Active Directory Group Policy for UNIX

Gerald Carter, Developer, SAMBA/Centeris

Outline

- Active Directory Group Policy overview
  - Why should you care?
- Windows Group Policy architecture
- Group Policy on Linux/UNIX
  - Currently available options

Active Directory Group Policy

- Introduced with Windows 2000 as an efficient way to manage large numbers of machines
- Primarily used for standardized security settings and desktop lockdown
- Natural mechanism for planning, deploying, enforcing and demonstrating compliance with security regulations
- Extensible by 3rd party solutions to enhance the list of policy settings by allowing server and client side extensions.
  - Easy to leverage is Administrative Templates and the Registry CSE
- Advanced reporting tools exist to show the settings that are in effect (RSOP and GPO summary)

Windows Group Policy architecture

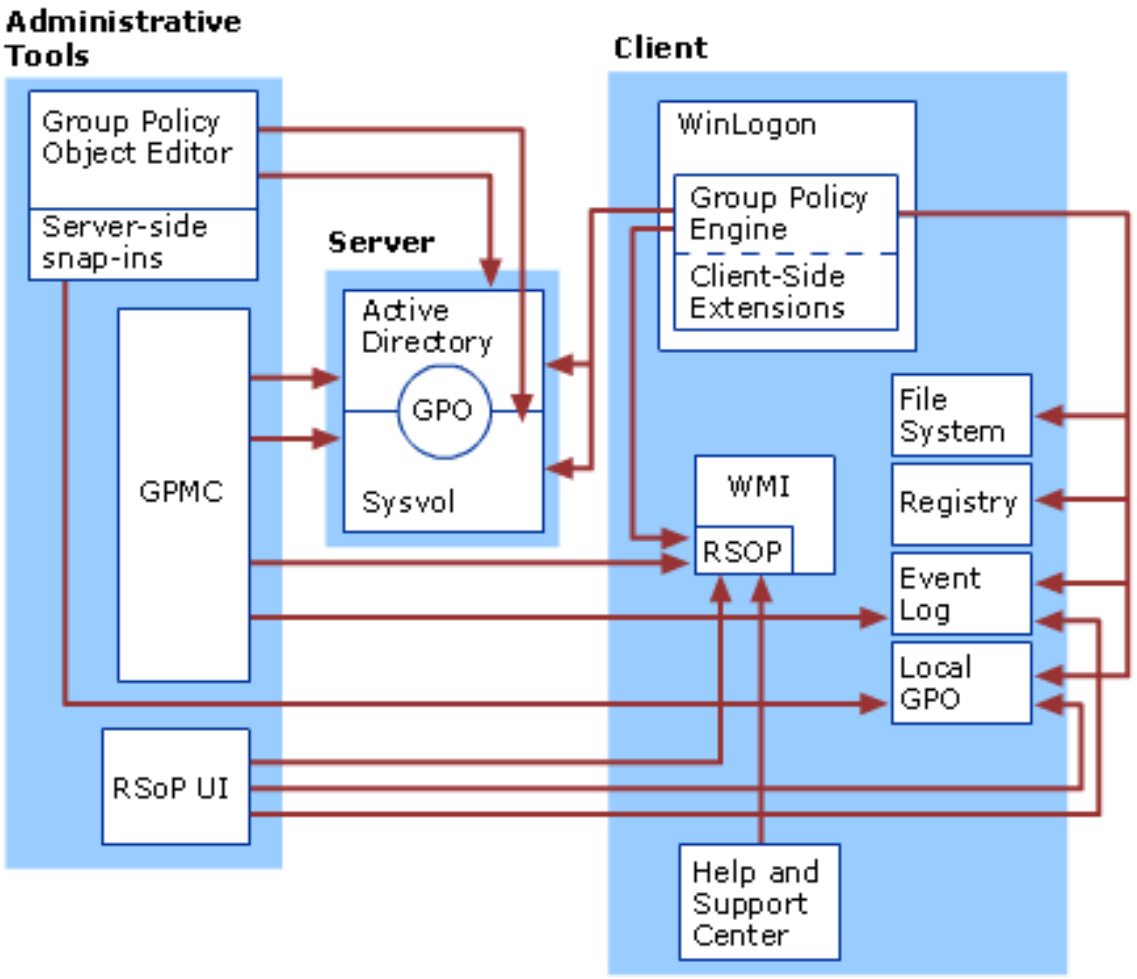
centeris

- Combination of LDAP attributes and data in SYSVOL
- *Sites, Domains* and *OUs* can have GP *objects* attached to them (via the *gPLink* attribute)
- GPOs are applied hierarchically with inheritance (and bits for controlling this behavior)
- A GP object is a bag of *machine settings* and *user settings*
- Group Policy clients poll AD to check for policy changes
- Machine settings applied at boot and when changed; user settings applied at logon
- User settings are applied as per both the machine's and the user's AD object location
- Hierarchy in AD supports inheritance blocking, and policy enforcement

Windows Group Policy Components

- Infrastructure Components
  - Client Side Extensions
  - Server Side Extensions
  - Winlogon
  - SysVol
  - Active Directory
- UI Components
  - Group Policy Object Editor
  - Group Policy Management Console

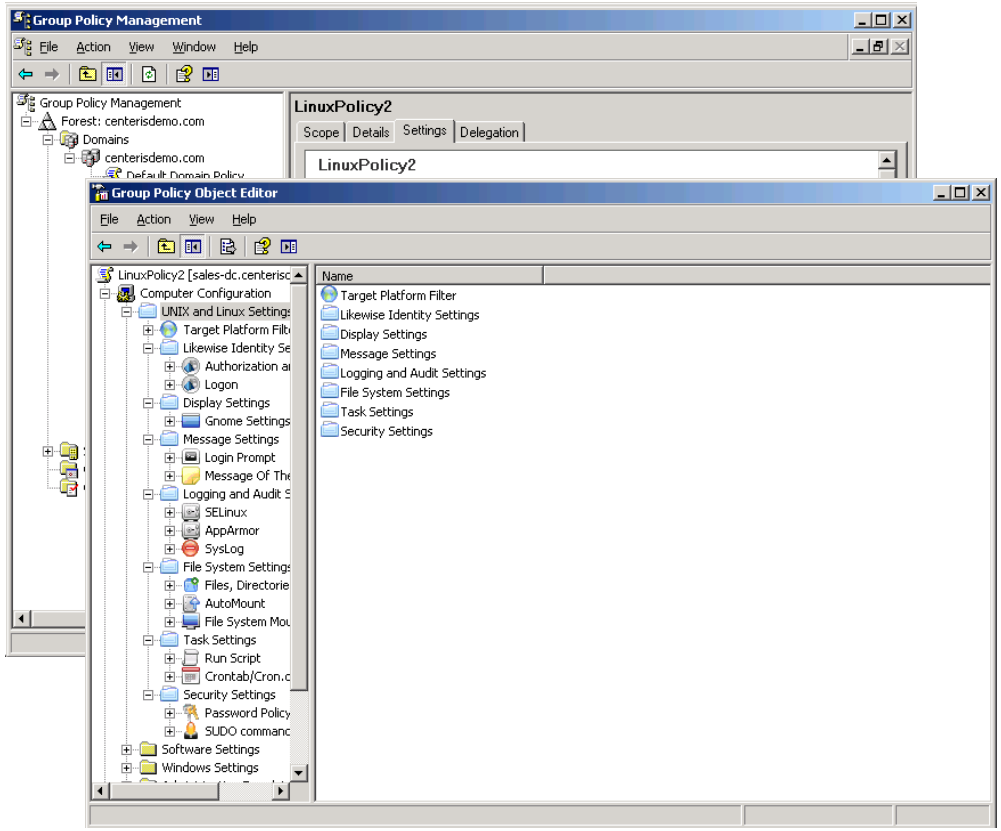
How Group Policy Works



Source: Microsoft MSDN

Group Policy for Linux/UNIX

- Leverage AD Group Policy for one-to-many computer configuration
- Either use Admin Templates or UNIX specific policies for system, security, & user settings
- No completely open source solution available at this time



Group Policy Details

UNIX/Linux Policies

- Files
- Scripts
- SUDO
- Cron
- Login Prompt
- Message of the Day
- SELinux
- AppArmor
- Syslog
- Log Rotate
- AutoMount
- File System Mounts

Likewise Identity Policies

- Kerberos Settings
- Kerberos Refresh
- Cached Credentials
- Offline Logon Support
- ID Mapping Cache
- ID Map UID Range
- ID Map GID Range
- Nested Group Expansion
- Logon Rights
- Home Directory Creation
- Home Directory Properties
- Replacement Characters

Local Account Policies

- Max Password Age
- Min Password Age
- Min Password Length
- Password Complexity
- GNOME Settings

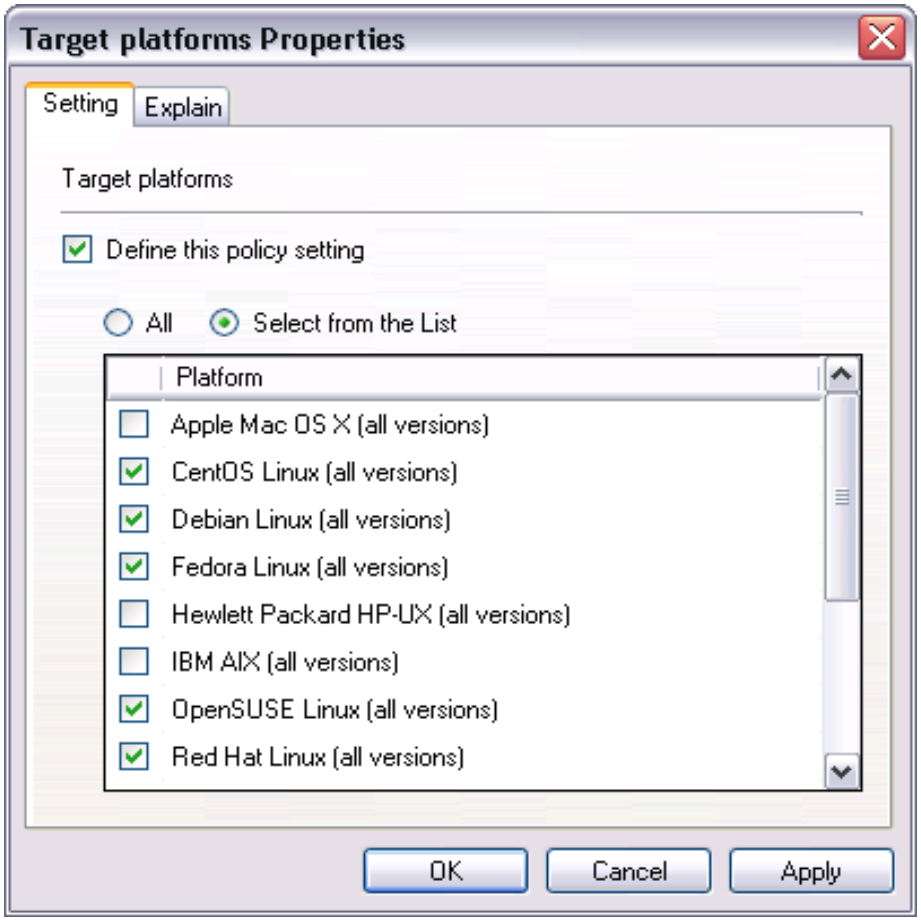
Mac Policies

- System Prefs Security
- Auto User Login
- Secure Virtual Memory
- Auto Logout from Inactivity
- Firewall Settings
- Network settings for IP/DNS, AppleTalk, and Bluetooth

Platform specific settings

- Each GPO has a way of indicating which platforms are to apply the settings specified in the object.

- This allows one GPO to define settings you wish to apply to one platform, and for another GPO to have settings unique to another type of platform



UNIX GP Implementations

- Commericial
  - Centeris – Likewise Identity
    - http://www.centeris.com/
  - Quest Vintela
    - http://www.quest.com/
  - Centrify
    - http://www.centrify.com/
- Open Source
  - Ongoing research in Samba