IT 609
Network and System Administration

Application Management

Tuesday September 23, 2021

Section Overview

- Operating System Management (finish)
- Application Management
- Assignment #01 - Part 1

End User Computing

Windows - Registry

A unified repository for configuration and preference information

Replaces old system of many separate `.ini` files

Editing via `regedit`

Can be accessed over a network

Security privileges apply to particular branches or sub-trees

Registry values can be read and set via APIs as well as by exporting/importing Registry files (`.reg`)

Registry Organization

Two major sections:

- Machine data
- User data

Items that apply to the whole computer and all users are in the Machine sections

Personal settings are in the User areas

Standard permissions model means that administrators can modify most of both of these while normal users can only modify their User section

Windows – Registry Hives

HKEY_CLASSES_ROOT

Link to HKLM\Software\Classes

File types, extension mapping, resources

HKEY_CURRENT_USER

Link to HKU\<CurrentUserSID>

HKEY_USERS (HKU)

.DEFAULT - minimal user settings/prefs

HKU/<SID> - user preferences and settings, stored in Documents and Settings

Only portion of Registry that members of the Users group can modify

Windows – Registry Hives

HKEY_LOCAL_MACHINE (HKLM)

- Hardware - created at each boot
- SAM - Security Access Manager
- Security - more security settings
- Software - software configuration for all users
- System - hardware, device drivers, etc.

HKEY_CURRENT_CONFIG

Link to HKLM\System\CurrentControlSet\Hardware Profiles\Current

What's The Right Way

Best practices for OS setup and management are sometimes confusing and conflicting

Good sources:

- The OS vendor
- Security groups like CIS and SANS

Companies and government organizations may have specifically defined practices

- DOD - STIGs

Monitoring & Logs

Log data is only as useful as the OS and application programmers make them!

System admins can use logs in different ways

- Good
  - Review log files when anything "bad" happens
- Better
  - Periodically check log files for anything abnormal
- Best
  - Automated system to check log files for you and report errors or suspicious activity

Monitoring & Logs

Windows

- Event Log Service - Application, Security, System, & others
- Accessed through Event Viewer
- Can also turn on auditing of file access, etc

macOS & Linux

- `syslogd` - system log daemon
- Configured in `/etc/syslog.conf`
- Writes to various files in `/var/log`
- Security related items in `/var/log/secure.log`

Mobile Challenges

Multiple platforms

Locked operating systems

Configuration

App Stores

Lost devices

BYOD

It's mobile

It just isn't like Windows!!!!!!

Mobile Device Management

- Centralized control and management
- Deployment of standard setups to corporate devices
- On-demand enrollment of BYOD
- Over-the-air control
  - Configure settings
  - Deploy or remove applications
  - Enforce update installation
- Lost device security
  - Location reporting
  - Remote lock and wipe

Software Licensing

What is Licensing?

- Software is protected by Copyright laws.
  - It is illegal to simply duplicate it without the permission of the author/owner?
  - May also be protected by patents
- License - A set of terms that the copyright holder requires you to accept in order to use it or make a duplicate.
  - Licenses can be restrictive or loose
- EULA - End User License Agreement
  - Aka shrink-wrap or click-through licenses (have been held up as binding by courts)

Kinds of Software & Licensing

- Proprietary Software.
  - Most commercial software
  - Generally restrictive EULA's
  - User is granted rights to use, and little else

Kinds of Software & Licensing

- Open Source Software
  - Not necessarily “free”
  - Author still holds copyright
  - Generally liberal terms granted for use and distribution

Kinds of Software & Licensing

- Public Domain Software
  - Anything released into the Public Domain is free from any copyright or other restriction
  - No licenses are necessary

Free Software Licenses

- The freedom to run the program, for any purpose.
- The freedom to study how the program works, and adapt it to your needs. Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help your neighbor.
- The freedom to improve the program, and release your improvements to the public, so that the whole community benefits. Access to the source code is a precondition for this.

Free Software Foundation, Inc. 2004. http://www.gnu.org/philosophy/free-sw.html

Common Licenses

- GPL - Gnu Public License
  - Free
  - Copyleft - Requires that all derivative works are also placed under the GPL

- BSD - Berkeley System Distribution
  - Free
  - No requirement placed on derived works

- Shared Source - several programs
  - Not free
  - Access to source code is granted for proprietary software

GPL, Open Source, & Business

- If GPL requires that all derived works are also under the GPL, then how can you sell GPL software?
- GPL does not prohibit charging for distribution mechanisms, support, training, documentation, etc
- Other licenses are less restrictive
- Many companies are have products based on open source, in whole or in part


Purchasing Software

http://blogs.technet.com/b/cdnitmanagers/archive/2012/01/10/back-to-the-basics-with-microsoft-software-licensing-options.aspx

Purchasing Software

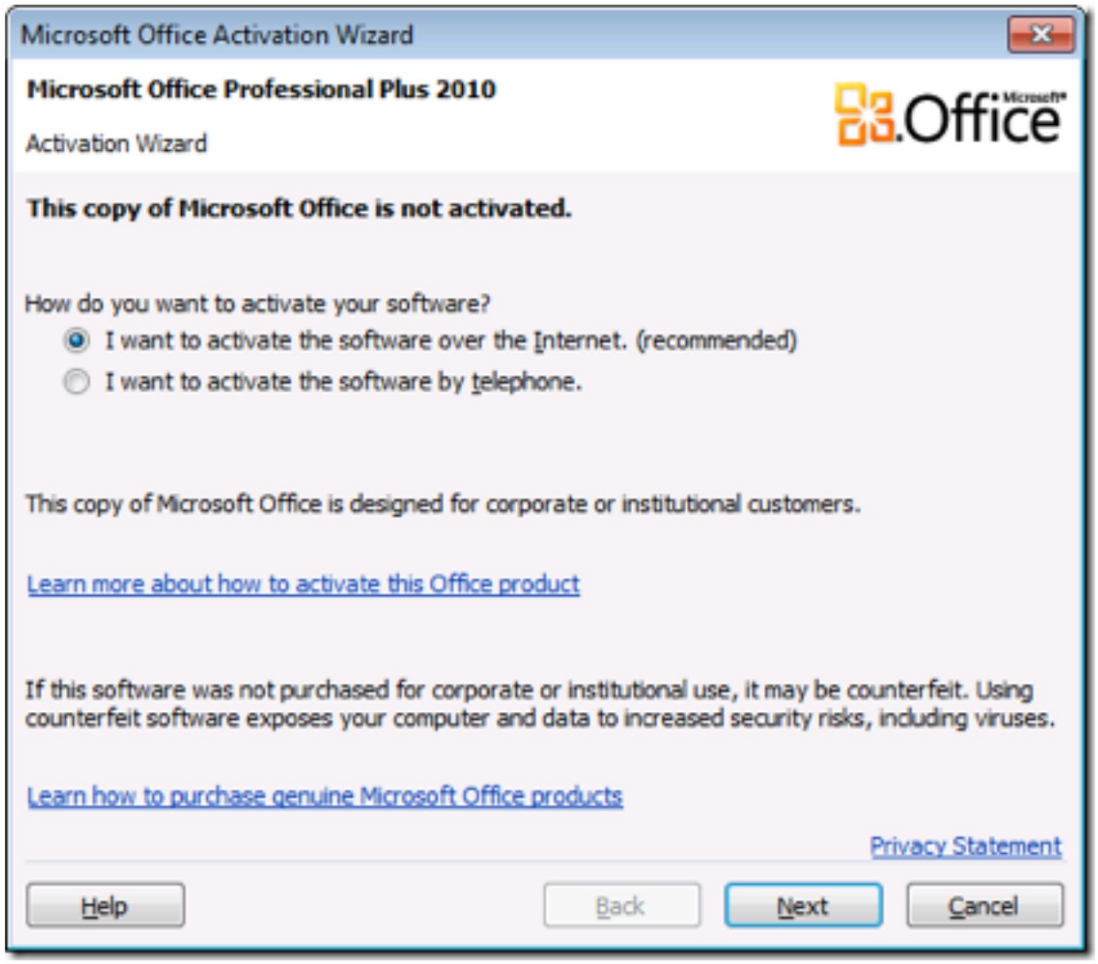
Shareware

"App Stores"

Site, Network, Concurrent Use

Site License	Allows use on all computers in an organization or at a given location. (May have quantity limits.)
Network License	Allows use by all computers on a given network. Usually has some central control service.
Concurrent Use License	Limit to how many copies can run at a time via a central metering service. May cost more than a normal license.

Installation & Activation



Perpetual, Subsription, & Maintenance

Perpetual License	You own it forever, but that might not get you future versions.	Pay once. Pay for each update.
Subscription	On-going fees to have the rights to use the program. Includes new versions and support (sometimes).	Pay yearly, but get updates.
Maintenance	Add-on for a perpetual license to get support and new versions.	Hopefully cheaper than buying each update.

Software Deployment

Computer Life Cycle

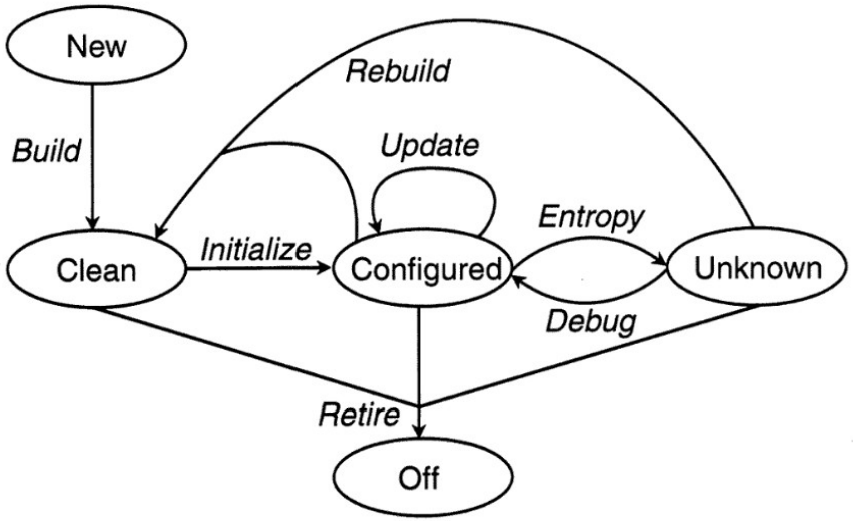


Figure 1.1: Evard's life cycle of a machine

Rémy Evard, 1997. "An Analysis of a Unix System Configuration"

Computer Life Cycle

- The goal of proper system administration is to keep the device in the “configured” state as long as possible.
- How do you get a device into that state quickly?
- How do you keep it from being affected by Entropy (i.e. keep in that state)?
- How do you handle the Update process?
- How do you efficiently repeat this for 100s or 1000s of devices?

General Procedures

- Plan - Partitions, naming schemes, etc
- Install OS - Be selective
- Update/Patch OS
- Configure OS
- Install Applications
- Update Applications
- Configure Applications
- Test, fix, test, fix, test, fix, test, fix, test,...
- Deploy

Some Observations

- The base OS must be solid
- Never trust someone else's installation
- Install only what you need
- OS's have bugs!
- Applications have bugs!
- Installing one thing can affect or break or change
- something else
- There is never enough time to test all interactions

$\therefore$ Deploy slowly

Benefits of Automation

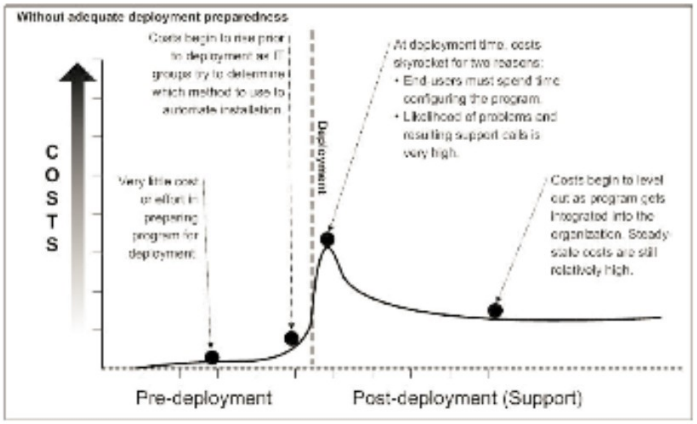


Figure 4.1: The Cost of Software Distribution without an ESP

Without automation, prep costs are low, but costs jump at deployment and support costs can stay elevated

The difference in costs between the proactive and the reactive approaches to software packaging is illustrated in Fig 4-1 and 4-2. It is clear that pre-deployment costs are greater with the ESP, but long-term savings are also quite evid Thus, the ESP is an essential part of a total cost of ownership (TCO) strategy.

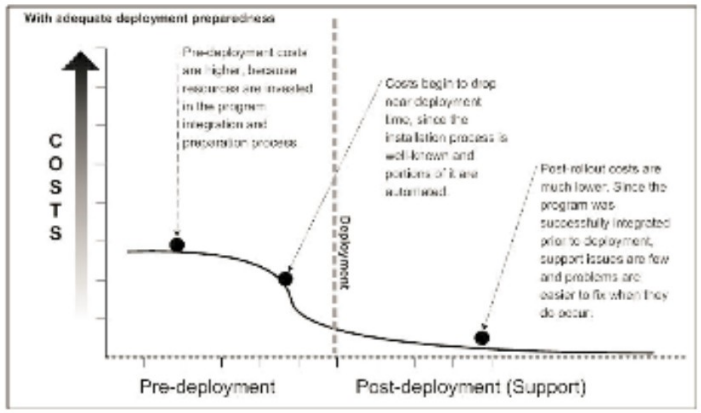


Figure 4.2: The Cost of Software Distribution with an ESP

With automation, there is far more prep work, but costs drop dramatically for both deployment and support

From Ruest, Nelson. Enterprise Software Packaging Practices, Benefits and Strategic Advantages. Wise Solutions, Inc. http://www.wise.com/esp/ESPWhitepaper.pdf

Automated Deployment

- Disk Imaging
  - Special utility to make an image of a filesystem or disk
  - Binary duplicate or file-by-file
  - Can deploy images over the network
  - All at once process
- Ghost
  - Now owned by Symantec (Norton Utilities, etc)
  - Disk imaging is often called “Ghosting” from this utility
- ImageX
  - Free imaging from Microsoft
  - Installation method for Windows OS
- Apple Software Restore

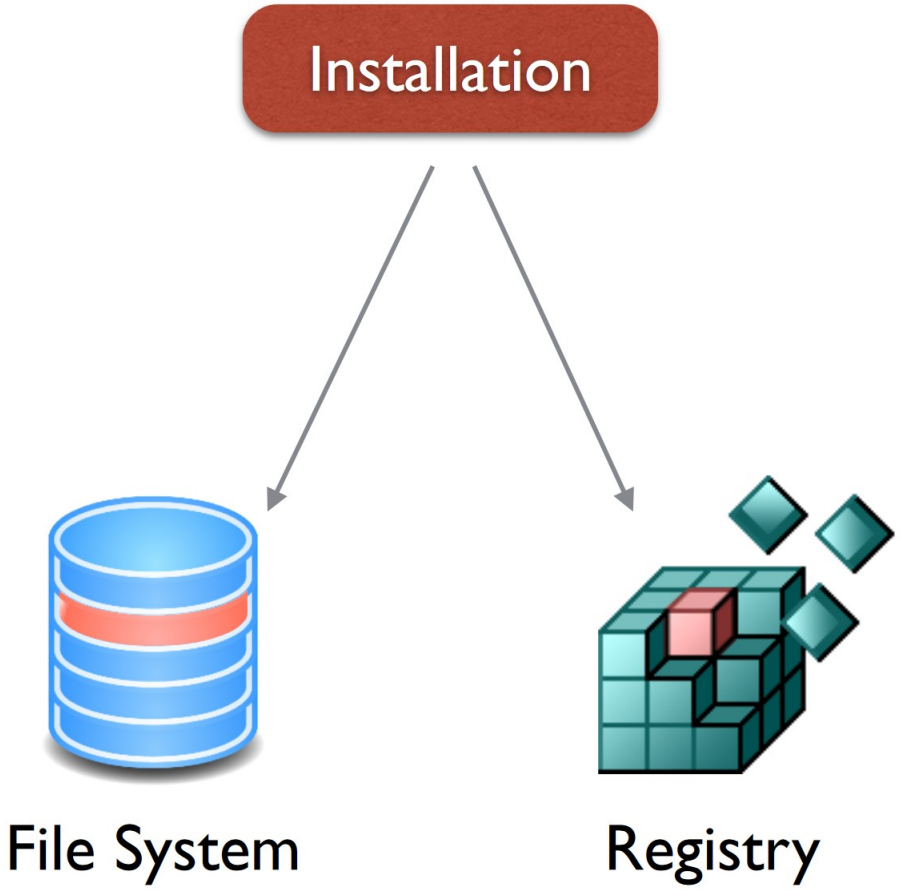
Automated Deployment

- Scripted Installation
  - One system installs and configures several packages
  - Lots of setup
  - May require re-packaging existing installers
- Unix “make” files
- Red Hat’s kickstart
- Windows MSI - Microsoft System Installer
- System Center Configuration Manager

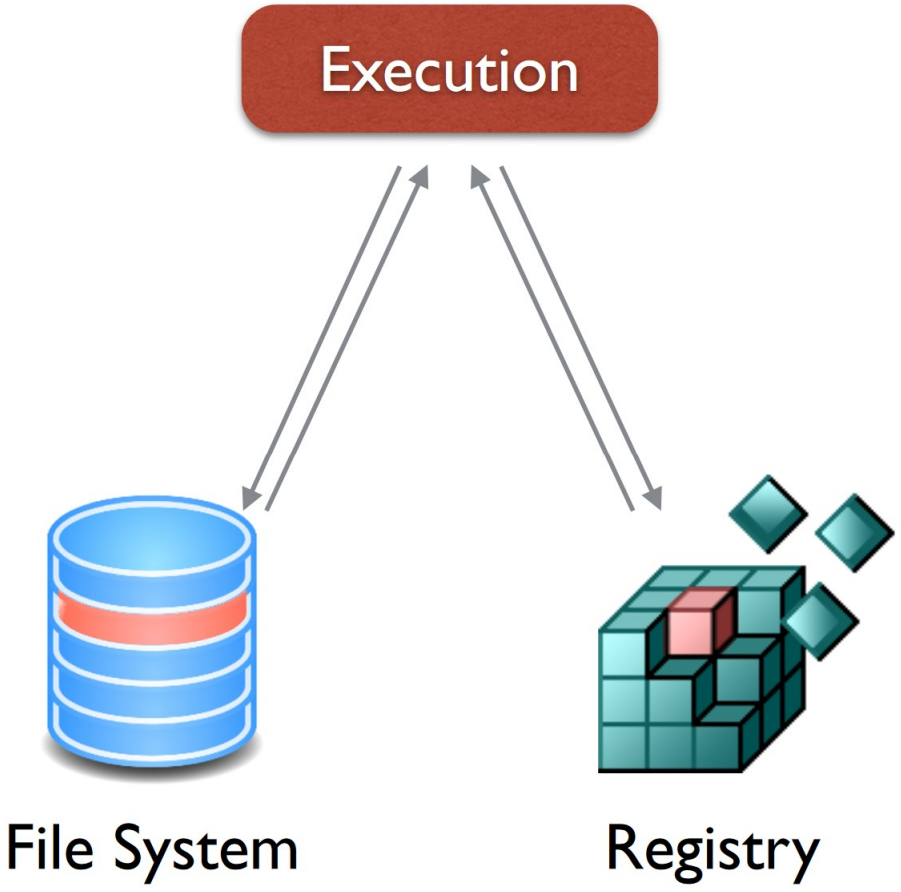
Automated Deployment

- Virtual Application
  - Package wrapping the entire application
  - Includes files as well as settings (Registry)
  - Can be used with traditional desktops or VDI
  - Download and “install” on the fly
  - Can remove itself after
- Thin App – VMware
- App-V - Microsoft
- Application Jukebox - Numecent

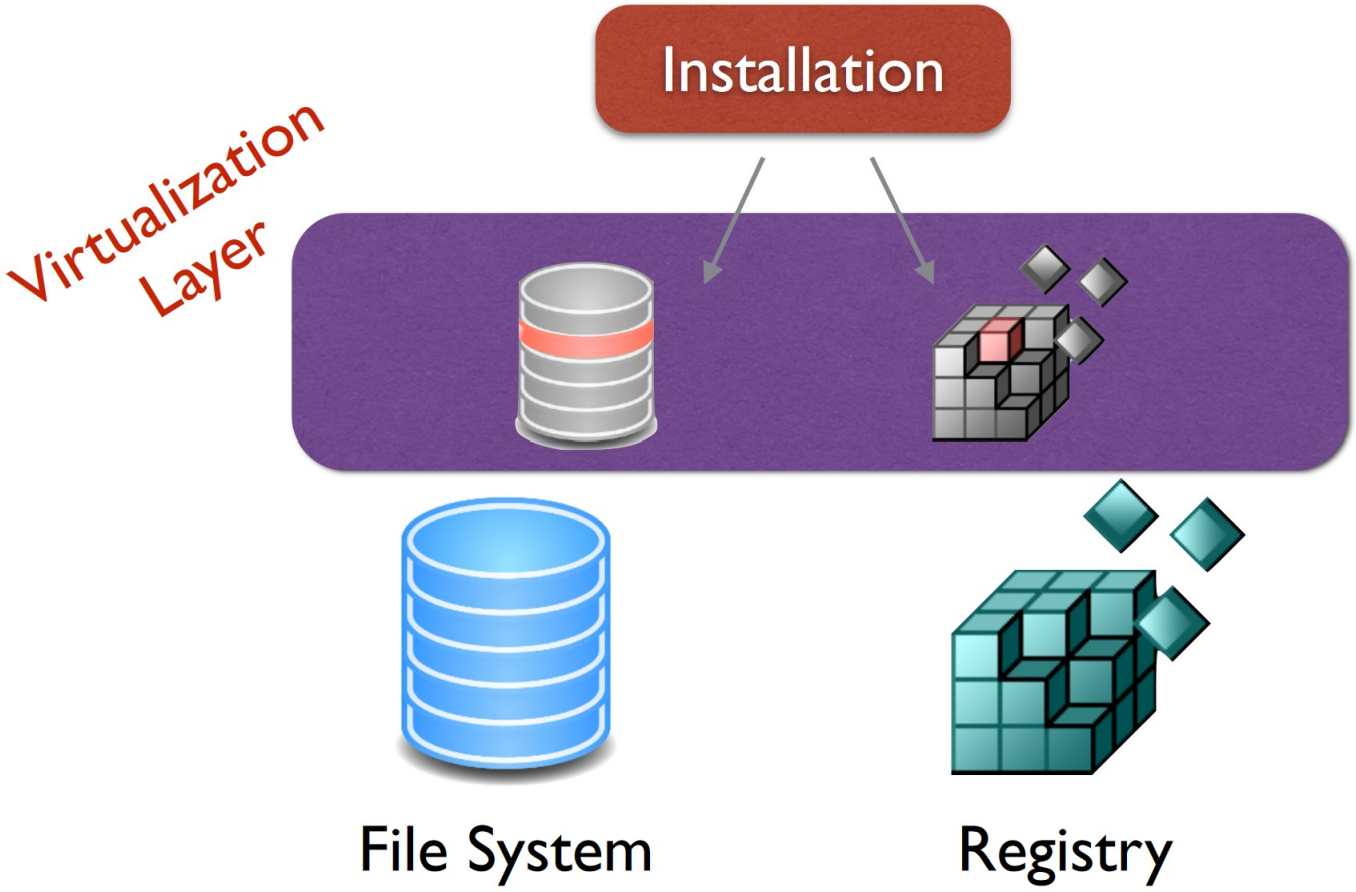
Normal Applications



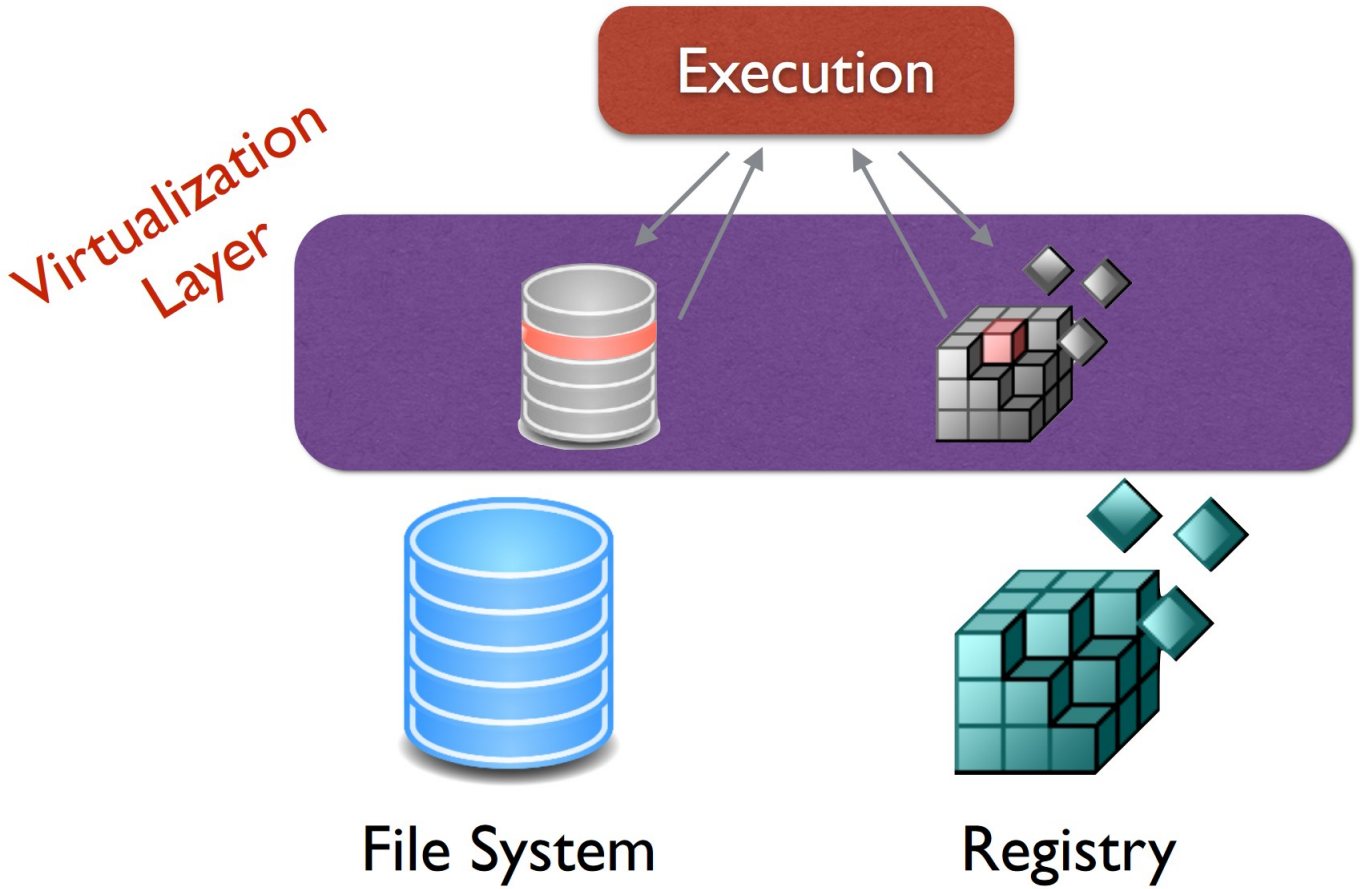
Normal Applications



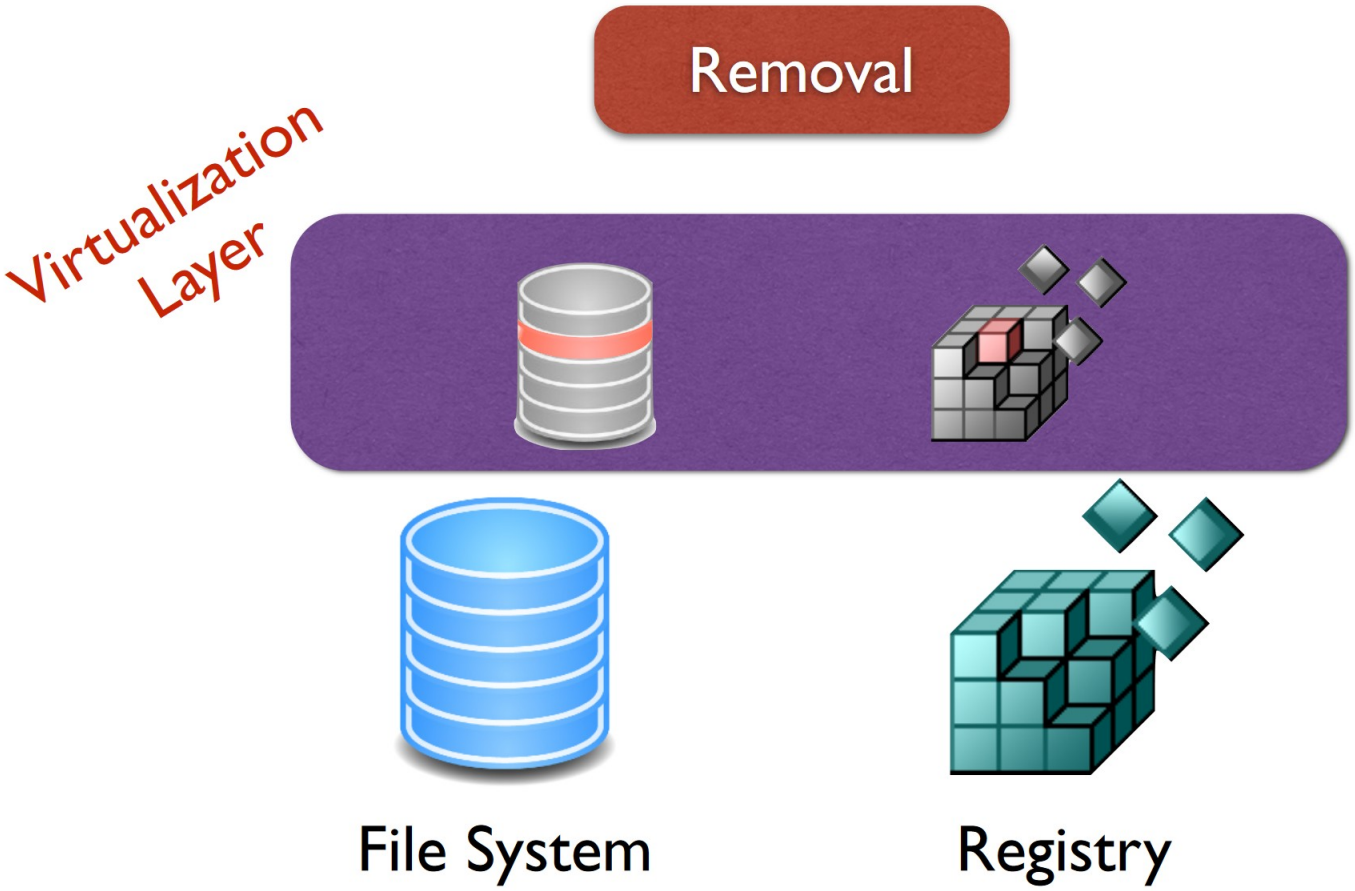
Virtual Applications



Virtual Applications



Virtual Applications



Homework Assignment

- Assignment #01 - Hardware Specification
- Reading