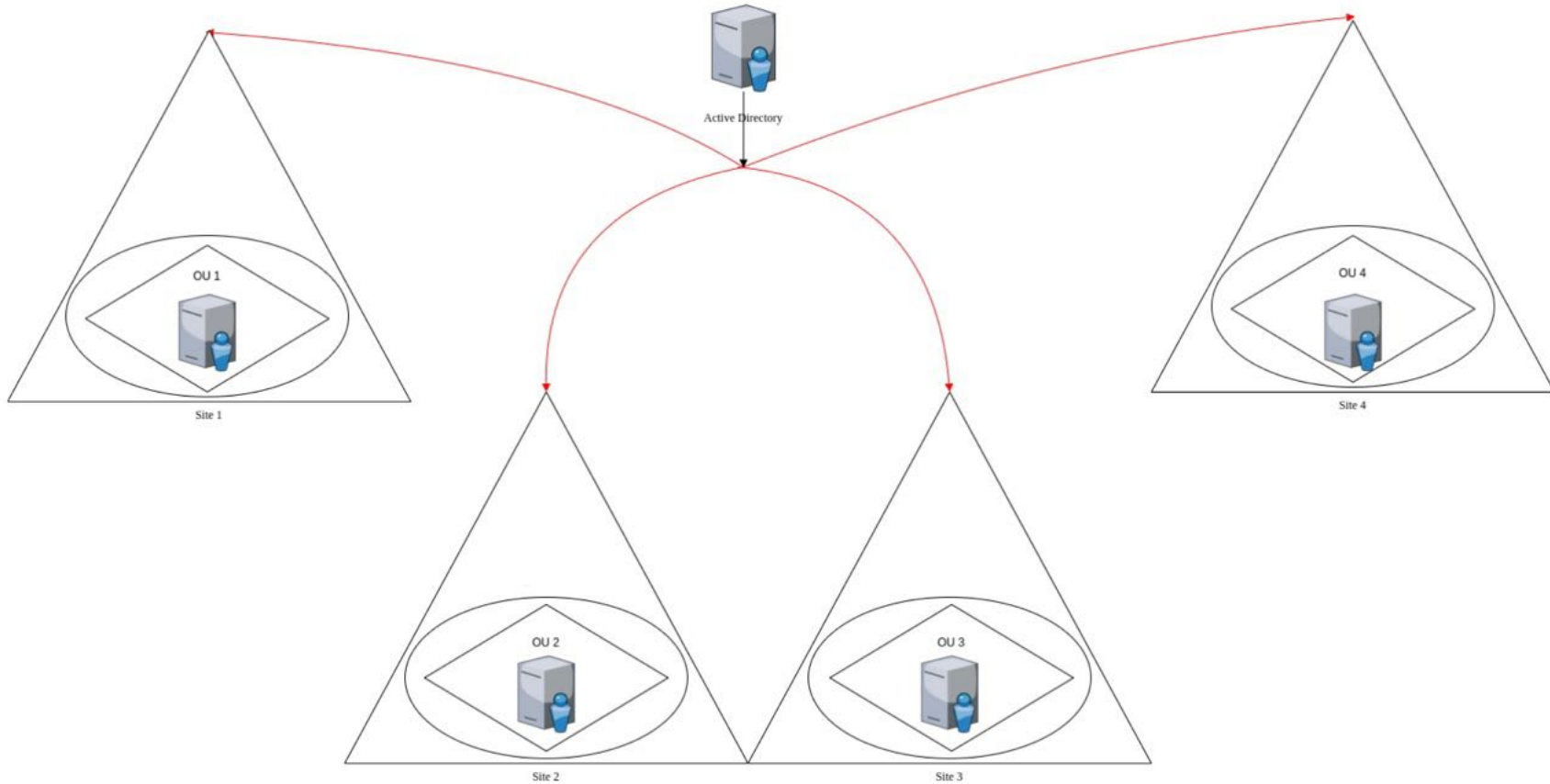
Integration of Linux Group Policy

10 MAY 2023

Integration with Winbind

Integrating Samba's Group Policy with Winbind is trivial (with caveat)

- Enable policy using smb.conf **apply group policies** = Yes
- Machine policy applies on the *Group Policy refresh interval*
- User policy applies *only at logon time*

Integration with SSSD

Integrating Samba gpupdate with SSSD requires oddjob-gpupdate

- **samba-gpupdate** and **oddjob-gpupdate** must both be installed

- The oddjob service will ensure both Machine and User policy are applied on the *Group Policy refresh interval*

WARNING: The package named **oddjob-gpupdate** in the ALT Linux distribution *is not the correct package for Samba.*

Best Practices for Setting Up and Configuring Linux Group Policy

10 MAY 2023

Configuring Policies

samba-tool is preferred for managing Linux Group Policy

- samba-tool can create, link, delete, and modify Group Policy Objects
- Always use the latest version of samba-tool for managing GPOs

Modifying Group Policies

The **samba-tool gpo manage** and **samba-tool gpo load** commands can modify GPOs

- Supported **samba-tool gpo manage** commands include:
    - smb.conf
    - Security (Password and Kerberos)
    - Startup Scripts
    - Files
    - Symlinks
    - Sudoers
    - Messages (MOTD/Issue)
    - PAM Access
    - OpenSSH

- Supported **samba-tool gpo load** commands include:
    - smb.conf
    - Password and Kerberos
    - Scripts
    - Sudoers
    - Messages (MOTD/Issue)
    - Certificate Auto Enrollment
    - Firefox
    - Chromium/Chrome
   - GNOME Settings
    - Firewalld

Troubleshooting

Common troubleshooting steps when investigating CSE issues

- First review the system logs for errors related to Group Policy processing, such as messages from samba-gpupdate or oddjobd:
  - sudo journalctl -xe | grep -E "(gpupdate|oddjob)"
- Next check the RSoP to see if policy applies:
  - sudo /usr/sbin/samba-gpupdate –rsop
- Next force policy application with debug enabled:
  - sudo /usr/sbin/samba-gpupdate –force –d 5
- Finally dump the Group Policy Cache to see if the policy applied:
  - sudo tdbdump /var/lib/samba/gpo.tdb -k "TESTSYSDM$" | xmllint --format -
- Refer to the docs for troubleshooting steps for a specific CSE.

New Documentation for Linux Group Policy

10 MAY 2023
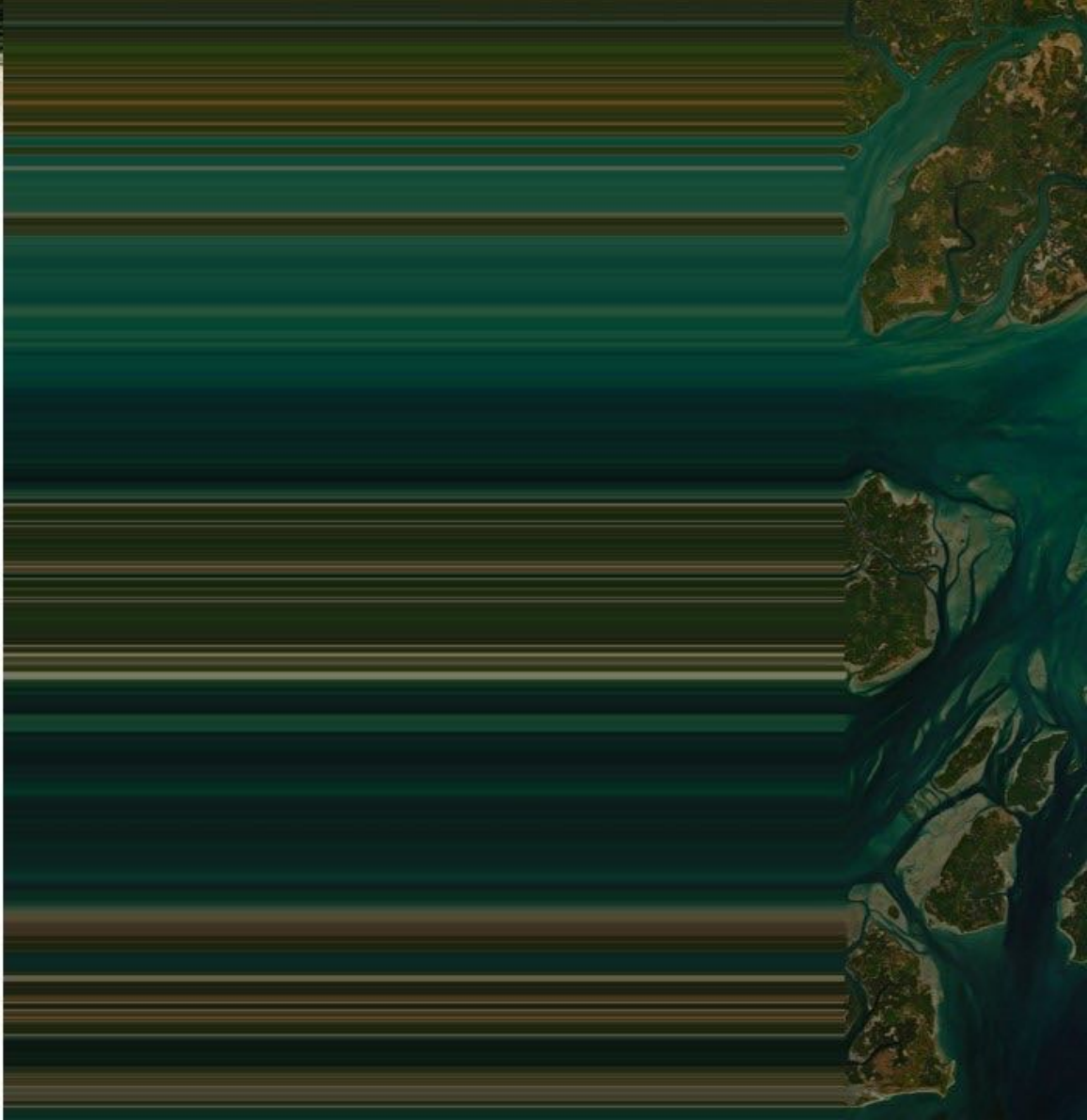
Group Policy on Linux

Documentation to simplify deploying Group Policy

- Available for free as an ebook, pdf, and online resource

- Physical print edition available

- Text is Creative Commons licensed

- Regularly updated with changes made to Samba Group Policy

Topics covered in the book

- Basic management instructions

- Details about each policy
  - How it's deployed
  - How to troubleshoot

- Creating your own policy

# Is Group Policy an MDM?

10 MAY 2023

Mobile Device Management

- MS has MDM Intune which replaces/complements Group Policy
- Some differences between Group Policy and an MDM:
    - Deployment and Management: AD vs. Cloud
    - Device Ownership: Org owned vs. Personal devices
    - Device Management Capabilities: Application Management, Content Management, and Monitoring and Reporting
    - Security Features: Biometric auth, device wiping, etc
    - Cloud Integration: Seamless integration with cloud services

Discussion & Questions
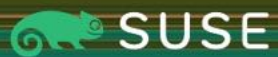
SUSE

Thank you

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

Frankenstrasse 146

90461 Nürnberg

www.suse.com