IT-ADVENTURES

MAKING IT FUN

Operating systems administration

Module 6

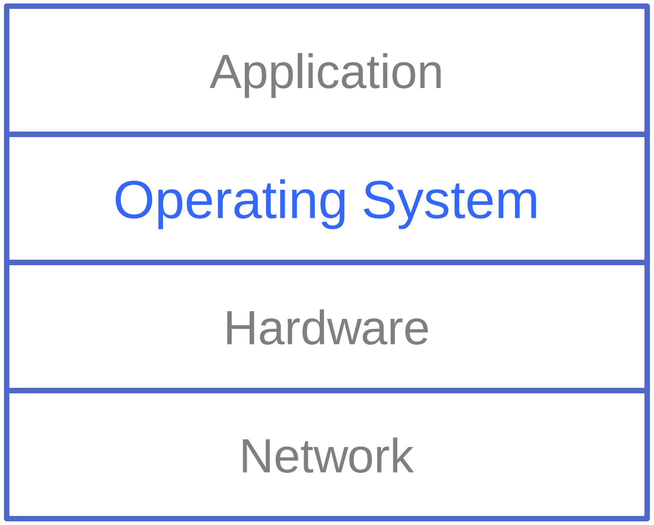
User versus Administrator

- User – person who utilizes services provided
  - Desires service availability, speedy results, peace of mind and ease of use
- Administrator – person responsible for ensuring services are provided
  - Strives to ensure technology meets the expectations of its users
  - Relies on other administrators to be successful

Administrator Objectives

- Top 5
  - Functionality
  - Performance
  - Availability
  - Security
  - Compliance

Common division of administrator duties



Application

Operating System

Hardware

Network

OS Administrator Responsibilities

- Installation
- Configuration
- Maintenance
- Migration – Hardware and/or OS
- Server Termination

OS Installation Process

- Load the OS onto a hardware platform
- Ensure the OS is able to use the various components of the platform
- Provide initial bare essential configuration information

OS Configuration Duties

- OS bundled services
  - Examples: Web server, DNS, Networking
  - Installation may be necessary
- Monitoring capabilities
- Fault tolerance
- Authentication
- Authorization
- File system structures
- Task automation & scheduling

OS Operations/Maintenance

- Functional and Security patches
  - Identify, test and install
- Troubleshooting
- Monitoring
- Operating System upgrades
  - Learn, test, plan, do
- Ensure functional task automation & scheduling
- Responding to requests and concerns

Hardware Migration

- Current system is being replaced by:
  - New hardware
  - Virtualization
- Ensure that current functionality is present on new hardware
- Ensure cutover to new hardware has few or no issues
  - This may require large data transfers before switch is completed

OS Migration

- Major changes in IT strategy cause moving services to new OS family
  - Typically not automated
  - Services software as well as OS may be changing
- Support may be needed to collect and prepare data for new platform
- Automation may need to be translated to be compatible with new platform

Purpose Migration

- Transfer applications and services to other systems
  - Only data preservation and transformation may be needed
- Accommodate needs of new service(s) and application(s)

Server Termination

- Before removal, system administrator or hardware technician must:
  - – Ensure needed data is not lost
  - – Ensure persistent storage like hard drives and BIOS do not contain sensitive information

OS Administrator Responsibilities

- Installation
- Configuration
- Maintenance
- Migration – Hardware and/or OS
- Server Termination

OS Installation

- What do you need to have?
  - Hardware platform
  - Compatible OS distribution & Drivers
  - Network connectivity
- What do you need to know?
  - Administrator’s first password
  - IP address or DHCP
    - Subnet netmask
    - Default route (x.y.z.254)
  - DNS name server (199.100.16.100)
  - Time zone
  - System’s name

- File system configuration
- Network interface type
- Purpose of system
- Language
- Virtual Memory size
- License key information
- Proxy server
  - 199.100.16.100:3128

OS Installation

- What should you consider in general?
  - File systems
    - What applications will be installed?
      - Where should the application files be installed?
      - Where should the data files be installed?
    - How much logging will be done?
      - Where are the logs going to be stored?
      - If local, how long do they need to be kept on disk?
    - Partitions with most free space might be the best place to put potentially large data files.
    - You want to avoid making major storage allocation changes soon after installation

OS Installation

- What should you consider in general?
  - Purpose and desired services
    - Some operating system installations allow tailoring of what services are installed
      - Incomplete set of services installed is inconvenient
      - Extra services results in larger unnecessary CPU, memory, storage footprint
    - Knowing helps with determining the network location of the system
  - Patching the system after install
    - Distribution can be very old
    - In practice, customized installation tools incorporate known good patches

OS Installation

- What should you consider with VM?
  - Balancing resource consumption with other VMs
    - VMWare has clever techniques to allocate more memory and CPU resources than actually exist
      - But, techniques rely on some running VMs to be idle
    - You will need to decide the following initial resource allocation for a VM:

- Host to run VM
- Intended OS for VM
- Number of virtual CPUs
- Amount of RAM
- Disk space – Can prevent installation if too small
- Number of NICS
- What virtual switch(es) to attach NICs to

OS Installation

- What should you consider with VM?
  - VMWare provides resource allocation suggestions based on selected OS.
    - They are worth accepting until you know you need more
  - Many resource adjustments are possible after VM installation
    - Many adjustments cannot be done while the VM is running
  - Locating the installation media
    - ISO or disc can be mounted by ESXi server
    - Media may be local to or is stored on a server accessible to your vSphere client.

OS Installation

- Getting started
  - ISO media are on a volume mounted by ESXi called “ISO Datastore”
  - OS specific installation handouts are available

Before you start

- Determine what network the VM should be part of.
- Locate the switch that serves that network.
  - If not present you will need to build a new vSwitch
- vSwitch assignments can be changed after installation, but it may save you work to identify or build the correct switch before building the VM

Configuration Notes from test via vCenter not local to ESXi

- Configuration = Typical or Custom (choice to select types of devices available to VM during construction)
- Name and Location = Virtual machine’s name (label useful for distinguishing VMs. Does not influence OS); Location is related to “Inventory Location” (placement is for organizational purposes)
- Resource Pool = Select a the pool related to you. (This indirectly assigns the VM to the collection of hardware resources provided to you)
- Storage = Location for the VM’s files (options let VMware decide where to put files or direct the files to a specific datastore resource

More config notes

- Guest Operating System = Windows/Linux/Other and then select specific version. (This is important for the hypervisor to understand and helps with default resource size suggestions)
- Network = You can decide how many NICs to provide the VM initially. More NICs can be added later. With each NIC you must assign it to a switch. If you don't like your choices of switches, then stop you might want to stop and build that switch first. Switch assignment can be changed, but it can affect the initial behavior and security of the VM.

More config notes

- Create a Disk = Select the size of the virtual hard disk of the VM. Select whether you want the drive to be fully constructed and whether you need to have construction performed immediately or you can wait. Lazy = as time permits, Eager = as soon as possible, Thin = construct as needed. (The OS will be told how big its disk is. But thin provisioning does not actually allocate the space designated. Instead it grows the file as needed. This is “slower” and risks an actual falling short on a nearly full disk?)
- Review summary
- Commit
- Boot VM

Installing Windows 7

- Initial boot
- Connect vm to ISO store – Choice to select is “Connects to ISO image on a datastore” Select “ISO Datastore” in the Browse Datastores dialog box. Select an ISO file in this case Windows_7_64 bit.iso
  - Put focus on console and press enter
- First dialog asks for Language, Time and currency format, keyboard or input method – Default values are fine
- Installation method upgrade or custom – choose custom
- Accept license terms
- User account name and Computer name
- Password for new account (ITAdventureland)
- Protecting the computer – Use recommended settings, Install important updates only, ask me later
- Time zone, time and date
- Choose a network type – Home, Work, Public (sets initial security settings)

Installing Windows 7

- Initial network configuration was not done
  - Assumes DHCP but that requires a DHCP server attached to same switch as NIC
  - Connecting to external network requires a path to it or be attached to the external NIC’s switch 6.87.159.0/24, router 6.87.159.2546
- Install VMWare tools installation (VM/Guest/Install Vmware tools) – Typical install is fine

END

VIDEO SEGMENT 1

Key Administration Concepts

- Authentication
- Authorization
- File Systems
- Monitoring
- Troubleshooting

Authentication

- Dominant method – Passwords
- Local vs Central Authentication
  - Local: User credentials managed by individual system
  - Central: Systems refer to a central credential store (ex. Active Directory)

Central Authentication

- Client OS
  - Default is local
  - Requires configuration
    - Client needs to be aware of central store
    - Authorization to use central store may be required
      - Windows requires the client “join” the domain
- Server OS
  - Depends on server role and OS type
    - Unix/Linux typically default local
    - Windows standalone – local
    - Windows domain controllers - central

Central Authentication

- Advantages
  - Know one password to access multiple systems
  - One place to create and manage users
  - Common password policy
- Disadvantages
  - Single password to compromise
  - Complexity – network must work or have credentials cached, software configuration and operational glitches

Central Authentication

- Unix/Linux support for pluggable authentication modules (PAM)
  - Supports integration with Windows user credentials

Authorization

- Roles – A function assumed by a user when using a system
  - Users may be assigned multiple roles
  - Roles are assigned permissions, role based access control (RBAC)
  - Unix: root Windows: Administrator, Power User, User, Guest
- User level
  - Individuals are assigned permissions

Authorization Controls

- Process control
  - Limit who can manage services
  - Limit who can execute a command or run a program
    - Unix uses root or sudo or su
    - Windows uses roles (ex. Administrator, Power User) or authenticated privilege escalation
- File system control
  - Many hard drive file systems enforce access control

File System Controls

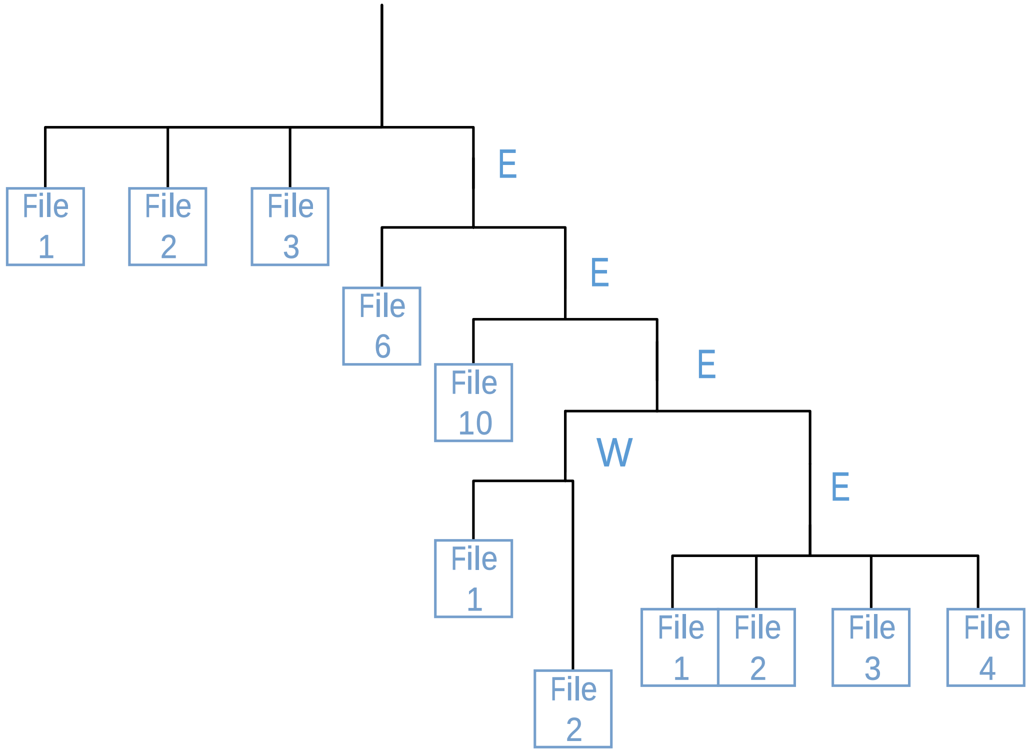
- File system permissions
  - Read, write, execute (Unix)
  - Full control, Modify, Read & Execute, Read, Write (basic Windows)
- Who can be authorized
  - Individual users, groups of users, roles
  - Unix has owner/group/other
- Target of authorization
  - Directories and files
- Who can authorize
  - Traditionally owner and administrators

Balancing Act

- Permissions can promote
  - Stability
  - Security
  - Safety
- Overly restrictive permissions
  - Prevent functionality
  - Limit performance
  - Data loss
  - Interrupt operations

File System Structures

- Structures in the form of an upside down tree



Copyright 2013 Iowa State University

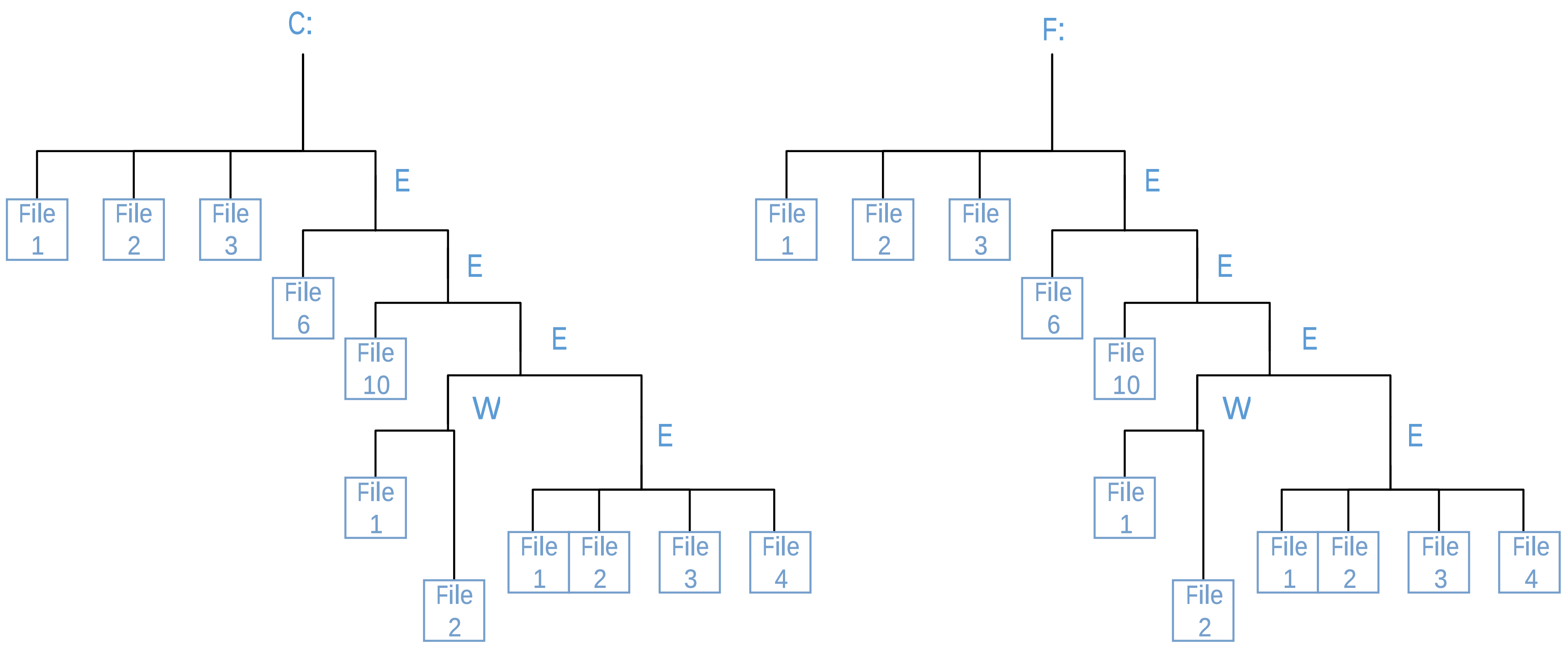
File System Structure

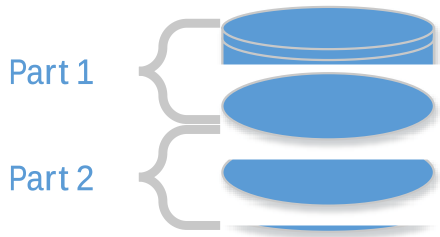
- Every file or directory must have a unique absolute name
- Each file in a directory must have a unique name
  - Between directories multiple files can have same name
- Directories are special files
  - Contain listing of files and subdirectories located in directory, physical locations within file system and permissions to files and subdirectories

Logical Windows File System

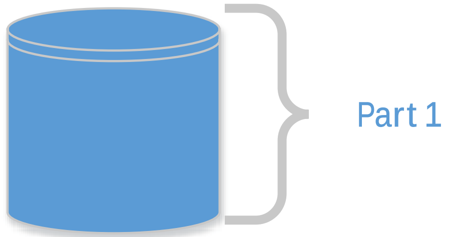
- Media is organized into logical containers
- These containers are called partitions
  - Each unique storage device has at least 1 partition
  - Partitions have been structured with a file system
  - Windows treats each partition as a unique file system
    - Partitions can be on local disk
    - CD Rom/DVD
    - Network file share

Logical Windows File System





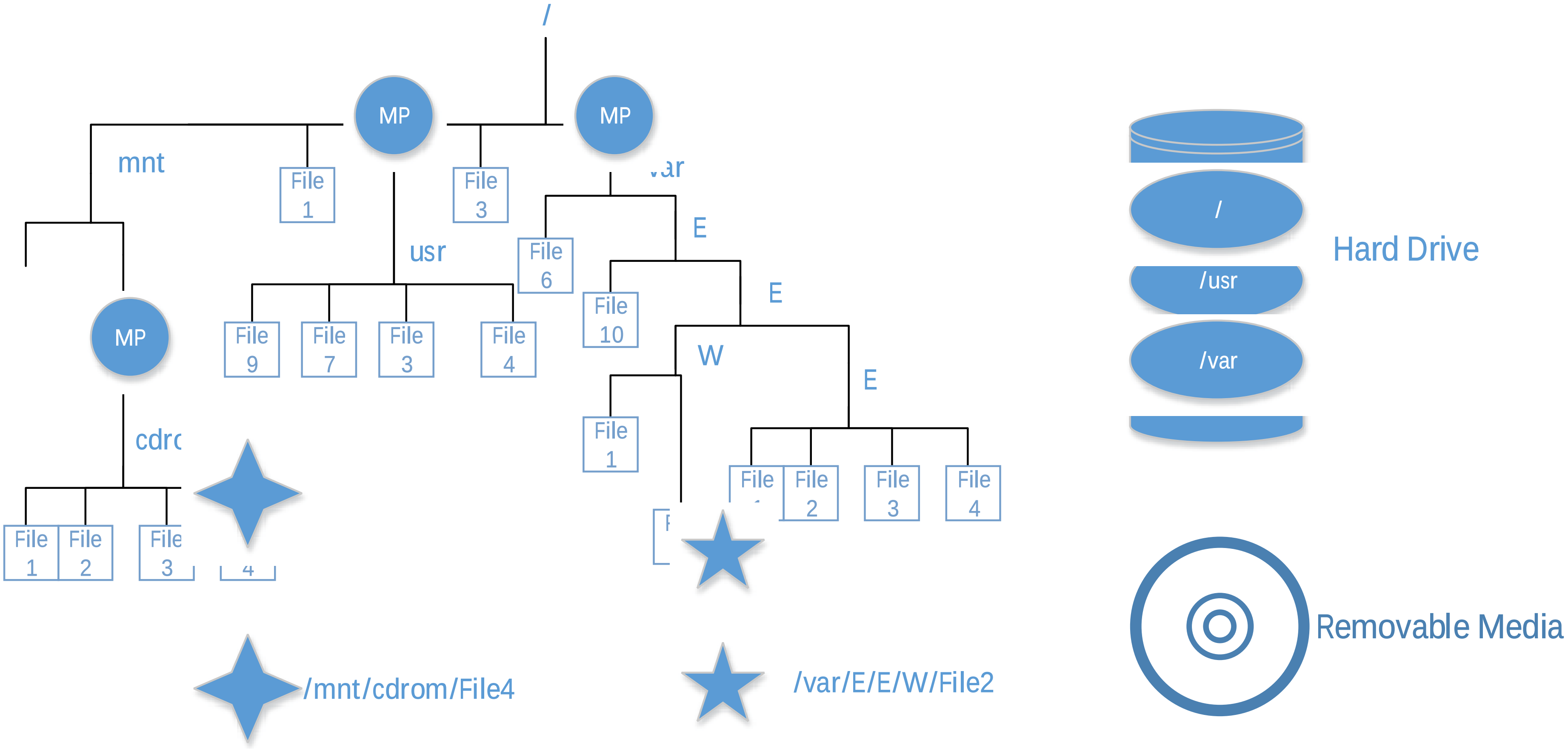
Same drive two different partitions
Two different drives each with at least one partition



Logical Unix File System

- Like Windows, all media has at least one partition organized with a file system
- Each independent partition has a root directory “/”.
- To access a partition it must be “mounted”
- Mounting grafts an independent partition into the active file system.
  - There is only one root directory on active system
  - Mount points are directories defined in the active file system mounted

Logical Unix File System



Common File System Activities

- Mount file systems
- Format partitions
- Verify file system’s integrity
- Read
- Search for files or locate content
- Modify content or file names
- Delete
- Create directories
- Create files
- Copy files and directories
- Bundle files and directories
- Deposit multiple files and directories
- Manage space
- Manage permissions
- Backup & restore

Monitoring

- Awareness of status of:
  - – OS and system configuration
  - – Resource consumption
    - Available capacity
  - – Activities being performed
  - – Security
    - Operational status of controls
    - Violations of controls
  - – Operational errors or warnings
    - System level – operations, patches, hardware issues
    - Applications – operations
    - Task Automation

OS and System Configuration

- Status tools available for:
  - OS recognition of hardware
  - OS Type
  - System name
  - File storage configuration
  - Network configuration
  - File system structure

Resource Consumption

- Computing status and statistics
- Networking status and statistics
- File system usage
- I/O Statistics

Activities Performed

- Current users logged in
- Process list
- Security controls
  - Logging authorized resource use provides a trail to follow
- Event log entries by applications or services may help

Operational Monitoring

- Operational events can indicate serious problems
- Patches may not install
- Excessive heat is bad
  - Systems might be in a room miles away
- Imminent disk failure may be reported
- Task automation should generate log events to know of failures and help troubleshooting
- Backup systems may fail to backup or restore

Security Monitoring

- Operational controls
  - Verify desired controls are operating
  - Verify desired controls are configured properly
  - Verify any needed signature updates have occurred (ex. Anti-virus)
  - Verify system integrity
    - Verify desired controls have not been replaced with unauthorized substitutes
    - Verify sensitive files have not been altered unexpectedly

Security Monitoring

- Policy enforcement monitoring
  - Enable logging where needed
  - Logging authorized and denied activity may be necessary
  - Review logs that are generated
  - Follow-up on suspicious activity that is unexpected and unexplained
    - This can be challenging
      - Volume, tools, information quality and concepts

Troubleshooting

- Similar to a murder mystery
  - Who, what, when, how, why?
- Who is many times replaced by which
  - Which component is reporting a problem?
  - What appears to be the symptoms?
  - When did this problem appear to start?
  - How could this problem have occurred?
  - Why did this problem occur?

Post Troubleshooting

- How can we avoid this problem?
- What could we be doing differently?
- Who else should know, so it does not happen elsewhere?

Troubleshooting Tips

- Ask yourself, “Was whatever that is ‘broken’ ever ‘work’ correctly?”
  - No, issue might be with design, implementation, installation or configuration
  - Yes, ask yourself “What changed?” or “Could an unexpected event have caused this?”
- Determining the possible causes helps to narrow focus and ask good questions

Troubleshooting Tips

- Understanding how things work is key to building a good set of possible causes
- Eliminating possible causes:
  - Pick a possible cause and try to rule it out
  - Start with ruling out the simple
    - Ex. Computer is unplugged, wrong network port
  - Ruling out a cause relies on aligning a cause to the symptoms
    - This too requires an understanding of how things work
    - Symptoms need to be accurate and ideally complete
      - You may be relying on others to report the symptoms
      - Others may not know what behavior to communicate or how
        - Good human sources are those who have an understanding
    - Poor alignment justifies the cause to be ruled out
      - Single cause is most likely, but multiple causes are possible (rule out simple 1st)
        - Multiple causes may explain the symptoms better than one

Troubleshooting Tips

- Eliminating possible causes (contd.):
  - Ask probing questions that can reveal additional symptoms or conditions that support or rule out a possible cause
- Identifying the root cause or the “why”
  - Important
    - Essential for knowing what to “fix”.
      - Treating symptoms may not resolve the problem
    - Problem is not resolved until knowing why, but sometimes symptoms disappear before knowing
  - Ideally the conditions of the problem align with no or with minor discrepancy with the root cause candidate chosen. The alignment is ideally justified by observed evidence.