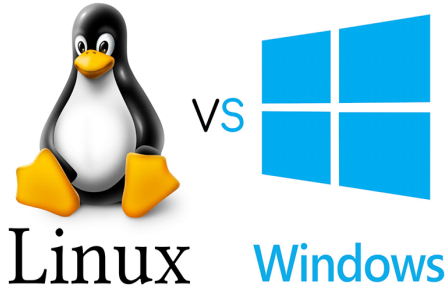
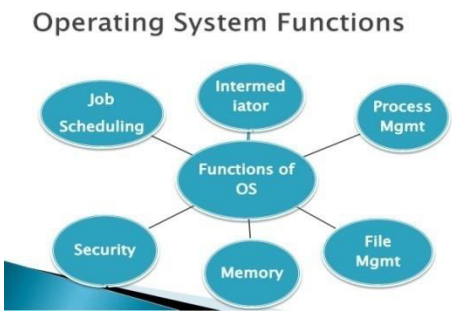
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week15Day1 : OS Management, System Monitoring Tools , Linux Performance Optimization, Resource Monitoring Tools, Application Performance Tuning, Data Collector Sets, Alerts





Linux System Monitoring Tools

- **top – Process activity monitoring command**
- top command display Linux processes. It provides a dynamic real-time view of a running system i.e. actual process activity. By default, it displays the most CPU-intensive tasks running on the server and updates the list every five seconds.

Linux System Monitoring Tools (top)

Hot Key	Usage
t	Displays summary information off and on.
m	Displays memory information off and on.
A	Sorts the display by top consumers of various system resources. Useful for quick identification of performance-hungry tasks on a system.
f	Enters an interactive configuration screen for top. Helpful for setting up top for a specific task.
o	Enables you to interactively select the ordering within top.
r	Issues renice command.
k	Issues kill command.
z	Turn on or off color/mono

Linux System Monitoring Tools

- **vmstat – Virtual memory statistics**
- The vmstat command reports information about processes, memory, paging, block IO, traps, and cpu activity.
  # vmstat 3
- **Display Memory Utilization Slabinfo**
- # vmstat -m
- **Get Information About Active / Inactive Memory Pages**
- # vmstat -a

Linux System Monitoring Tools

- **w – Find out who is logged on and what they are doing**
- w command displays information about the users currently on the machine, and their processes.
  # w username

Linux System Monitoring Tools

- **uptime – Tell how long the Linux system has been running**
- uptime command can be used to see how long the server has been running. The current time, how long the system has been running, how many users are currently logged on, and the system load averages for the past 1, 5, and 15 minutes.
  # uptime

Linux System Monitoring Tools

- **ps – Displays the Linux processes**
- ps command will report a snapshot of the current processes. To select all processes use the -A or -e option:
  # ps -A
- **Show Long Format Output**
- # ps -Al
  To turn on extra full mode (it will show command line arguments passed to process):
  # ps -AlF
- **Display Threads (LWP and NLWP)**
- # ps -AlFH
- **Watch Threads After Processes**
- # ps -AlLm

Linux System Monitoring Tools

- **free – Show Linux server memory usage**
- free command shows the total amount of free and used physical and swap memory in the system, as well as the buffers used by the kernel.
  # free

Linux System Monitoring Tools

- **iostat – Montor Linux average CPU load and disk activity**
- iostat command report Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network filesystems (NFS).
  # iostat

Linux System Monitoring Tools

- **sar – Monitor, collect and report Linux system activity**
- sar command used to collect, report, and save system activity information. To see network counter, enter:
  # sar -n DEV | more
  The network counters from the 24th:
  # sar -n DEV -f /var/log/sa/sa24 | more
  You can also display real time usage using sar:
  # sar 4 5

Linux System Monitoring Tools

- **mpstat – Monitor multiprocessor usage on Linux**
- mpstat command displays activities for each available processor, processor 0 being the first one. mpstat -P ALL to display average CPU utilization per processor:
  # mpstat -P ALL

Linux System Monitoring Tools

- **pmap – Montor process memory usage on Linux**
- pmap command report memory map of a process. Use this command to find out causes of memory bottlenecks.
  # pmap -d PID
  To display process memory information for pid # 47394, enter:
  # pmap -d 47394

Linux System Monitoring Tools

- **netstat – Linux network and statistics monitoring tool**
- netstat command displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
  # netstat -tulpn
  # netstat -nat

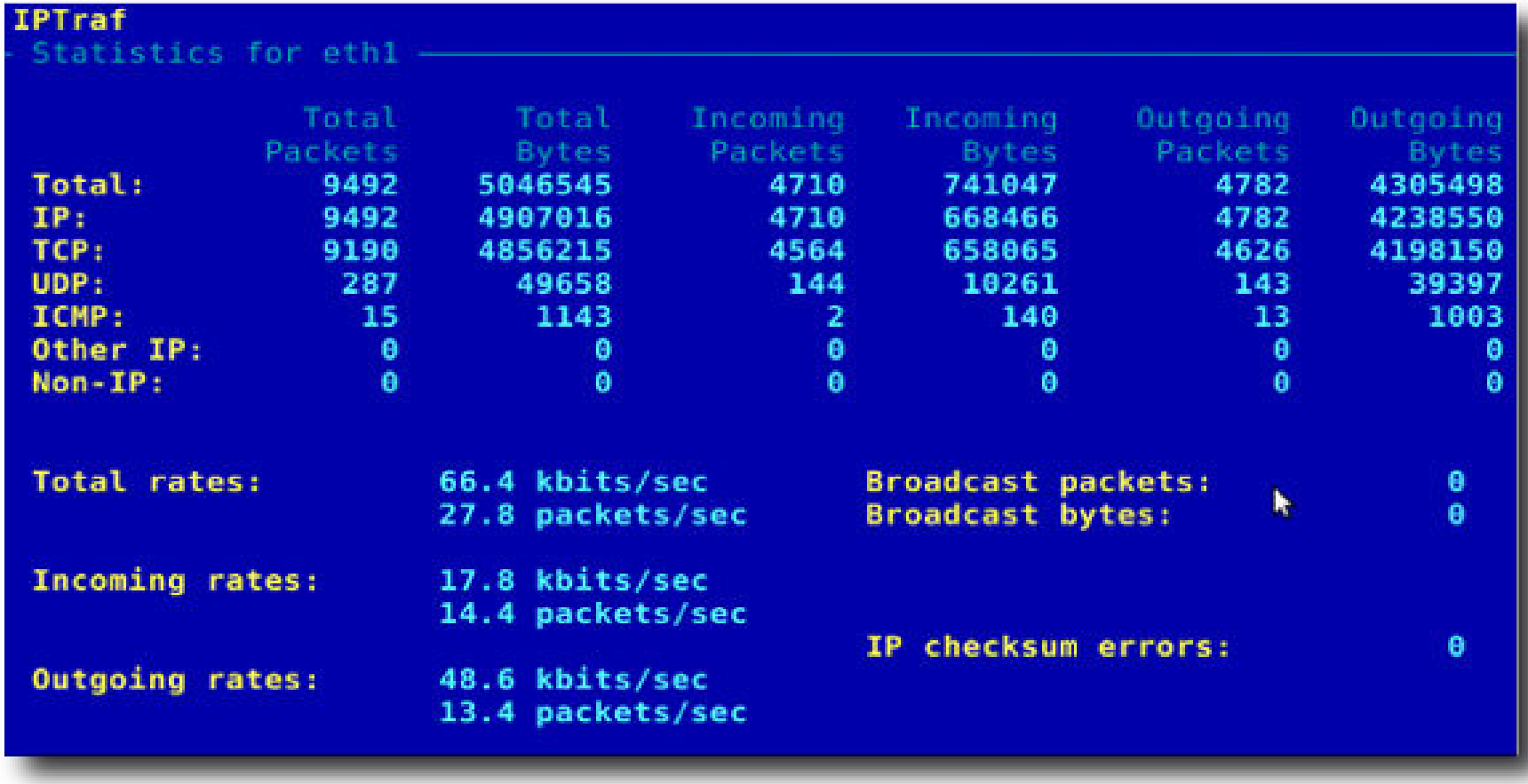
Linux System Monitoring Tools

- **ss – Network Statistics**
- ss command use to dump socket statistics. It allows showing information similar to netstat. Please note that the netstat is mostly obsolete. Hence you need to use ss command. To ss all TCP and UDP sockets on Linux:
  # ss -t -a
  OR
  # ss -u -a
  Show all TCP sockets with process SELinux security contexts:
  # ss -t -a -Z

Linux System Monitoring Tools

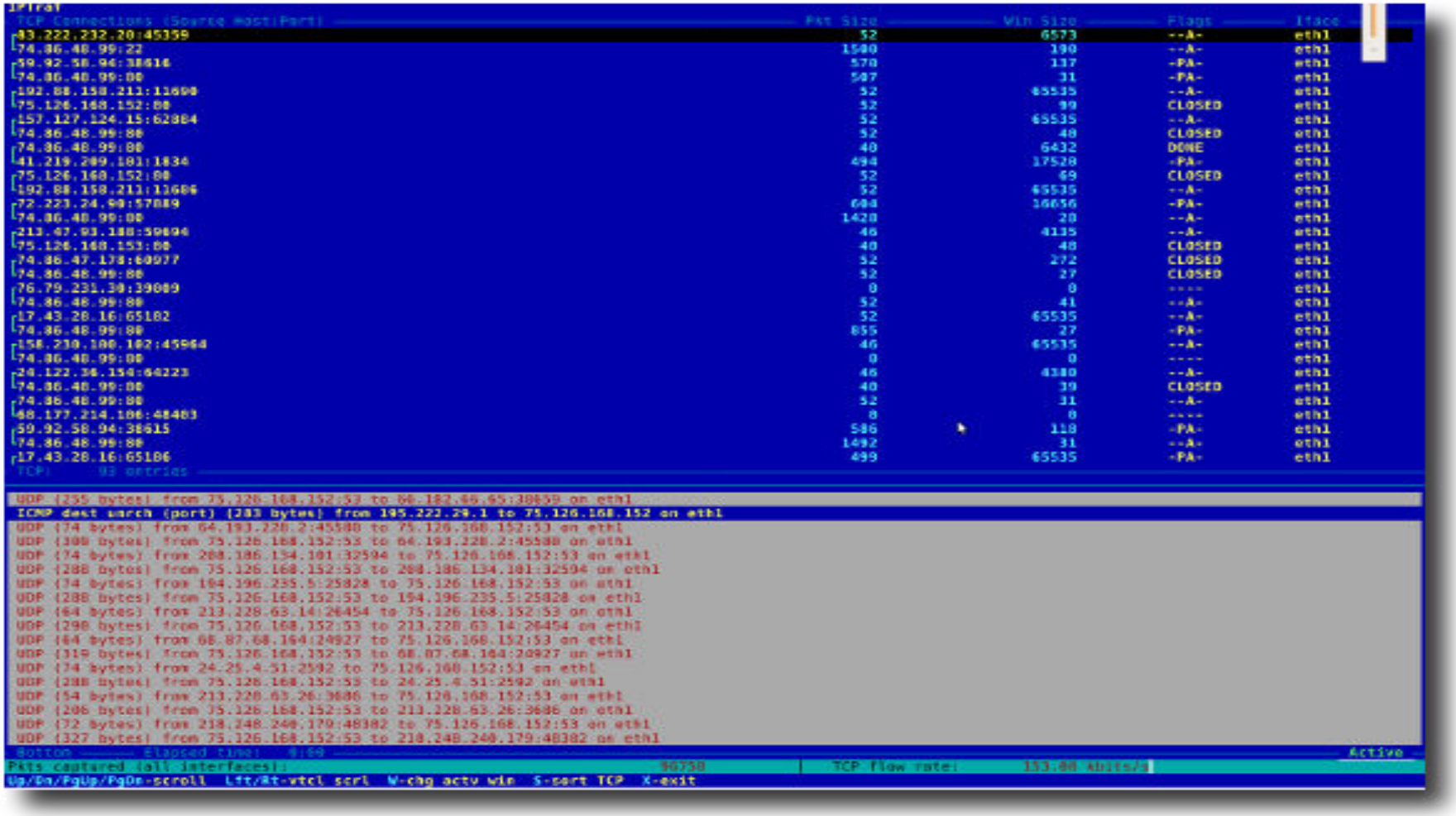
- **iptraf – Get real-time network statistics on Linux**
- iptraf command is interactive colorful IP LAN monitor. It is an ncurses-based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP and OSPF information, Ethernet load info, node stats, IP checksum errors, and others. It can provide the following info in easy to read format:
- Network traffic statistics by TCP connection
- IP traffic statistics by network interface
- Network traffic statistics by protocol
- Network traffic statistics by TCP/UDP port and by packet size
- Network traffic statistics by Layer2 address

Linux System Monitoring Tools



General interface statistics: IP traffic statistics by network interface

Linux System Monitoring Tools



Network traffic statistics by TCP connection

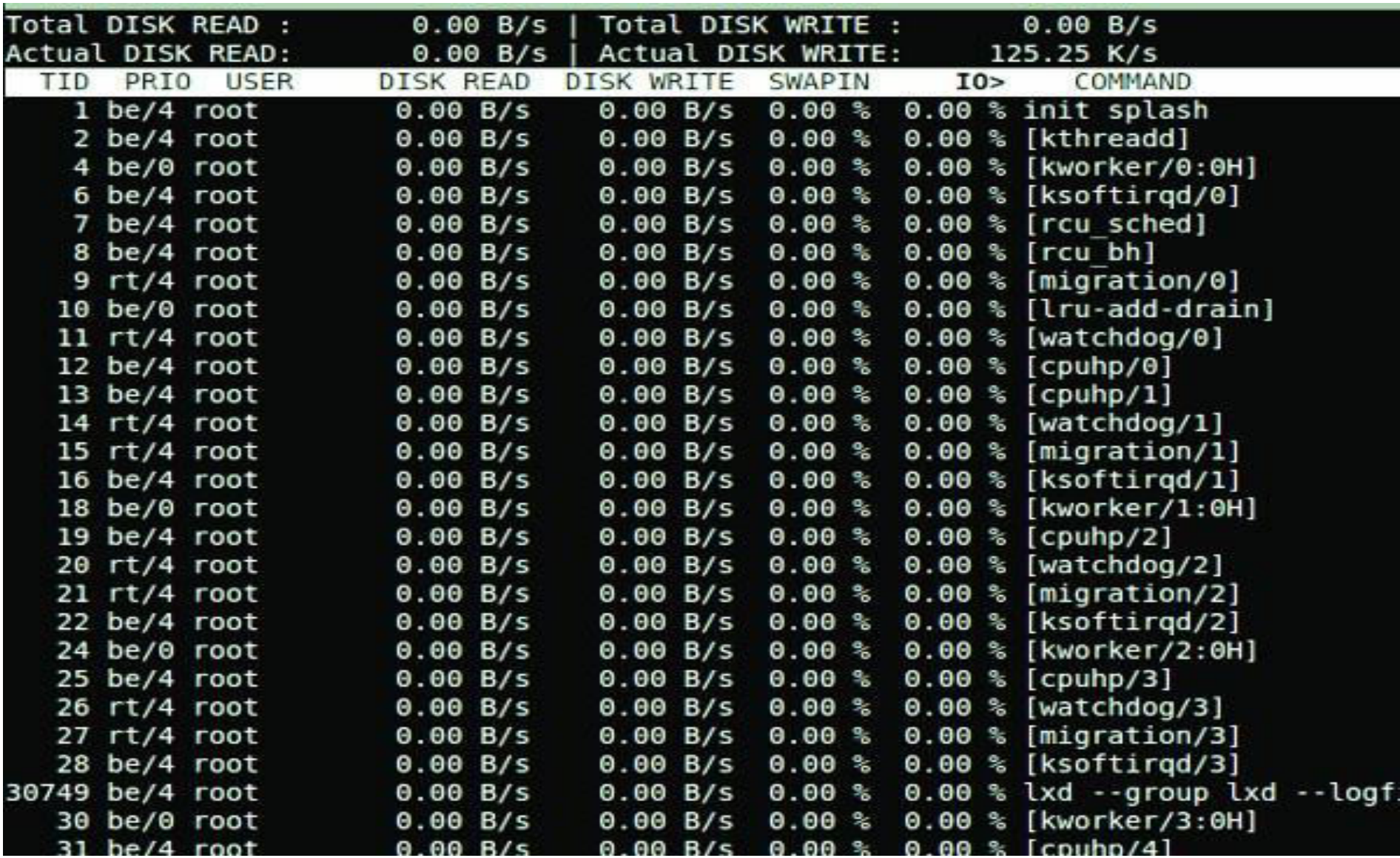
Linux System Monitoring Tools

- **tcpdump – Detailed network traffic analysis**
- tcpdump command is simple command that dump traffic on a network. However, you need good understanding of TCP/IP protocol to utilize this tool. For.e.g to display traffic info about DNS, enter:
  # tcpdump -i eth1 'udp port 53'
  View all IPv4 HTTP packets to and from port 80, i.e. print only packets that contain data, not, for example, SYN and FIN packets and ACK-only packets, enter:
  # tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)‘
- Show all FTP session to 202.54.1.5, enter:
  # tcpdump -i eth1 'dst 202.54.1.5 and (port 21 or 20'
  Print all HTTP session to 192.168.1.5:
  # tcpdump -ni eth0 'dst 192.168.1.5 and tcp and port http'

Linux System Monitoring Tools

- **iotop – Linux I/O monitor**
- iotop command monitor, I/O usage information, using the Linux kernel. It shows a table of current I/O usage sorted by processes or threads on the server.
  $ sudo iotop

Linux System Monitoring Tools



```
Total DISK READ :       0.00 B/s | Total DISK WRITE :       0.00 B/s
Actual DISK READ:       0.00 B/s | Actual DISK WRITE:     125.25 K/s
  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN      IO>    COMMAND
    1 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % init splash
    2 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kthreadd]
    4 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/0:0H]
    6 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
    7 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcu_sched]
    8 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [rcu_bh]
    9 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/0]
   10 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [lru-add-drain]
   11 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/0]
   12 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuhp/0]
   13 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuhp/1]
   14 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/1]
   15 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/1]
   16 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/1]
   18 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/1:0H]
   19 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuhp/2]
   20 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/2]
   21 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/2]
   22 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/2]
   24 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/2:0H]
   25 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuhp/3]
   26 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/3]
   27 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/3]
   28 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/3]
30749 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % lxd --group lxd --logf
   30 be/0 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kworker/3:0H]
   31 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuhp/4]
```

Linux System Monitoring Tools

- **htop – interactive process viewer**
- htop is a free and open source ncurses-based process viewer for Linux. It is much better than top command. Very easy to use. You can select processes for killing or renicing without using their PIDs or leaving htop interface.
  $ htop

Linux System Monitoring Tools

- **atop – Advanced Linux system & process monitor**
- atop is a very powerful and an interactive monitor to view the load on a Linux system. It displays the most critical hardware resources from a performance point of view. You can quickly see CPU, memory, disk and network performance. It shows which processes are responsible for the indicated load concerning CPU and memory load on a process level.
-

  $ atop

Linux System Monitoring Tools

- **ac and lastcomm –**
- You must monitor process and login activity on your Linux server. The psacct or acct package contains several utilities for monitoring process activities, including:
- ac command : Show statistics about users' connect time
- lastcomm command : Show info about about previously executed commands
- accton command : Turns process accounting on or off
- sa command : Summarizes accounting information

Linux System Monitoring Tools

- **monit – Process supervision**
- Monit is a free and open source software that acts as process supervision. It comes with the ability to restart services which have failed. You can use Systemd, daemontools or any other such tool for the same purpose.

Linux System Monitoring Tools

- **nethogs- Find out PIDs that using most bandwidth on Linux**
- NetHogs is a small but handy net top tool. It groups bandwidth by process name such as Firefox, wget and so on. If there is a sudden burst of network traffic, start NetHogs. You will see which PID is causing bandwidth surge.
  $ sudo nethogs

Linux System Monitoring Tools

- **iftop – Show bandwidth usage on an interface by host**
- iftop command listens to network traffic on a given interface name such as eth0. It displays a table of current bandwidth usage by pairs of hosts.
  $ sudo iftop

Linux System Monitoring Tools

- **vnstat – A console-based network traffic monitor**
- vnstat is easy to use console-based network traffic monitor for Linux. It keeps a log of hourly, daily and monthly network traffic for the selected interface(s).
  $ vnstat

Linux System Monitoring Tools

- **nmon – Linux systems administrator, tuner, benchmark tool**
- nmon is a Linux sysadmin's ultimate tool for the tunning purpose. It can show CPU, memory, network, disks, file systems, NFS, top process resources and partition information from the cli.
  $ nmon

Linux System Monitoring Tools

- **glances – Keep an eye on Linux system**
- glances is an open source cross-platform monitoring tool. It provides tons of information on the small screen. It can also work in client/server mode.
  $ glances

Linux System Monitoring Tools

- **strace – Monitor system calls on Linux**
- Want to trace Linux system calls and signals? Try strace command. This is useful for debugging webserver and other server problems. See how to use to trace the process and see What it is doing.

Linux System Monitoring Tools

- **/proc/ file system – Various Linux kernel statistics**
- /proc file system provides detailed information about various hardware devices and other Linux kernel information.
  See Linux kernel /proc documentations for further details.
  Common /proc examples:
  # cat /proc/cpuinfo
  # cat /proc/meminfo
  # cat /proc/zoneinfo
  # cat /proc/mounts

Linux System Monitoring Tools

- **Nagios – Linux server/network monitoring**
- Nagios is a popular open source computer system and network monitoring application software.
- Monitor all your hosts, network equipment and services.
- It can send alert when things go wrong and again when they get better. FAN is "Fully Automated Nagios". FAN goals are to provide a Nagios installation including most tools provided by the Nagios Community. FAN provides a CDRom image in the standard ISO format, making it easy to easilly install a Nagios server. A wide bunch of tools are including to the distribution, in order to improve the user experience around Nagios.

Linux System Monitoring Tools

- **Cacti – Web-based Linux monitoring tool**
- Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality.
- Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices. It can provide data about network, CPU, memory, logged in users, Apache, DNS servers and much more. See how to install and configure Cacti network graphing tool under CentOS / RHEL.

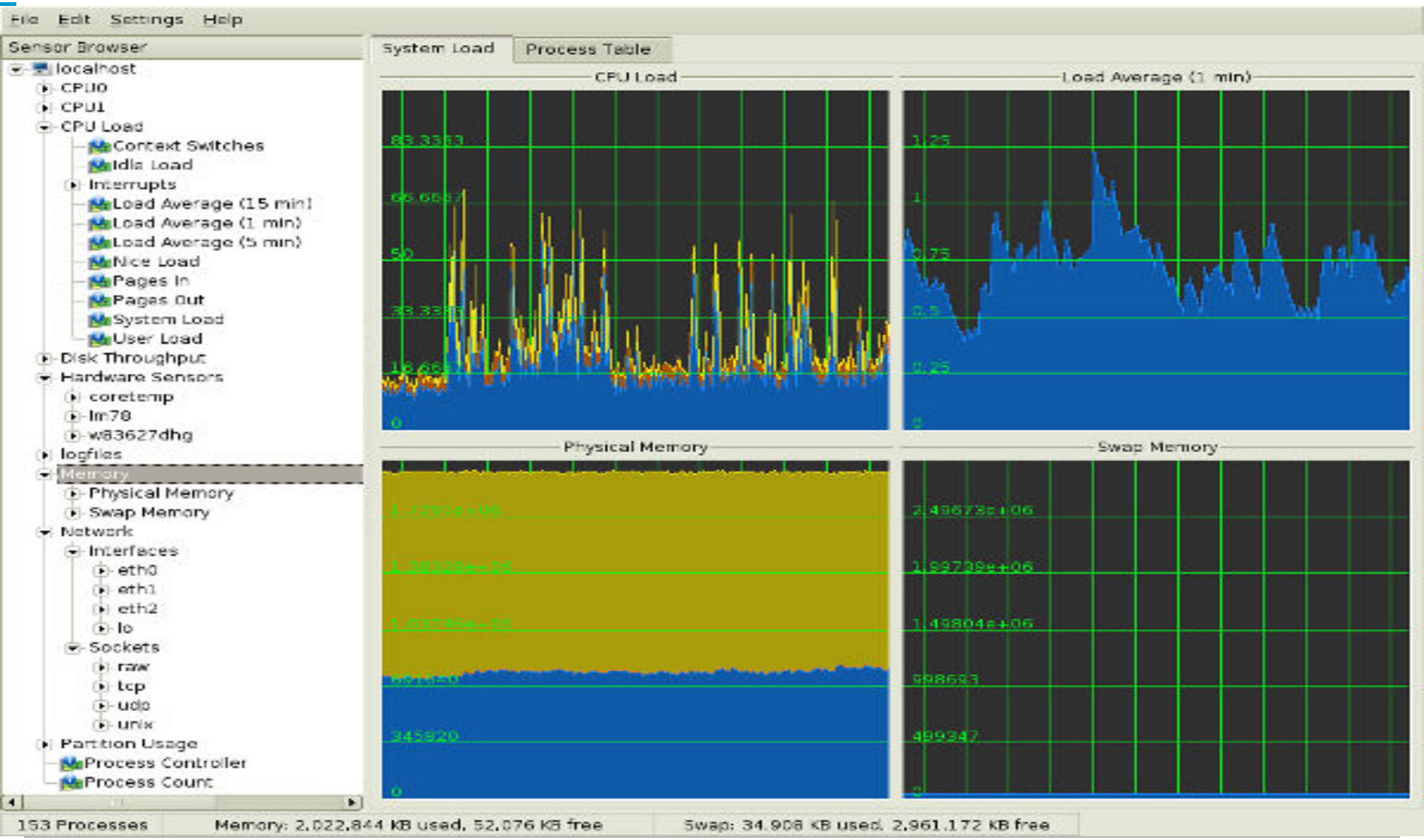
Linux System Monitoring Tools

- **KDE System Guard – Real-time Linux systems reporting and graphing**
- KSysguard is a network enabled task and system monitor application for KDE desktop.
- This tool can be run over ssh session. It provides lots of features such as a client/server architecture that enables monitoring of local and remote hosts.
- The graphical front end uses so-called sensors to retrieve the information it displays.

Linux System Monitoring Tools

- **KDE System Guard – Real-time Linux systems reporting and graphing**
- A sensor can return simple values or more complex information like tables.
- For each type of information, one or more displays are provided.
- Displays are organized in worksheets that can be saved and loaded independently from each other.
- KSysguard is not only a simple task manager but also a very powerful tool to control large server farms.

Linux System Monitoring Tools



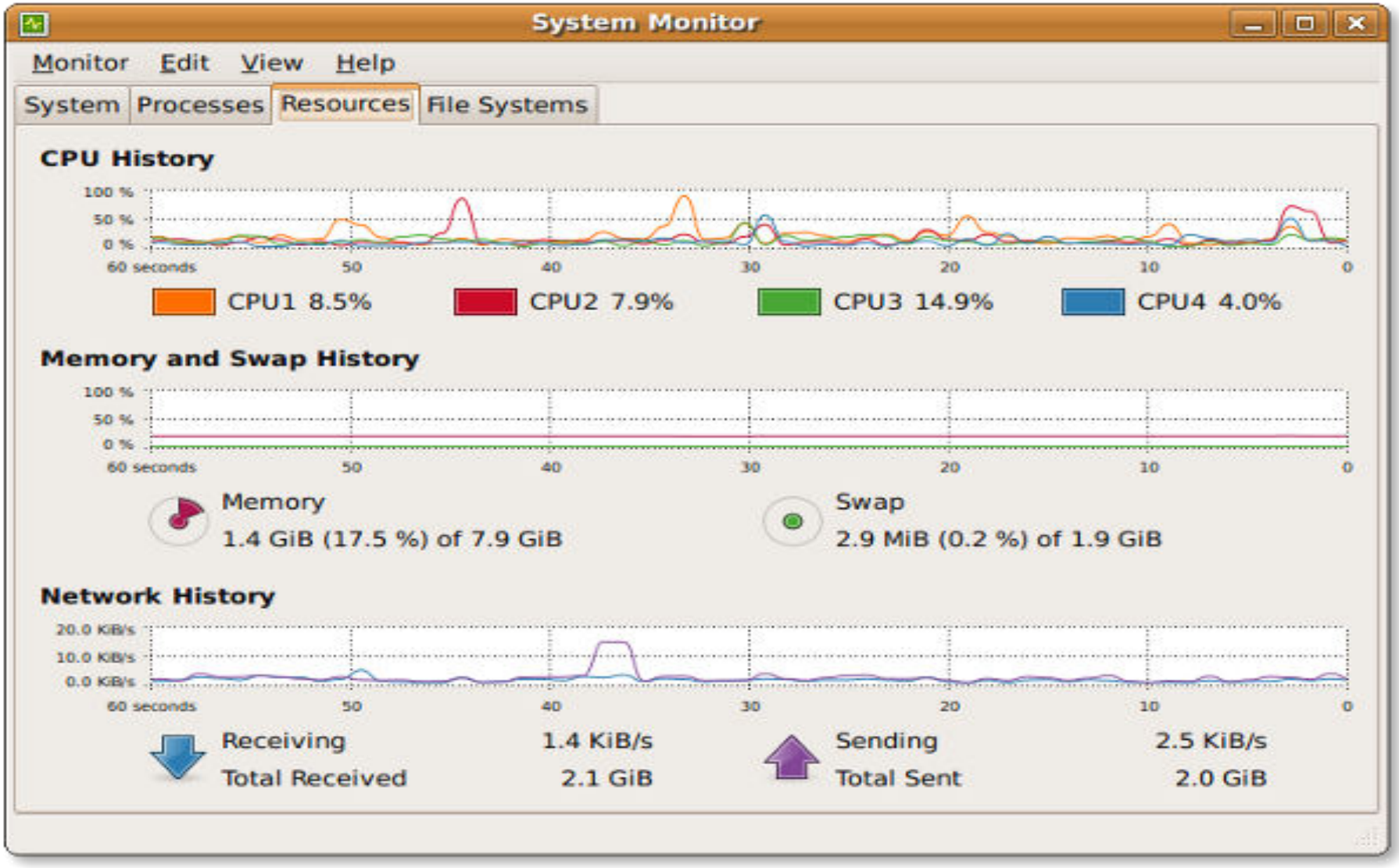
Linux System Monitoring Tools

- **Gnome Linux system monitor**
- The System Monitor application enables you to display basic system information and monitor system processes, usage of system resources, and file systems. You can also use System Monitor to modify the behavior of your system. Although not as powerful as the KDE System Guard, it provides the basic information which may be useful for new users:
- Displays various basic information about the computer's hardware and software.
- Linux Kernel version
- GNOME version
- Hardware

Linux System Monitoring Tools

- **Gnome Linux system monitor**
- Installed memory
- Processors and speeds
- System Status
- Currently available disk space
- Processes
- Memory and swap space
- Network usage
- File Systems
- Lists all mounted filesystems along with basic information about each.

Linux System Monitoring Tools



Linux System Monitoring Tools

- nmap – scan your server for open ports.
- lsof – list open files, network connections and much more.
- ntop web based tool – ntop is the best tool to see network usage in a way similar to what top command does for processes i.e. it is network traffic monitoring software. You can see network status, protocol wise distribution of traffic for UDP, TCP, DNS, HTTP and other protocols.

Linux System Monitoring Tools

- Conky – Another good monitoring tool for the X Window System. It is highly configurable and is able to monitor many system variables including the status of the CPU, memory, swap space, disk storage, temperatures, processes, network interfaces, battery power, system messages, e-mail inboxes etc.
- GKrellM – It can be used to monitor the status of CPUs, main memory, hard disks, network interfaces, local and remote mailboxes, and many other things.
- mtr – mtr combines the functionality of the traceroute and ping programs in a single network diagnostic tool.
- vtop – graphical terminal activity monitor on Linux
- gtop – Awesome system monitoring dashboard for Linux/macOS Unix terminal
-

Open Source Offers a Different Perspective

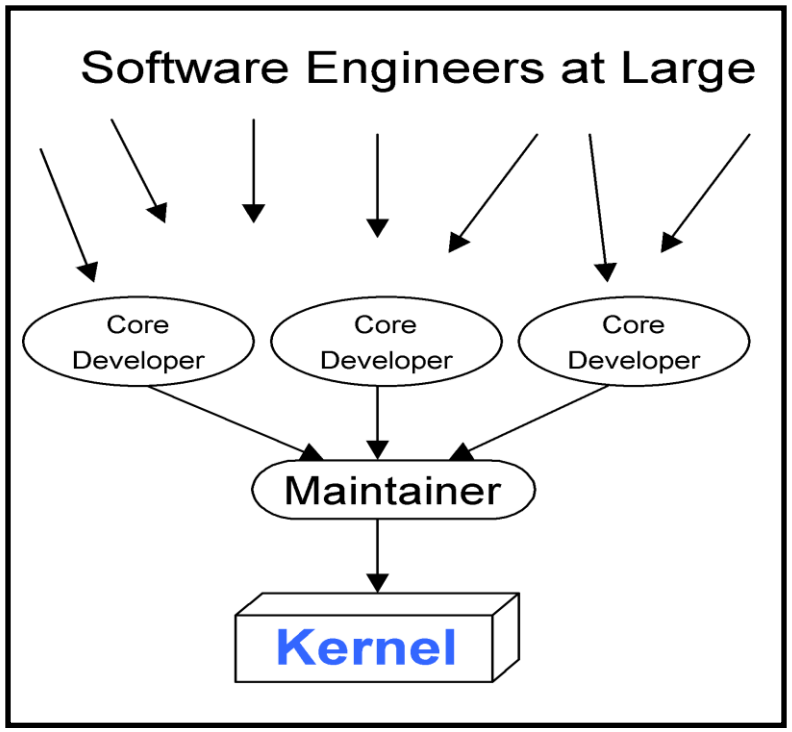
The Open Source Model is a very pragmatic way of evolving software in a rapidly changing environment. It harnesses the collective wisdom, experiences, expertise and requirements of its most demanding users to ensure that their needs are rapidly met.

- How and Why it Works…
  - Open Source development
  - Defect & fixes
  - Releases
  - Darwinian Nature
  - Community and Integrity
  - Release early, release often
- Public Licensing
  - Accountability
  - Internal & external distribution
- No Vendor Lock-in

- Linux is Open Source
  - It does scale
  - It is ready for the enterprise
  - It runs on business apps
  - It is secure
  - There are skills available

What is Open Source?

- Community develops, debugs, maintains
- Usually high quality, high performance software
- Reliable, flexible, low cost
- More information: www.opensource.org
- Examples of Open Source Software:
  - Apache — web server
  - Eclipse — app development
  - Gnome — desktop environment
  - Mozilla — (Netscape) browser
  - Open Office — (Star Office) productivity suite
  - Perl — language
  - Samba — file/print
  - SendMail — mail server
  - Tomcat — application server



Linux Performance Optimization Fundamentals

- Hardware and software configuration options
- Understand performance tools and how to use them
- Analysis of results obtained from the tools so suitable changes can be made to positively impact the server performance

Linux Server Performance Optimization Objectives

- **To conduct deep-dive analytical performance investigations**
  - Provide performance testing and analysis and post results for base kernel
  - Measure performance and scalability of Linux via selected benchmarks; publish key benchmark results
- **Identify bottlenecks so developers can improve performance and scalability**
- **Optimize the performance of Linux across the areas of hardware, firmware and software**
- **Provide tools and utilities to the Linux community**

General Tools Requirements

- Uniform set of performance tools across platforms and Linux distributions :
  - Ia32
  - Ia64
  - ppc64 (32 and 64-bit apps)
  - S390
  - S390x (32 and 64 bit apps)
  - x86-64 (32 and 64-bit apps)
- Integrated with distribution
- Preferably open source
- Preferably no reboot required
- Work correctly/uniformly in guest partitions

Linux Profiling Tools

- The most time-consuming and frequently used sections of a program should be optimized first; profiling tools can be used to discover these areas
- Code profiling tools collect information about the code executing on the system
- The system is periodically interrupted so the information can be collected.
- The information is then used to analyze the performance of the code
- Code profilers
  - kernprof
  - gprof
  - oprofile

oprofile

- capable of profiling all parts of a running system, from the kernel to user-level code
- released under the GNU GPL
- consists of a kernel module and a daemon for collecting sample data, and several post-profiling tools
- leverages the hardware performance counters of the CPU to enable profiling of a wide variety of interesting statistics, which can also be used for basic time-spent profiling
- profiling can be started and stopped anytime
- several post-profiling tools; http://oprofile.sourceforge.net

gprof

- part of the GNU binutils distribution, is a well known profiler designed to monitor a program's execution
- to use gprof, a program needs to be compiled and linked with profiling enabled
- when the program executes, a profile data file is generated; using the relationship between the program symbol table and the call graph profile, gprof calculates the amount of time spent in each routine and constructs the call graph for all parents and descendents.

gprof

- Output for each function:
  - The *flat profile* shows time spent in each function, and the number of times that function was called
  - total execution times, the call counts, the time in msec or usec the call spent in the routine itself, as well as the routine and its descendents
  - The *annotated source* listing is a copy of the program's source code, labeled with the number of times each line of the program was executed

Kernprof

Developed and support by SGI

- **supports a number of profiling techniques**
- **its simplest mode creates a Program Counter (PC) value histogram for the kernel**
- **both standard timer-based sampling, and sampling based on the hardware performance counters, are supported**
- **the use of performance counters gives a significant advantage to kernprof, as relevant performance events such as cache misses can be analyzed.**
- **http://oss.sgi.com/projects/kernprof/**

Tracing Tools

- **Linux Trace Toolkit**
  - **Suite of tools designed to trace and extract program execution profile information**
    - processor utilization and allocation information for a certain period of time
  - **Consists of 4 parts**
    - Patched kernel to enable events to be logged
    - Linux kernel module that stores events into its buffer and then signals the trace daemon when reaching data limits
    - Trace daemon that writes the data collected by the kernel module
    - Data decoder (visualizer) for converting and displaying trace data
  - **LTT has support for Real Time Application Interface (RTAI), a real-time Linux extension.**
  - **LTT can also be used with Dynamic Probes (Dprobes) version 1.2 or later, to provide a universal (dynamic) tracing capability for Linux**

  - **http://www.opersys.com/LTT/index.html**

Tracing Tools

- **strace**
  - **Strace is a system call trace**
    - Debugging tool which prints out a trace of all system calls made by a process/program
    - Program to be traced need not be recompiled for this, so it can be used on binaries for which there is no source
  - **In the simplest case, strace runs the specified command until it exits**
  - **Intercepts and records the system calls which are called by a process and the signals which are received by a process**
  - **The name of each system call, its arguments and its return value are printed to standard error or to the file specified with the -o option**
  - **Each line in the trace contains the system call name, followed by its arguments in parentheses and its return value**

Resource Monitoring Tools

- Linux provides facilities to monitor the utilization of memory resources under /proc filesystem
  - /proc/meminfo and /proc/slabinfo; capture the state of the physical memory
- Vmstat – virtual memory statistics
- Top – process statistics
- Netstat – network statistics
- Systat – sar, iostat, mpstat

For more information:
http://perso.wanadoo.fr/sebastien.godard/

Resource Monitoring Tools – Other Tools

- **Lockmeter**
  - **instruments the spin locks in a multiprocessor Linux kernel**
  - **used to identify which portions of the kernel code are responsible for causing lock contention; Lockmeter allows the following statistics to be measured for each spin lock:**
    - The fraction of the time that the lock is busy
    - The fraction of accesses that resulted in a conflict
    - The average and maximum time that the lock is held
    - The average and maximum time spent spinning for the lock
- **Performance Inspector**
  - **http://www-124.ibm.com/developerworks/oss/pi/index.html**

Benchmarks used in Linux

- Targeted because their workloads represent a diverse set of applications
- Benchmarks
  - Java: SPECjbb, SPECjAppServer, SPECpower_ssj
  - HPC: SPECcpu, SPEComp, stream, Linpack
  - Networking: Netperf and netop
  - I/O: disk tests with SCSI and FAStT, SPECsfs
  - Web Server: SPECwebSSL, SPECweb
  - Database: TPC-C and TPC-H
  - Coming soon from SPEC: Service Oriented Architecture (SOA), Session Initiated Protocol (SIP), Virtualization

Tuning Tips: I/O and Network

- **Sequential Read Tuning**
  - Increase max_readahead size using hdparm command
  - Read ahead is a function of page cache size
- **I/O Scheduler Tuning**
  - Increase nr_requests to 1024 (improves on most I/O workloads)
- **NFS Tuning**
  - bump up NFS daemons in large NFS server
  - larger Maximum Transmission Unit (MTU); 9000 bytes on gigabit Ethernet
  - Use NFS over TCP and not UDP on Linux

Tuning Tips: Database

- Use Asynchronous I/O for database page cleaners
- Raw devices (raw I/O) provide performance superior to filesystems
- Using disk controllers that provide write caching can provide significant performance improvements, particularly for database logs in an OLTP environment.
- Be sure to consult Linux sysctl tuning as per database vendor recommendations
- The deadline I/O scheduler has proven to be best for both TPC-C and TPC-H workloads

Tuning Tips: Java

- Can use either 32-bit and 64-bit JVM
- The JVM can exploit large page support provided in the 2.6 kernel
  - Enable large page support using –Xlp for the Java heap
  - Can improve performance between 6-15%
- Increase the available virtual memory
  - Set /proc/<pid>/mapped_base to 0x10000000 (default is 0x40000000)
  - Adds approximately three more 256MB segments to the JVM – allows 3.2 GB heap
- Use 32-bit JVM for smaller systems (up to 1-way to 8-way)
  - 32-bit JVM can give 10% boost in workloads like SPECjbb
- Consider using 64-bit JVM for larger systems (over 8-way systems)
  - For 16-way and greater, the 32-bit JVM has scaling limits which will offset the 10% speed boost

Linux Application Performance Tuning

Three Levels of Performance Tuning

- 1: Hardware, Networking, Linux
- 2: Native Code, JVM
- 3: App Server, Resources, Application

- Levels 2 and 3 can be tuned independent of the operating system

Linux Application Performance Tuning

Top Down Approach

- Treat whole System as black box
- Collect performance data, analyze, identify suspected bottlenecks
- Focus on bottlenecks by going one step lower, using tools, microbenchmarks, etc.
- Repeat steps until bottleneck is found

- Make sure other layers have been exhausted before focusing on Linux Tuning

- ***Give Linux the benefit of the doubt by making it the last suspect***, except when it is rather obvious and undeniable that the problem is Linux related

oprofile

- capable of profiling all parts of a running system, from the kernel to user-level code
- released under the GNU GPL

- consists of a kernel module and a daemon for collecting sample data, and several post-profiling tools.
  - For 2.2 and 2.4 Linux kernels, the module must be compiled into the kernel source tree while beginning with 2.5.43, oprofile has been merged with the kernel and it is enabled through a configuration selection
- leverages the hardware performance counters of the CPU to enable profiling of a wide variety of interesting statistics, which can also be used for basic time-spent profiling
- profiling can be started and stopped anytime
- Profiles user-level code, the whole system
- several post-profiling tools; http://oprofile.sourceforge.net

Ifconfig

- ifconfig
  - The *ifconfig* command is used to bind the IP address, host name, net mask, broadcast address, and other network configuration parameters to a particular network interface.
  - The *ifconfig* command is run at boot time by the startup scripts called by the *init* process.
  - Unfortunately, every vendor has added its own options to the *ifconfig* command, with the list of options growing daily.
  - This fact makes it almost impossible to tabulate all options available for every operating system environment.

Host Configuration

- ifconfig
  - You can use the *ifconfig* command to examine and/or modify interface parameters while the system is up and running.
  - When issued with the *–a* flag, *ifconfig* prints the configuration information for all interfaces.
  - Note that IPv4 and IPv6 information is listed separately on dual-stack hosts.
  - Because the implementation details may differ on various versions of Linux, it is best to consult the *ifconfig* manual page on your system for more information on this command.

Configuration NIC IP address

- NIC: Network Interface Card
- Use “ifconfig” command to determine IP address, interface devices, and change NIC configuration
- Any device use symbol to determine
  - eth0: Ethernet device number 0
  - eth1: ethernet device number 1
  - lo : local loopback device
  - Wlan0 : Wireless lan 0

Determining NIC IP Address

```
[root@tmp]# ifconfig -a

eth0 Link encap:Ethernet HWaddr 00:08:C7:10:74:A8
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:11 Base address:0x1820

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:787 errors:0 dropped:0 overruns:0 frame:0
TX packets:787 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:82644 (80.7 Kb) TX bytes:82644 (80.7 Kb)
```

Changing IP Address

- We could give this eth0 interface an IP address using the ifconfig command.

```
[root@tmp]# ifconfig eth0 10.0.0.1 netmask 255.255.255.0 up
```

- The "up" at the end of the command activates the interface.

- To make this permanent each time boot up by add this command in /etc/rc.local file which is run at the end of every reboot.

Host Configuration

- The ifup Script
  - The */etc/sysconfig/network-scripts/ifup* script file is invoked at boot time by *init*.
  - The script reads the interface files and parses the entries.
  - The information from the entries is used to configure each network interface with the proper values.
- The ifdown Script
  - The */etc/sysconfig/network-scripts/ifdown* script file is invoked at shutdown time by *init*.
  - The script reads the interface files and parses the entries.
  - The information from the entries is used to shut down each network interface.

  - ***Different Systems may have different file names or different path***

Host Configuration

- **The network-functions Script**
  - **The */etc/sysconfig/network-scripts/network-functions* script file contains a "library" of functions used by the *ifup* and *ifdown* scripts.**
  - **The functions include code for setting the net mask, host name, broadcast addresses, and gateways.**
  - **The functions perform operations required to configure an interface up or down.**

route

- **route**
  - **The *route* command is used to add and manage static routing tables on the host.**
    - Static routes are, as the name implies, routes that should not change very often.
    - The routers then decide how to deliver the data to the final destination.
    - The *route* command allows the administrator to manually add a static route to this “default gateway” router.
    - The generic call to the route command is as follows.

route [-f] keyword [type] destination gateway [metric]

How to Change Default Gateway

```
[root@tmp]# route add default gw 192.168.1.1 wlan0
```

- **In this case, make sure that the router/firewall with IP address 192.168.1.1 is connected to the same network as interface wlan0**
- **Once done, you'll need to update "/etc/sysconfig/network" file to reflect the change. This file is used to configure your default gateway each time Linux boots.**

```
NETWORKING=yes
HOSTNAME=bigboy
GATEWAY=192.168.1.1
```

Packet Loss Measurement

```
netman: ping -s mit.edu
PING mit.edu: 56 data bytes
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=0. time=42. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=1. time=41. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=2. time=41. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=3. time=40. ms
64 bytes from MIT.MIT.EDU (18.72.0.100): icmp_seq=4. time=40. ms

----mit.edu PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 40/40/42
```

ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet.
-i TTL	Time To Live.
-v TOS	Type Of Service.
-r count	Record route for count hops.
-s count	Timestamp for count hops.
-j host-list	Loose source route along host-list.
-k host-list	Strict source route along host-list.
-w timeout	Timeout in milliseconds to wait for each reply.

Tripwire

- A file and directory integrity checker.
- Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes.
- Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.
- Linux users may also want to consider AIDE, which has been designed to be a free Tripwire replacement. Or you may wish to investigate Radmind, RKHunter, or chkrootkit. Windows users may like RootkitRevealer from Sysinternals.

Tripwire

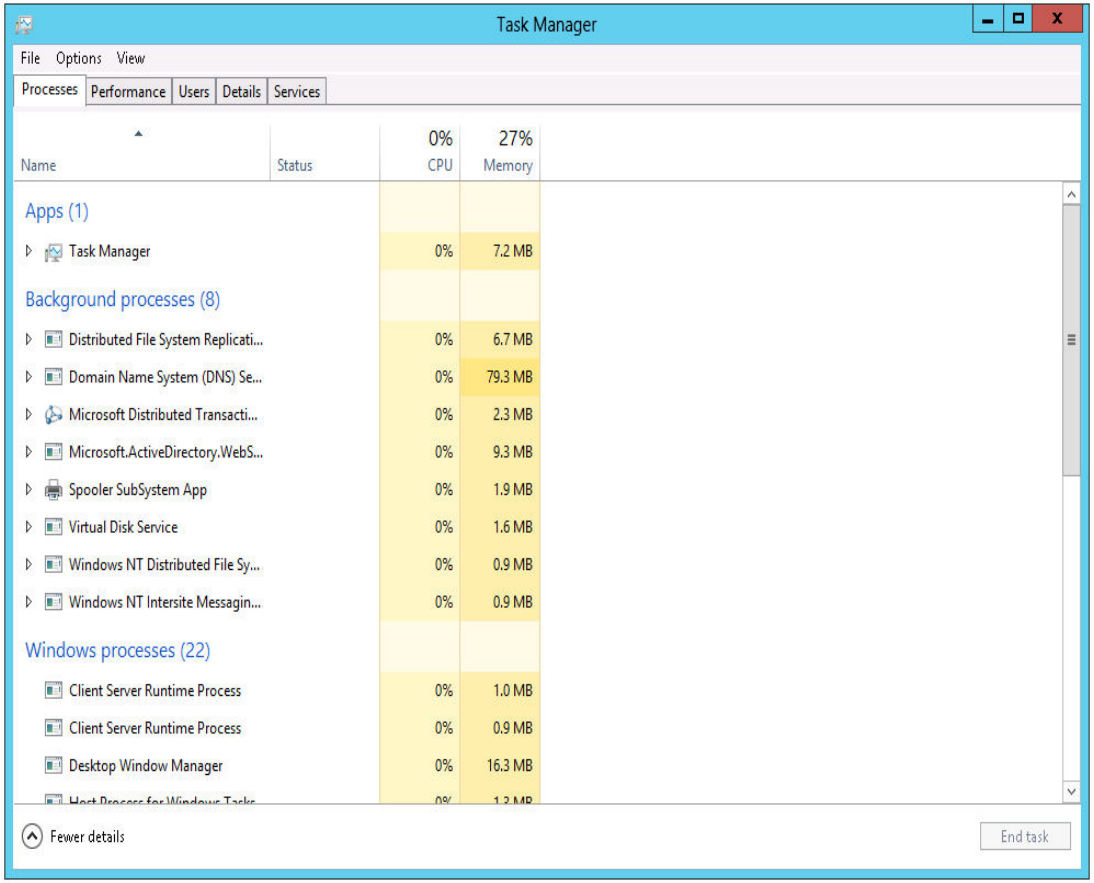
- Tripwire is a tool that checks to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc.
- Where is it ?
  - Commercial version : http://www.tripwire.com/
  - For Linux user : http://www.tripwire.org/
  - For Unix user : ftp://coast.cs.purdue.edu/pub/COAST/Tripwire/tripwire-1.2.tar.Z

Windows Monitoring Tools

- Overview of Task Manager
- Overview of Performance Monitor
- Overview of Resource Monitor
- Overview of Reliability Monitor
- Overview of Event Viewer
- Monitoring a Server With Server Manager

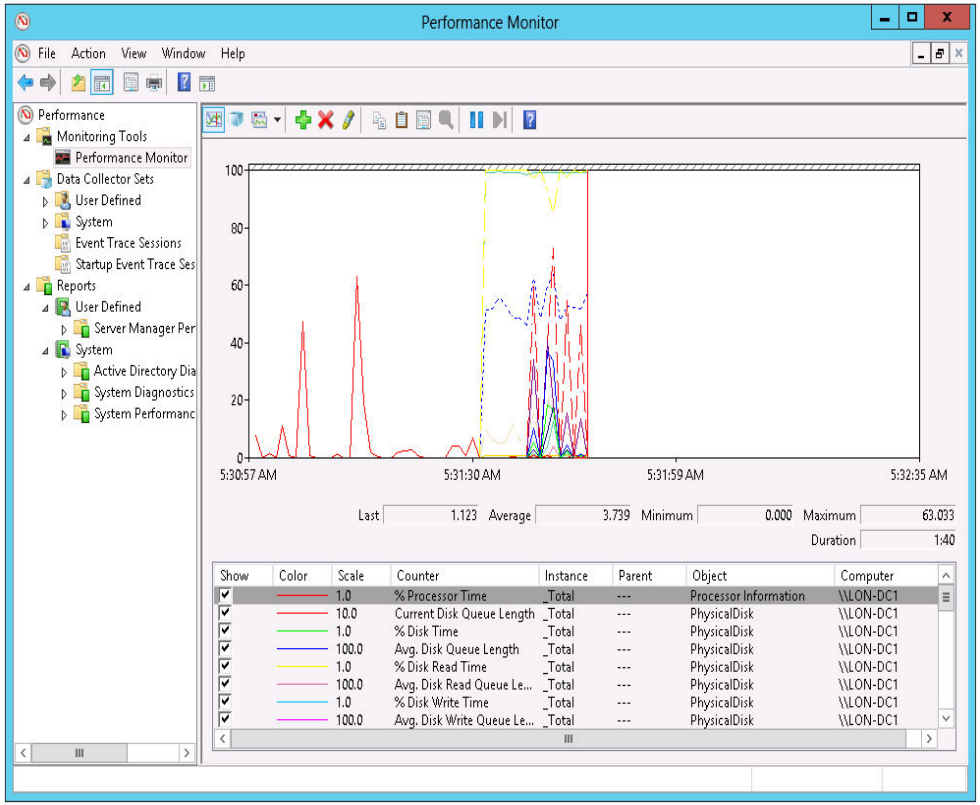
Overview of WindowsTask Manager

- **Windows Task Manager helps you to identify and resolve performance-related issues**



Overview of Windows Performance Monitor

- Performance Monitor enables you to view current performance statistics, or to view historical data
- Gathered through the use of Data Collector Sets



Overview of Windows Performance Monitor

Primary Processor Counters:

- Processor > % Processor Time
- Processor > Interrupts/sec
- System > Processor Queue Length

Primary Disk Counters:

- Physical Disk > % Disk Time
- Physical Disk > Avg. Disk Queue Length

Primary Network Counters:

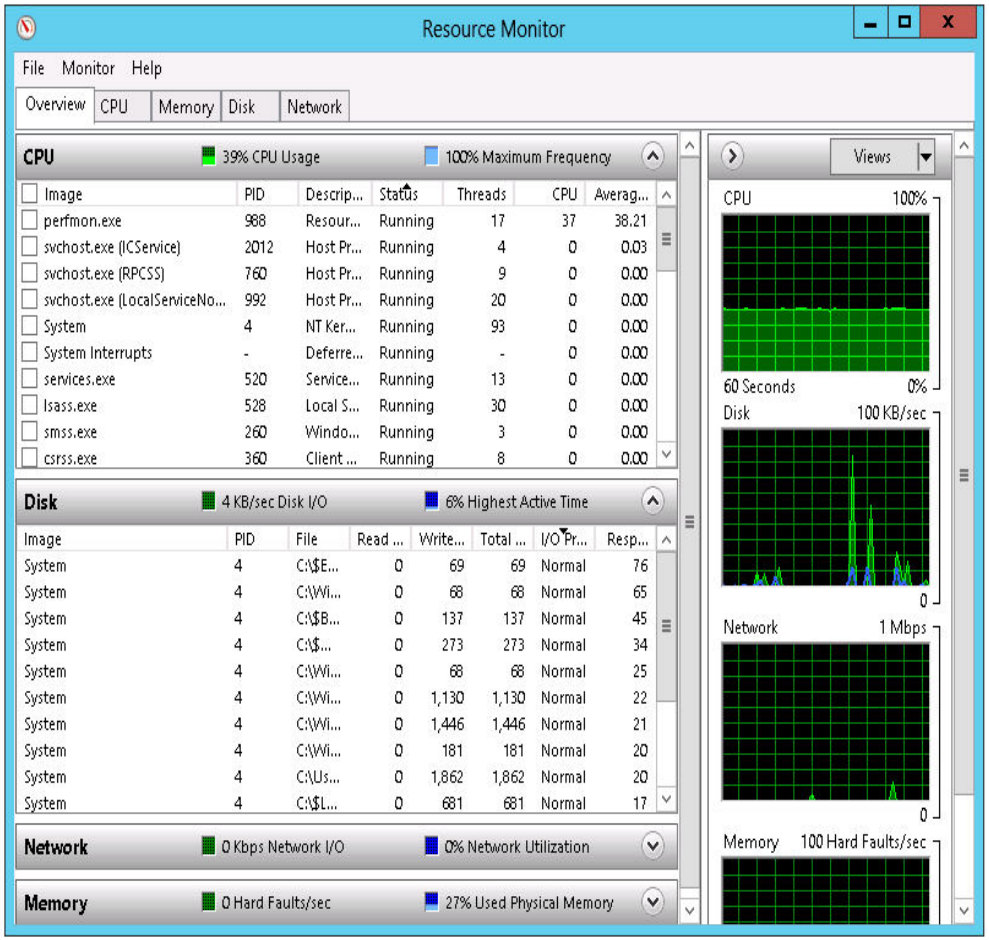
- Network Interface > Current Bandwidth
- Network Interface > Output Queue Length
- Network Interface > Bytes Total/sec

Primary Memory Counter:

- The Memory > Pages/sec counter

Overview of Windows Resource Monitor

- **Resource Monitor provides an in-depth look at the real-time performance of your server**

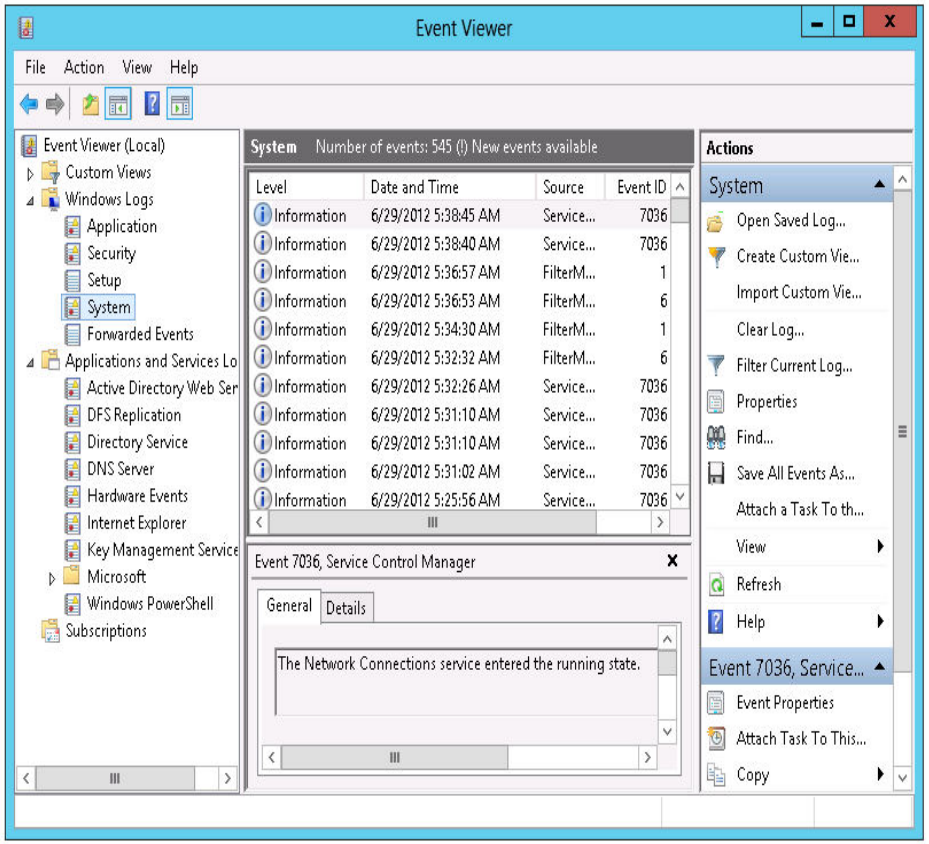


Overview of Windows Reliability Monitor

- Monitors hardware and software issues
- Provides Stability Index number (from 1 to 10)
  - 1 represents lowest stability
  - 10 represents highest stability
- Reliability monitor window components include:
  - Historical reports on stability index
  - Reliability details
  - Action to be performed – saving historical data, starting Problem Reports console, checking online for a solution to specific problem

Overview of Windows Event Viewer

- **Event Viewer provides categorized lists of essential Windows log events, and log groupings for individual installed applications and specific Windows component categories**



Overview of Windows Event Viewer

- Event Viewer provides the ability to
  - View multiple logs
  - Create customized views
  - Configure tasks scheduled to run in response to events
  - Create and manage event subscriptions
- Event Viewer has many built-in logs such as
  - Application log
  - Security log
  - Setup log
  - System log
  - Forwarded events

Monitoring a Server With WindowsServer Manager

Server Manager console:

- Installed by default on Windows Server 2016/2019.
- Supports monitoring of Windows Server operating systems
- Provides a centralized monitoring dashboard
- Analyzes or troubleshoots different types of issues
- Identifies critical events
- Monitors the status of Best Practices Analyzer tool

Using Windows Performance Monitor

- Performance Baselines, Trends, and Capacity Planning
- What Are Data Collector Sets?
- Demonstration: Capturing Counter Data with a Data Collector Set
- What Are Alerts?
- Demonstration: Configuring an Alert
- Demonstration: Viewing Reports in Performance Monitor
- Monitoring Network Infrastructure Services
- Considerations for Monitoring Virtual Machines

Performance Baselines, Trends, and Capacity Planning

- By calculating performance baselines for your server environment, you can more accurately interpret real-time monitoring information
- By establishing a baseline, you can:
  - Interpret performance trends
  - Perform capacity planning
  - Identify bottlenecks
- Analyze performance trends to predict when existing capacity is likely to be exhausted
- Plan the capacity for the key hardware components – processor, disk, memory and network

What Are Data Collector Sets?

- Data collector sets enable you to gather performance-related and other system statistics for analysis
- Data collector sets can contain the following types of data collectors:
  - Performance counters
  - Event trace data
  - System configuration information

What Are Alerts?

- An alert notifies the administrator of events that have occurred or performance thresholds that have been reached
- When creating an alert, configure the following settings:
  - Alert when
  - Alert Action
  - Alert Task

Considerations for Monitoring Virtual Machines

Considerations for monitoring virtual machines:

- Virtual machines must be assigned sufficient resources for their workload
- If multiple virtual machines run on a host, ensure the host has enough resources
- Resources are shared, so performance of one virtual machine can affect the performance of others
- You must remember to monitor the resource utilization on the host as well as the guests

Monitoring Event Logs

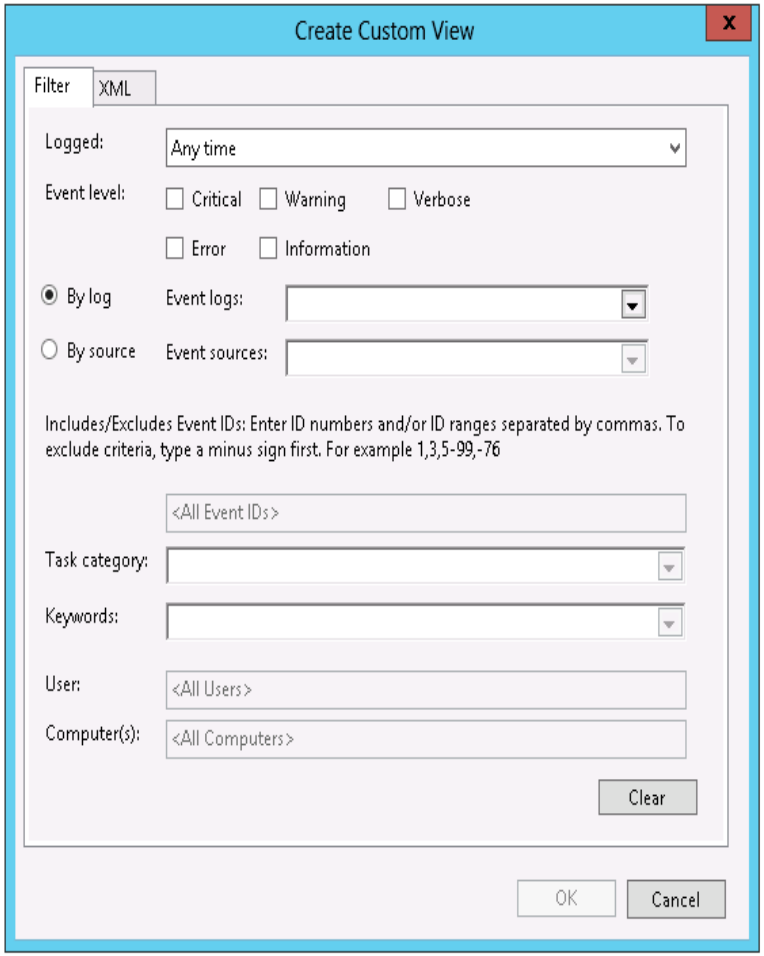
- Using Server Manager to View Event Logs
- What Is a Custom View?
- Demonstration: Creating a Custom View
- What Are Event Subscriptions?

Using Server Manager to View Event Logs

- Server Manager provides a centralized location for event logs from remote servers
- Event logging
  - Enabled by default
  - Categorized by technology – AD DS, DNS, Remote Access
- Customized views
  - Create queries for specific types of events that need to be displayed
  - Configure event data that needs to be displayed

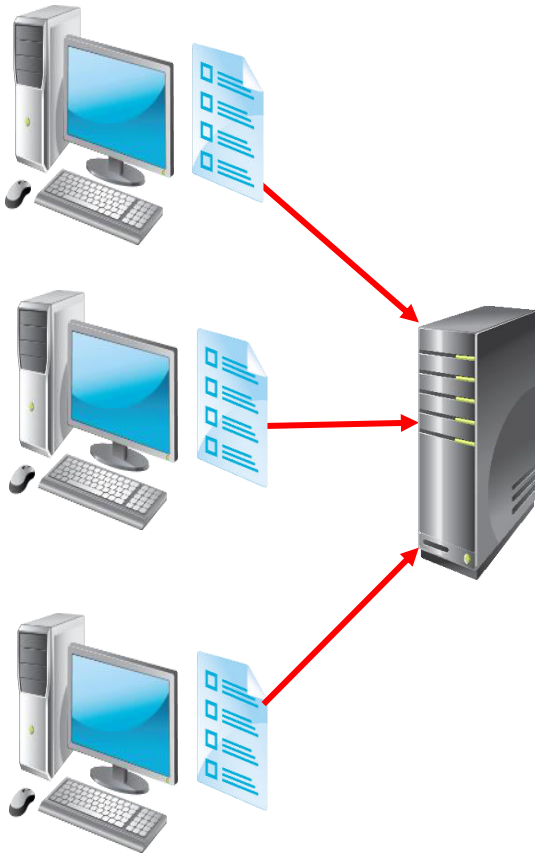
What Is a Custom View?

- Custom views allow you to query and sort just the events that you want to analyze



What Are Event Subscriptions?

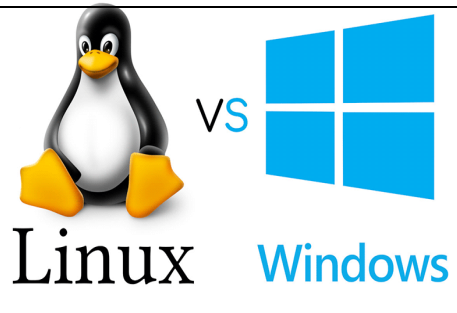
- **Event subscriptions allow you to collect event logs from multiple servers, and then store them locally**

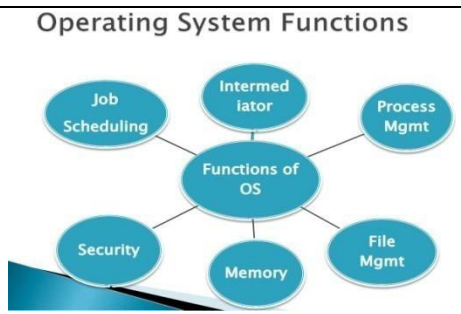


CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week15Day1 : Configuring Windows Updates, Backup and Recovery, Deploy Backup Strategy, Restoring System State Data





Objectives

- Configuring Windows Updates
- Perform backup and restore operations
- Developing backup strategies
- Different Types of Backups

Configuring Windows Updates

- When Microsoft releases a new operating system, users may encounter issues and security deficiencies.
- Both of these can cause your network to have many problems. So to help fix these issues, Microsoft will release updates and security fixes on a weekly and/or monthly basis.
- It is important for an IT department to keep their network systems up-to-date with these fixes.
- Well there are two main ways to do this.
  - You can let your users all connect to Microsoft's website one at a time and grab updates
  - you can setup a Windows Server Update Services (WSUS) server to get these updates. Then that WSUS server can release the updates to your users.

Configuring Windows Updates Services

- Tools that you need to understand when dealing with updates.
  - **Windows Update** This utility attaches to the Microsoft website through a user-initiated process, and it allows Windows users to update their operating systems by downloading updated files (critical and noncritical software updates).
  - **Windows Server Update Services (WSUS)** This utility is used to deploy a limited version of Windows Update to a corporate server, which in turn provides the Windows updates to client computers within the corporate network.
  - This allows clients that are limited to what they can access through a firewall to be able to keep their Windows operating systems up-to-date.

Windows Update

- *Windows Update* is available for most Windows operating systems and it allows the system to receive updates from Microsoft.
  - Examples of updates include security fixes, critical updates, updated help files, and updated drivers.

Windows Update control panel

- If you want to use Windows Update, an administrator would click Start ➢ Settings ➢ Update & security. You would then see the following options:
  - **When the Last Updates Were Done** When you enter into the Windows Update settings, the first thing you will see is when the last updates were done (if any).
  - **Check For Updates Button** This allows you to manually check to see if any updates are available for the operating system.
  - **Update History** This allows you to track all of the updates that you have applied to your server.

Windows Update control panel

- If you want to use Windows Update, an administrator would click Start ➢ Settings ➢ Update & security. You would then see the following options:
  - **Change Active Hours** This setting allows you to set your active hours on the system. So for example, you worked on this system or the server was most active from 8:00am to 6:00pm, you can set those hours so that the Windows Update knows when to download and install updates.
  - **Restart Options** This setting allows you to customize when the system will restart after the machine receives its updates.
  - **Advanced Options** This customizes what updates you receive when you use Windows Update.

Advantages of Using WSUS

- Using WSUS has many advantages:
  - It allows an internal server within a private intranet to act as a virtual Windows Update server.
  - Administrators have selective control over what updates are posted and deployed from the public Windows Update site. No updates are deployed to client computers unless an administrator first approves them.
  - Administrators can control the synchronization of updates from the public Windows Update site to the WSUS server either manually or automatically.
  - Administrators can configure Automatic Updates on client computers to access the local WSUS server as opposed to the public Windows Update site.
  - WSUS checks each update to verify that Microsoft has digitally signed it. Any updates that are not digitally signed are discarded.

Advantages of Using WSUS

- Using WSUS has many advantages:
  - Administrators can selectively specify whether clients can access updated files from the intranet or from Microsoft's public Windows Update site, which is used to support remote clients.
  - Administrators can deploy updates to clients in multiple languages.
  - Administrators can configure client-side targeting to help client machines get updates. Client-side targeting allows your organization's computers to automatically add themselves to the computer groups that were created in the WSUS console.
  - Administrators can configure a WSUS statistics server to log update access, which allows them to track which clients have installed updates. The WSUS server and the WSUS statistics server can coexist on the same computer.
  - Administrators can manage WSUS servers remotely using HTTP or HTTPS if their web browser

Configuring a WSUS

- **Update Source And Proxy Server**
  - This option allows you to configure whether this WSUS server synchronizes either from Microsoft Update or from another WSUS server on your network.
- **Products And Classifications**
  - This option allows you to select the products for which you want to get updates and the type of updates that you want to receive.
- **Update Files And Languages**
  - This option allows you to choose whether to download update files and where to store these update files. This option also allows you to choose which update languages you want downloaded.
- **Synchronization Schedule**
  - This option allows you to configure how and when you synchronize your updates. Administrators can choose to synchronize manually or to set up a schedule for daily automatic synchronization.

Configuring a WSUS

- **Automatic Approvals**
  - This option allows you to specify how to approve installation of updates automatically for selected groups and how to approve revisions to existing updates.
- **Computers**
  - This option allows you to set computers to groups or use Group Policy or Registry settings on the computer to receive updates.
- **Server Cleanup Wizard**
  - This option allows you to clean out old computers, updates, and update files from your server.
- **Reporting Rollup**
  - This option allows you to choose whether to have replica downstream servers roll up computer and update status to this WSUS server.

Understanding Backups

- One of the most important jobs of an IT administrator is to protect the company's data.
  - Doesn't matter if it's setting up security and permissions or installing a new firewall, we are trying to protect our data. It truly is our number one job.
  - Knowing that protecting our data is our primary task means that our IT departments have to ensure that we can recover that data in the event of a major catastrophe (like a fire in the server room) or hardware failure.
  - If you have deployed Active Directory in your network environment, your users now depend on it to function properly in order to do their jobs. From network authentications to file access to print and web services, Active Directory has become a mission-critical component of your business. Therefore, the importance of backing up the Active Directory data store should be evident.

Understanding Backups

- Here are several specific reasons to back up data:
  - **Protect Against Hardware Failures**
  - Computer hardware devices have finite lifetimes, and all hardware eventually fails. *Mean Time Between Failures (MTBF)* is the average time a device will function before it actually fails. There is also a rating derived from benchmark testing of hard disk devices that tells you when you may be at risk for an unavoidable disaster. Some types of failures, such as corrupted hard disk drives, can result in significant data loss.
  - **Protect Against Accidental Deletion or Modification of Data**
  - Although the threat of hardware failures is very real, in most environments, mistakes in modifying or deleting data are much more common. For example, suppose a system administrator accidentally deletes all of the objects within a specific OU. Clearly, it's very important to be able to retrieve this information from a backup.

Understanding Backups

- Here are several specific reasons to back up data:
  - **Protect Against a Major Catastrophe**
  - As IT administrators, it's tough to think that a major catastrophe would ever happen to our company, but we have to make sure we protect our company in the event of that very possibility. Fires, earthquakes, flooding, and tornados are just some of the events that we have to consider. Because of these types of events, we have to make sure that not only do we back up our data, we also get that data offsite. When I talk about offsite, I don't mean another building on the campus. It needs to be in another city or in a very safe location (like a safety deposit box).
  - **Keeping Historical Information**
  - Users and system administrators sometimes modify files and then later find out that they require access to an older version of the file. Or a file is accidentally deleted, and a user does not discover that fact until much later. By keeping multiple backups over time, you can recover information from prior backups when necessary.

Understanding Backups

- Here are several specific reasons to back up data:
  - **Protect Against Malicious Deletion or Modification of Data**
  - Even in the most secure environments, it is conceivable that unauthorized users (or authorized ones with malicious intent!) could delete or modify information. In such cases, the loss of data might require valid backups from which to restore critical information.
  - Windows Server includes a Backup utility (called wbadmin) that is designed to back up operating system files and the Active Directory data store. It allows for basic backup functionality, such as scheduling backup jobs and selecting which files to back up

Developing a Backup Strategy

- **For each OS and application you introduce, you should answer the following questions:**
  - **What are the possible failure scenarios?**
  - **Plan for the Worst scenario:**
    - HW, Power, Software failures. Deletion of objects and Files.
  - **What is critical data?**
  - **How often should backup be performed?**
  - **How can we ensure that the backups are useable?**
  - **Assume failure and consequences**
- **A good documented plan ensures that you quickly recover your data if it's lost.**

Developing a Backup Strategy

- **Guidelines for an effective strategy**
  - **Develop backup and restore strategies**
    - Appropriate **resources** and **personnel**
    - Test your Backup's
  - **Assign backup responsibilities**
  - **Back up entire volume (Disk Failures)**
  - **Keep three copies of the backup media**
    - Keep one copy "offsite"
  - **Perform trial restoration periodically**
    - Verify that your files were properly backed up.
  - **Secure storage of device and Backup media**
    - Prevent an un-authorised restore to your server.

Considerations for Choosing Backup Software

Selection criteria	What to consider?
Software	Availability of software support for Exchange's API-based online backups
Backup architecture	Support for any operating systems
Scheduling	Ability to schedule backups to achieve the most flexibility
Exchange API support	Support for API or the Volume Shadow Copy service Exchange writer
Tape management	Ability to automatically identify the tapes
Vendor support	Level of technical support and updates
Disaster recovery support	Ability for complete disaster recovery
Hardware support	Support for the technologies used in your company

Deploying a Backup Strategy

- **Who can perform backups and restores?**
  - **Backups: Domain Administrators, and Backup Operators**
  - **Restores: Domain Administrators**
  - **Custom Group:**
    - "**Back up files and directories**" right assigned to a security principal

Tombstone Period

- The object remains in the deleted objects container for the tombstone period
  - Default 60 days (SP1 = 180 days)
- The Garbage Collector removes any deleted objects for which the tombstone period has expired
  - Runs every 12 hours (default setting)

Workstation Backups

- Common local productivity files include:
  - Documents
  - Spreadsheets
  - Local databases
  - Presentations
- Workstation backups protect productivity
- Backup to server is most common

System Backups

- Store mission critical shared data
- Data loss affects many users
- Backups should be frequent, tested, and archived
- Appropriate for the servers' function

Backing Up System State Data

- When you are planning to back up and restore Active Directory, be aware that the most important component is known as the *System State data*.
- System State data includes the components upon which the Windows Server operating system relies for normal operations. The Windows Server Backup utility offers you the ability to back up the System State data to another type of media (such as a hard disk or network share).

Backing Up System State Data

- **Specifically, it will back up the following components for a Windows Server domain controller:**
- **Active Directory**
  - The *Active Directory data store* is at the heart of Active Directory. It contains all of the information necessary to create and manage network resources, such as users and computers. In most environments that use Active Directory, users and system administrators rely on the proper functioning of these services in order to do their jobs.
- **Boot Files**
  - *Boot files* are the files required for booting the Windows Server operating system and can be used in the case of boot file corruption.

Backing Up System State Data

- **Specifically, it will back up the following components for a Windows Server domain controller:**
- **COM+ Class Registration Database**
  - The *COM+ Class Registration database* is a listing of all of the COM+ Class registrations stored on the computer.
  - Applications that run on a Windows Server computer might require the registration of various share code components.
  - As part of the System State backup process, Windows Server stores all of the information related to Component Object Model+ (COM+) components so that it can be quickly and easily restored.

Backing Up System State Data

- **Specifically, it will back up the following components for a Windows Server domain controller:**
- **Registry**
  - The Windows Server *Registry* is a central repository of information related to the operating system configuration (such as desktop and network settings), user settings, and application settings. Therefore, the Registry is absolutely vital to the proper functioning of Windows Server
- *Sysvol* **Directory**
  - The *Sysvol directory* includes data and files that are shared between the domain controllers within an Active Directory domain. Many operating system services rely on this information in order to function properly.

Backing Up Active Directory

- One of the most essential duties of an administrator is ensuring that data and operating system information is backed up in case of a failure.
- Procedures that include the frequency of backups in addition to the type of information that needs to be backed up should be planned and implemented in every organization.

Backing Up Active Directory

- Backing up critical volumes involves backing up the following data:
  - The ***system volume***, which hosts the boot files, which consist of ***bootmgr.exe*** (the Windows boot loader) and the ***Boot Configuration Data (BCD)*** store, which describes boot applications and boot application settings and replaces the boot.ini file in previous versions of Windows.
  - The ***boot volume***, which hosts the Windows operating system and the Registry.
  - The volume that hosts the SYSVOL share.
  - The volume that hosts the Active Directory database (Ntds.dit).
  - The volume that hosts the Active Directory database log files.

Active Directory Backup

- System State Backup
  - System Startup Files – System files to boot
  - System registry
  - Class registration database of COM+
  - Sysvol
  - Active Directory database files
  - Active Directory-integrated DNS
  - Certificate Services database (if installed)
  - Cluster Service (if installed)

Active Directory Database

- Database Files includes:
  - Ntds.dit. The AD database
  - Edb.chk. The checkpoint file. recovery
  - Edbxxx.log. The transaction logs; circular logging only
  - Edb.log   The current log file (10 MB)
  - Res1.log & Res2.log. Reserved logs. shutdown
- Located in %systemroot%\ntds by default

Common Server Core Configuration Tasks (cont.)

- Dcpromo switches:
  - /replicaOrNewDomain
  - /replicaDomainDNSName
  - /ConfirmGC
  - /InstallDNS
  - /UserName
  - /Password
  - /RebootOnSuccess
  - /SafeModeAdminPassword

Diagnosing and Troubleshooting Active Directory

- To assist you with obtaining more detailed information in the event logs, you can set the event logs to record diagnostic information specific to processes related to Active Directory.
  - To enable, modify the following registry key:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

Active Directory Diagnostic Tools

Tool	Description
Dcdiag	This command-line tool can analyze the state of the domain controllers in the forest or enterprise and report any problems to assist in troubleshooting.
Repadmin	This command-line tool can check replication consistency between replication partners, monitor replication status, display replication metadata, and force replication events and knowledge consistency checker (KCC) recalculation.
Netdom	This command-line tool can manage and verify trusts, join computers to domains, and verify replication ability and permissions between partners.

Active Directory Diagnostic Tools

ADSIEdit	This graphical tool is an MMC snap-in that can be used to verify the current functional level and perform low-level Active Directory editing. Use this tool to add, delete, and edit Active Directory objects.
LDP	This graphical support tool provides a much more detailed method of adding, removing, searching, and modifying the Active Directory database.
Nltest	This command-line tool is typically used to verify trusts and check replication.
Dsacls	This command-line tool can be used to display or modify permissions of an Active Directory object. In effect, it is equivalent to an object's Security tab.

Backup Types

- Backup types include:
  - Normal Full backup
  - Incremental backup
  - Differential backup
  - Daily backup
  - Copy backup

Normal Backup

- Default type of backup performed by Backup utility
- Backs up all selected files and folders and clears the archive attribute on each
- This type of backup can be inefficient because it does not take into account whether files have changed
- Normal backups (also referred to as *system* or *full backups*) back up all of the selected files and then mark them as backed up. This option is usually used when a full system backup is made. Windows Server supports this backup.

Incremental Backup

- Backs up only files that have changed since last normal or incremental backup
- Clears the archive attributes of the files
- Reduces the size of backup jobs
- Restore process is more complicated
  - Normal backup and incremental backups must be restored in order

Incremental Backup

- *Incremental backups* copy any selected files that are marked as ready for backup (typically because they have not been backed up or they have been changed since the last backup) and then mark the files as backed up. When the next incremental backup is run, only the files that are not marked as having been backed up are stored. Incremental backups are used in conjunction with normal (full) backups.
- The most common backup process is to make a full backup and then make subsequent incremental backups. The benefit to this method is that only files that have changed since the last full or incremental backup will be stored. This can reduce backup times and disk or tape storage space requirements.
  - When recovering information from this type of backup method, a system administrator must first restore the full backup and then restore each of the incremental backups.

Incremental Backup (continued)

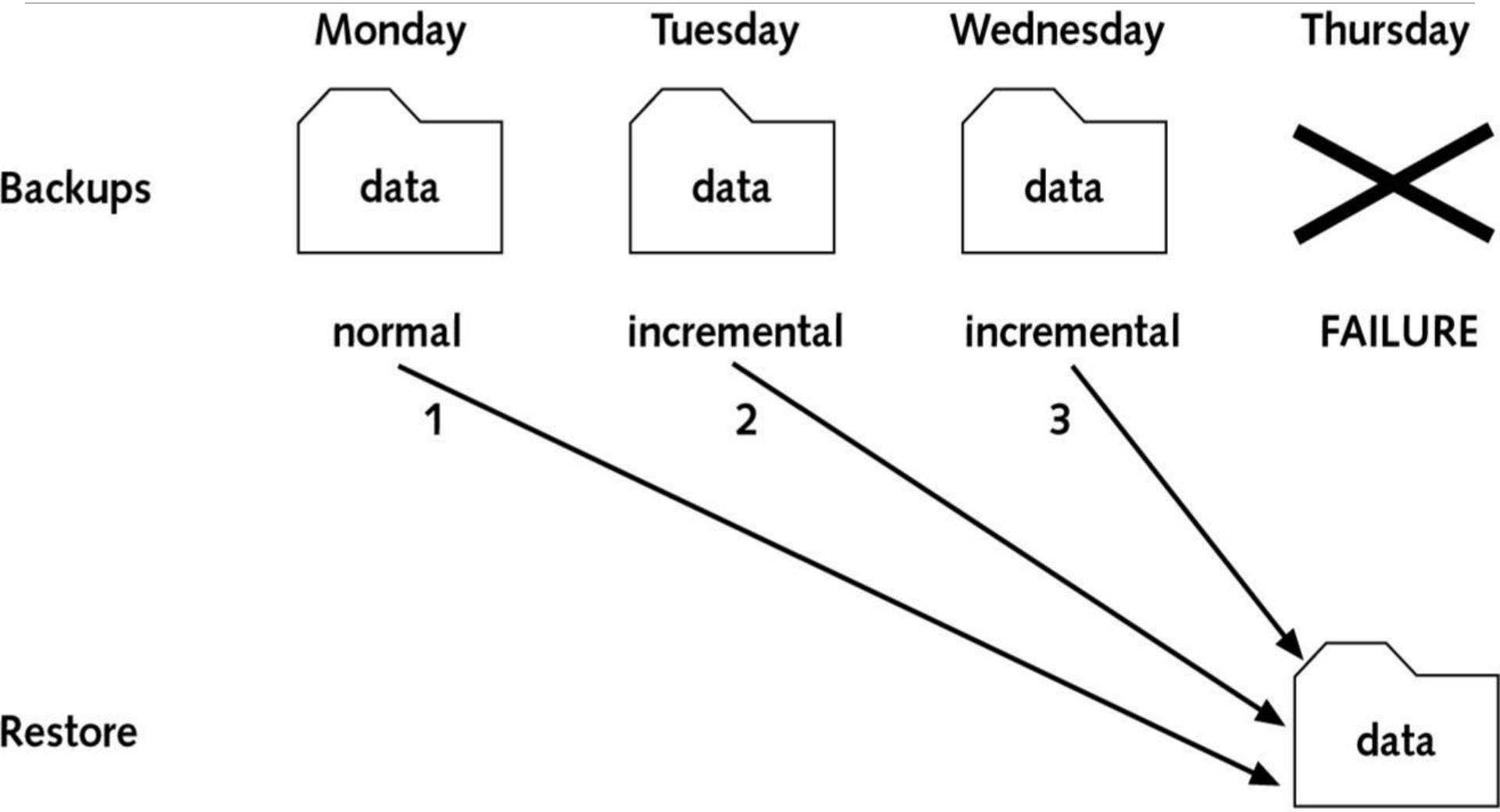


Figure 12-4 Incremental backup and restore operations

Differential Backup

- Backs up only files that have changed since last normal or incremental backup
- Does not clear the archive attributes of those files
  - A second differential backup will back up the same files since the first backup is not recorded by the archive attributes
- Reduces the size of backup jobs compared to normal backups but not incremental backups
- Restore process requires only the normal backup and the latest differential backup

Differential Backup

- *Differential backups* are similar in purpose to incremental backups with one important exception:
- Differential backups copy all of the files that are marked for backup but do not mark the files as backed up.
- When restoring files in a situation that uses normal and differential backups, you need only restore the normal backup and the latest differential backup.

Differential Backup (continued)

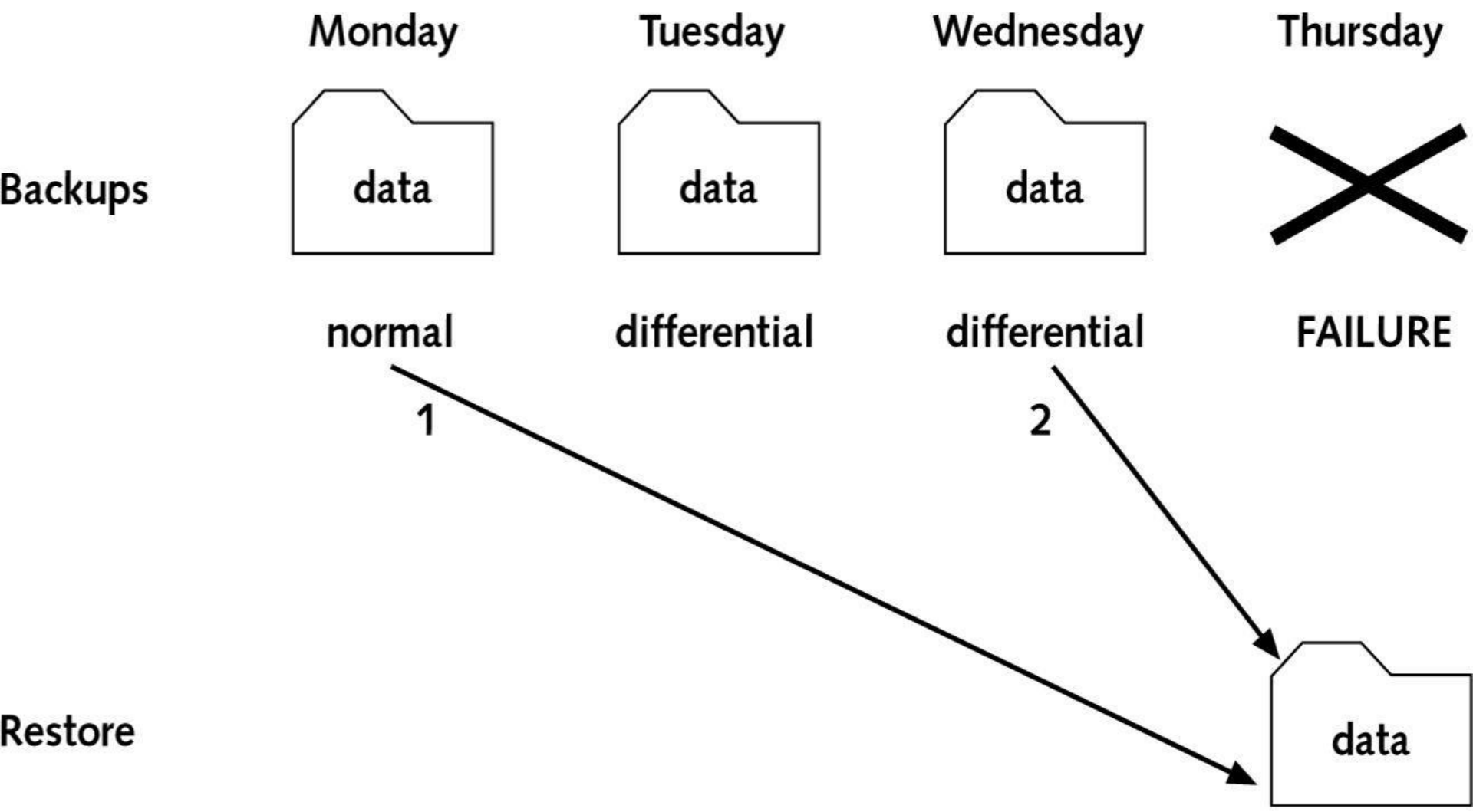


Figure 12-5 Differential backup and restore operations

Daily Backup

- Daily Backup
  - Backs up selected files or folders that were created or changed on the day of the backup
  - The archive attribute is not changed
  - *Daily backups* back up all of the files that have changed during a single day.
  - This operation uses the file time/date stamps to determine which files should be backed up and does not mark the files as having been backed up.

Copy Backup

- **Copy Backup**
  - **Exactly the same as a normal backup but doesn't change the archive attribute**
  - **Intended as a backup that will not interrupt other backup procedures (perhaps an archival copy)**
  - ***Copy backups* back up all of the selected files but do not mark them as backed up. This is useful when you want to make additional backups of files for moving files offsite or you want to make multiple copies of the same data for archival purposes.**

How to Choose a Backup Strategy

Backup strategy	Time to perform backup	Transaction logs	Number of sets required for restore	Time to perform recovery
Full backup	Longest amount of time	Are deleted	One backup set	Second fastest recovery
Full plus incremental	Least amount of time	Are deleted	One full backup set plus each incremental backup set	Longest recovery
Full plus differential	Progressively longer to complete	Are not deleted	One full backup set plus latest differential set	Second longest recovery
Copy backups	Same as full backup	Are not deleted	Same as full backup	Least amount of time to recover

Backup and Restore tools

- NTBACKUP
- NTDSUTIL
- LDP
- ADSIEDIT
- REPADMIN , REPLMON
- EVENT VIEWER

Ntbackup Limitations

- Support only ”Normal” backup of AD (Not incremental)
- You cannot back up AD by iteslf (Entire System state)
- ”System State” cannot be backed up from remote PC.
- ”System state” Restore can only be done when AD is offline
- Can ”only” be restored to the same DC
- The Backup tool does not encrypt the unencrypted backup contents during the backup process.

Factors Determining a Backup Strategy

- Important considerations include:
  - Target location
  - Files to include
  - Frequency
  - Organization type
  - Infrastructure components
  - Data reliance

Recovery Options

- Rebuild
  - Winnt32, Dcpromo, and Re-replicate
  - Known recovery time and results
- Restore
  - Windows Backup (Ntbackup.exe) to restore to a known good state
  - Re-replicate
- Repair
  - Esentutl repair of database is a last resort
  - Use integrity check to see if database is damaged

Recovery Console

- Allows administration of files on NTFS drives without completely loading OS
- Requires local Administrator password
- Can be run from the cd-rom or installed locally Winnt32 /cmdcons

Planning for Disaster Recovery

- Administrators need to be prepared for the possibility of server failure and/or file and folder loss at all times
- Windows Server features:
  - The Backup utility
  - Shadow Copies of Shared Volumes
  - Automated System Recovery
  - Advanced startup options
  - The Recovery Console

Windows Server Backup

Feature	When used (typical scenario)
Backup to DVD	*Adhoc , offsite backups.*
Backup to disk	*Periodic backup.*
Backup to n/w share	*Adhoc, redundancy*
File/Folder Recovery	*Accidental data loss, deletion*
Volume Recovery	*Disaster recovery of entire volume.*
System Recovery (from WinRE)	*Disaster recovery of OS volumes. But disk and disk layout intact.*
Full System Recovery (from WinRE)	*Disaster recovery to new disks. Format and repartition disks.*
System State Recovery	*AD Recovery* *Registry corruption*

Scheduling Backups

- In addition to specifying which files to back up, you can schedule backup jobs to occur at specific times.
- Planning *when* to perform backups is just as important as deciding *what* to back up.
- Performing backup operations can reduce overall system performance; therefore, you should plan to back up information during times of minimal activity on your servers.

Restoring System State Data

- In some cases, the Active Directory data store or other System State data may become corrupt or unavailable.
  - This could be due to many different reasons. A hard disk failure might, for example, result in the loss of data. Or the accidental deletion of an Organizational Unit (OU) and all of its objects might require a restore operation to be performed.
- The actual steps involved in restoring System State data are based on the details of what has caused the data loss and what effect this data loss has had on the system.
  - In the best-case scenario, the System State data is corrupt or inaccurate but the operating system can still boot.
  - If this is the case, all you must do is boot into a special *Directory Services Restore Mode (DSRM)* and then restore the System State data from a backup. This process will replace the current System State data with that from the backup. Therefore, any changes that have been made since the last backup will be completely lost and must be redone.

Restoring System State Data

- In a worst-case scenario, all of the information on a server has been lost or a hardware failure is preventing the machine from properly booting.
- If this is the case, here are several steps that you must take in order to recover System State data:
  - Fix any hardware problem that might prevent the computer from booting (for example, replace any failed hard disks).
  - Reinstall the Windows Server operating system. This should be performed like a regular installation on a new system.
  - Reinstall any device drivers that may be required by your backup device. If you backed up information to the file system, this will not apply.
  - Restore the System State data using the Windows Server Backup utility.

Backing Up and Restoring Group Policy Objects

- ***Group Policy Objects (GPOs)* are a major part of Active Directory.**
  - When you back up Active Directory, GPOs can also get backed up. You also have the ability to back up GPOs through the Group Policy Management Console (GPMC). This gives you the ability to back up and restore individual GPOs.
  - To back up all GPOs, open the GPMC and right-click the Group Policy Objects container. You will see the option Back Up All. After you choose this option, a wizard will start, asking you for the backup location. Choose a location and click Backup.
  - To back up an individual GPO, right-click the GPO (in the Group Policy Objects container) and choose Backup. Again, after you choose this option, a wizard will start, asking you for the backup location. Choose a location and click Backup.
  - To restore a GPO, it's the same process as above (backing up GPOs) except, instead of choosing Backup, you will either choose Manage Backups (to restore all GPOs) or Restore (for an individual GPO).

Restoring Active Directory

Active Directory has been designed with fault tolerance in mind.

- For example, it is highly recommended by Microsoft that each domain have at least two domain controllers. Each of these domain controllers contains a copy of the Active Directory data store. Should one of the domain controllers fail, the available one can take over the failed server's functionality. When the failed server is repaired, it can then be promoted to a domain controller in the existing environment. This process effectively restores the failed domain controller without incurring any downtime for end users because all of the Active Directory data is replicated to the repaired server in the next scheduled replication.
- In some cases, you might need to restore Active Directory from a backup. For example, suppose a system administrator accidentally deletes several hundred users from the domain and does not realize it until the change has been propagated to all of the other domain controllers. Manually re-creating the accounts is not an option because the objects' security identifiers will be different (all permissions must be reset). Clearly a method for restoring from backup is the best solution.

Understanding the *ntdsutil* Utility

- The primary method by which system administrators can do offline maintenance is through the ntdsutil command-line tool.
- You can launch this tool by simply entering **ntdsutil** at a command prompt. For the commands to work properly, you must start the command prompt with elevated privileges.
- The ntdsutil command is both interactive and context sensitive. That is, once you launch the utility, you'll see an ntdsutil command prompt.
- At this prompt, you can enter various commands that set your context within the application.
  - For example, if you enter **domain management**, you'll be able to enter domain-related commands. Several operations also require you to connect to a domain, a domain controller, or an Active Directory object before you perform a command.

Ntdsutil offline maintenance commands

Ntdsutil Command	Purpose
Help or ?	Displays information about the commands that are available within the Domain Management menu of the ntdsutil utility.
Activate instance %s	Sets NTDS or a specific AD LDS instance as the active instance.
Authoritative restore	Sets the domain controller for the authoritative restore of the Active Directory database.
Change service account	This allows an administrator to change the AD LDS service account to user name and password. You can use a “NULL” for a blank password, and you can use * to prompt the user to enter a password.
configurable settings	Allows an administrator to manage configurable settings.
DS behavior	Allows an administrator to view and modify AD DS or AD LDS behavior.
files	This command allows an administrator to manage the AD DS or AD LDS database files.
Group Membership Evaluation	Allows an administrator to evaluate the security IDs (SIDs) in a token for a given user or group.
LDAP policies	Administrators can manage the Lightweight Directory Access Protocol (LDAP) protocol policies.
metadata cleanup	Removes metadata from decommissioned domain controllers.
security account management	This command allows an administrator to manage SIDs.
Set DSRM Password	Resets the Directory Service Restore mode admini

Wbadmin Command-Line Utility

- The wbadmin command allows you to back up and restore your operating system, volumes, files, folders, and applications from a command prompt.
- You must be a member of the Administrators group to configure a backup schedule. You must be a member of the Backup Operators or the Administrators group (or you must have been delegated the appropriate permissions) to perform all other tasks using the wbadmin command.

Wbadmin Command-Line Utility

Command	Description
`Wbadmin enable backup`	Configures and enables a daily backup schedule.
`Wbadmin disable backup`	Disables your daily backups.
`Wbadmin start backup`	Runs a one-time backup.
`Wbadmin stop job`	Stops the currently running backup or recovery operation.
`Wbadmin get items`	Lists the items included in a specific backup.
`Wbadmin start recovery`	Runs a recovery of the volumes, applications, files, or folders specified.
`Wbadmin get status`	Shows the status of the currently running backup or recovery operation.
`Wbadmin start systemstaterecovery`	Runs a system state recovery.
`Wbadmin start systemstatebackup`	Runs a system state backup.
`Wbadmin start sysrecovery`	Runs a recovery of the full system state.

Backing Up Virtual Machines

- One of the main questions that you have to ask yourself when it comes to backing up a Hyper-V server is, Do I back up the Hyper-V server and the virtual machines as files, or do I back up each virtual machine as its own server?
- Virtual machines and the virtual hard drives that work with those virtual machines are just files that reside on a Microsoft Hyper-V server. But when they are running, they work as normal servers within the virtual environment.
- Some people like to back up the Hyper-V server and its files and some like to back up the virtual machines as servers. So what is best for your company? Well, it depends on what the virtual machines do and how much storage space you have.
- I have set up many companies and I have set up dozens of virtual machines and I personally like to back up the virtual machines as normal servers. I do have good reasons for this decision.

Backing Up Virtual Machines

- Let's say we set up a Windows Server 2016 server that works as a Hyper-V host. We then decide to load a virtual machine that will be a file server. We will do our normal daily backups once a day at night, and maybe we will even do a backup during the day at 1p.m.
- At 11:30 a.m., one of your users deletes a file that was created yesterday. Before deleting the file, the user had created 25 new documents. But that one file needs to be recovered. If we back up the virtual machines as files, depending on our backup software, we will need to restore the virtual machine file from last night. Okay, problem solved, but is it? Well actually it's not. Because when we restored last night's virtual machine files, we also lost all of our changes that have happened today.
- If we backed up the virtual machines as servers, we would then just need to restore the single file that was lost on that server. This would save us a lot of time and issues. But it can also cause some issues. By backing each virtual machine up as a server, your backups will require more space. So if your backup server, software, tapes, or cloud storage is large enough, then it may be best to back up each virtual machine as its own server.

Dynamic Disks

- Can set up a large number of volumes per disk
  - Volumes are similar to partitions but with additional capabilities
- Reasons to implement dynamic disks include
  - Can extend NTFS volumes
  - Can configure RAID volumes for fault tolerance and performance
  - Can reactivate missing or offline disks
  - Can change disk settings with restarting computer

Simple Volume and Spanned Volume

- A simple volume:
  - Dedicated, formatted portion of space on a dynamic disk
  - NTFS volumes can be extended (not system or boot)
- A spanned volume:
  - Space in 2 to 32 dynamic disks
  - Treated as a single volume
  - Allows you to maximize use of scattered space across several disks

Striped Volume

- Referred to as RAID level 0
- Implemented for performance enhancement, particularly for storage of large files
- Not fault tolerant
- Requires from 2 to 32 disks
- Data is written in 64 KB blocks across rows in the volume

Striped Volume (continued)

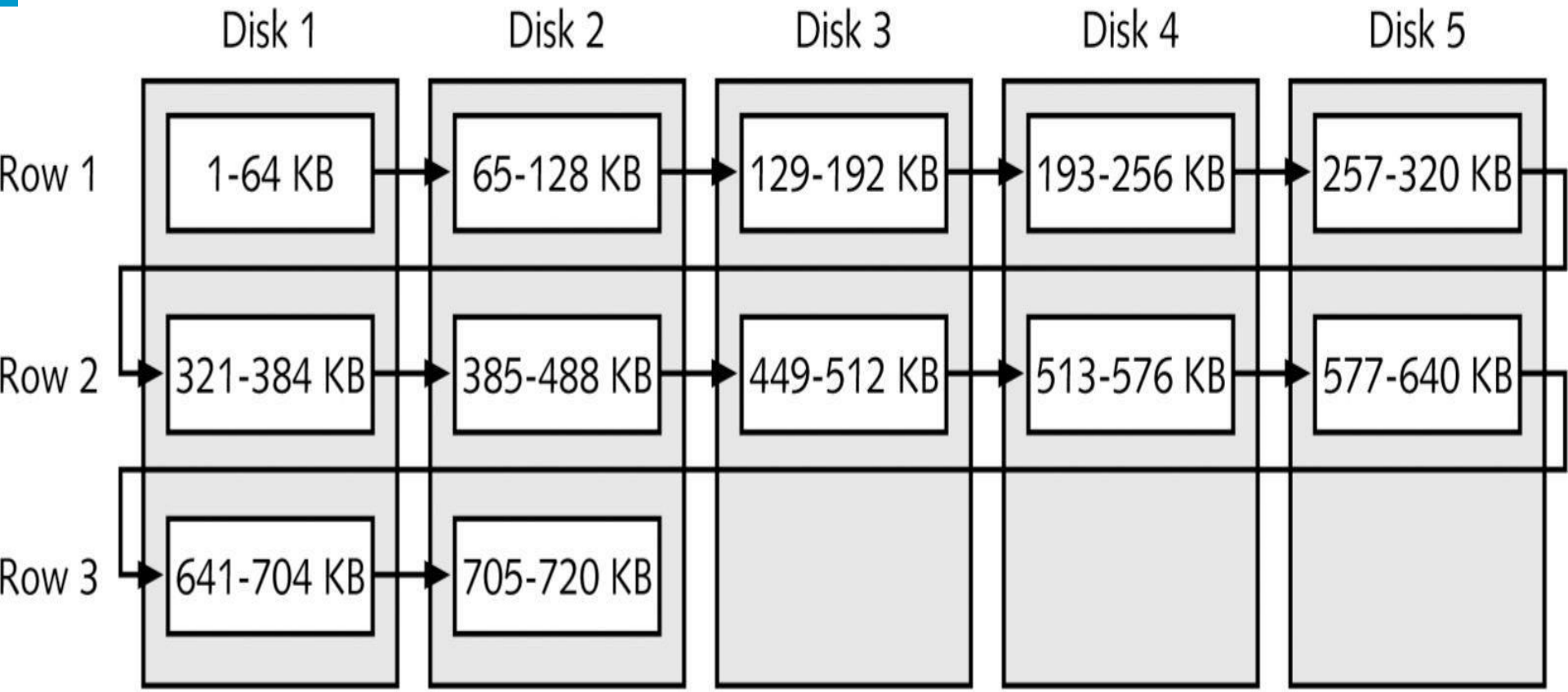
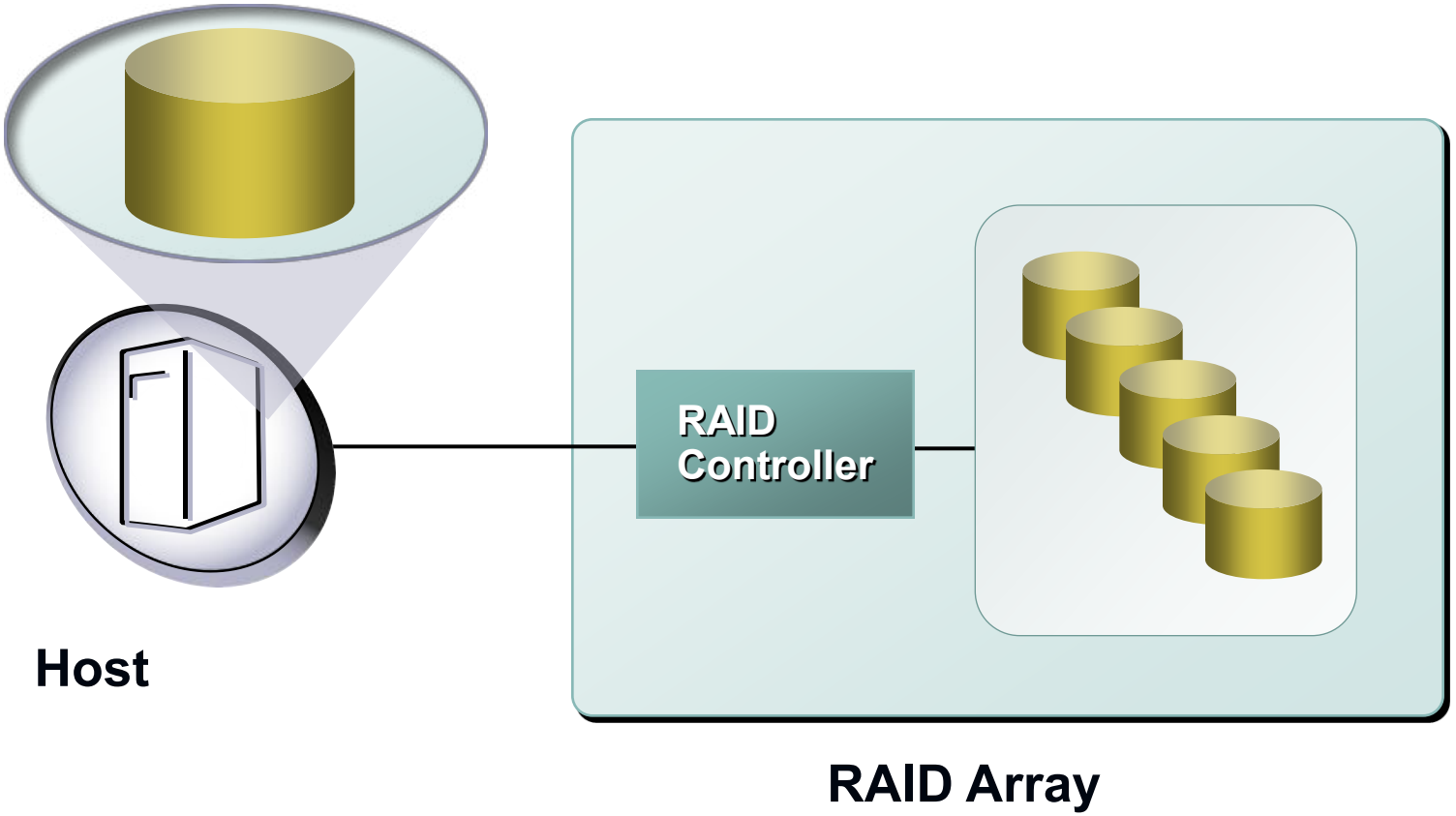
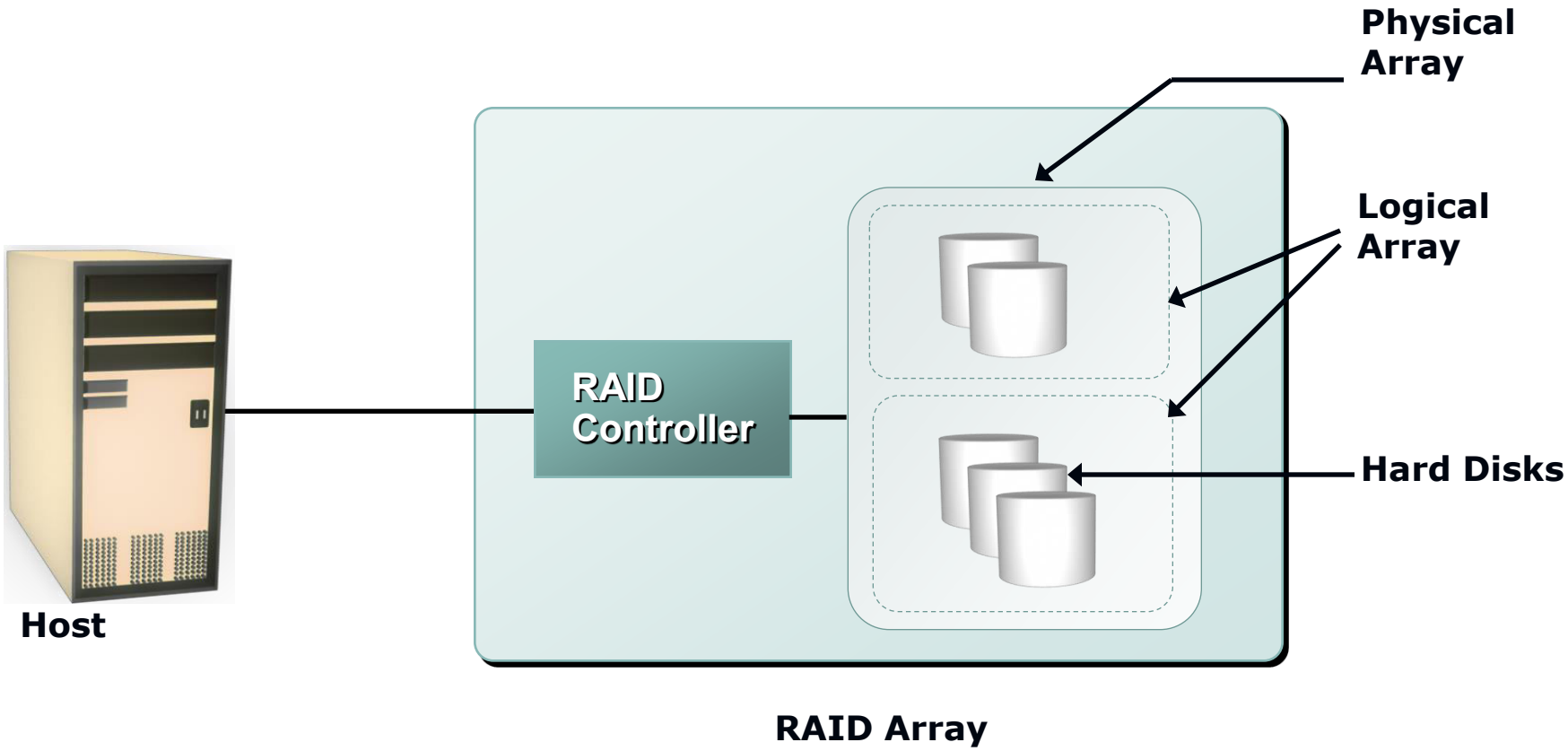


Figure 6-4 Disks in a striped volume

Backup with RAID - Redundant Array of Independent Disks



RAID Array Components



What is RAID?

Stands for Redundant Array of Independent Disks.

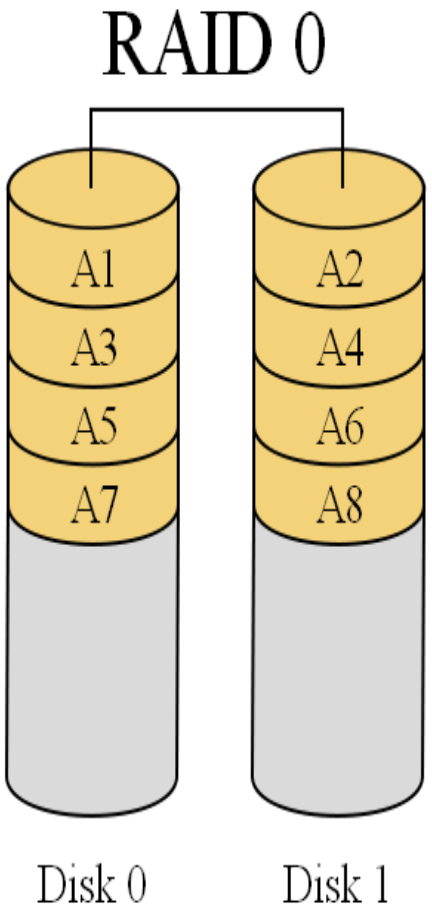
It's a technology that enables greater levels of performance, reliability and/or large volumes when dealing with data.

How?? By concurrent use of two or more 'hard disk drives'.

How Exactly?? Mirroring, Stripping (of data) and Error correction techniques combined with multiple disk arrays give you the reliability and performance.

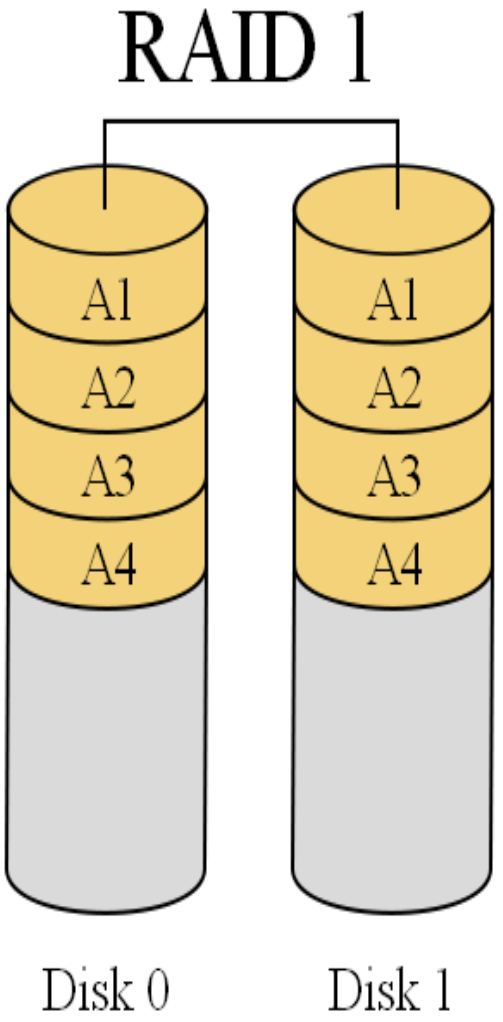
RAID 0

a. It splits data among two or more disks.
b. Provides good performance.
c. Lack of data redundancy means there is no fail over support with this configuration.
d. In the diagram to the right, the odd blocks are written to disk 0 and the even blocks to disk 1 such that A1, A2, A3, A4, … would be the order of blocks read if read sequentially from the beginning.
e. Used in read only NFS systems and gaming systems.



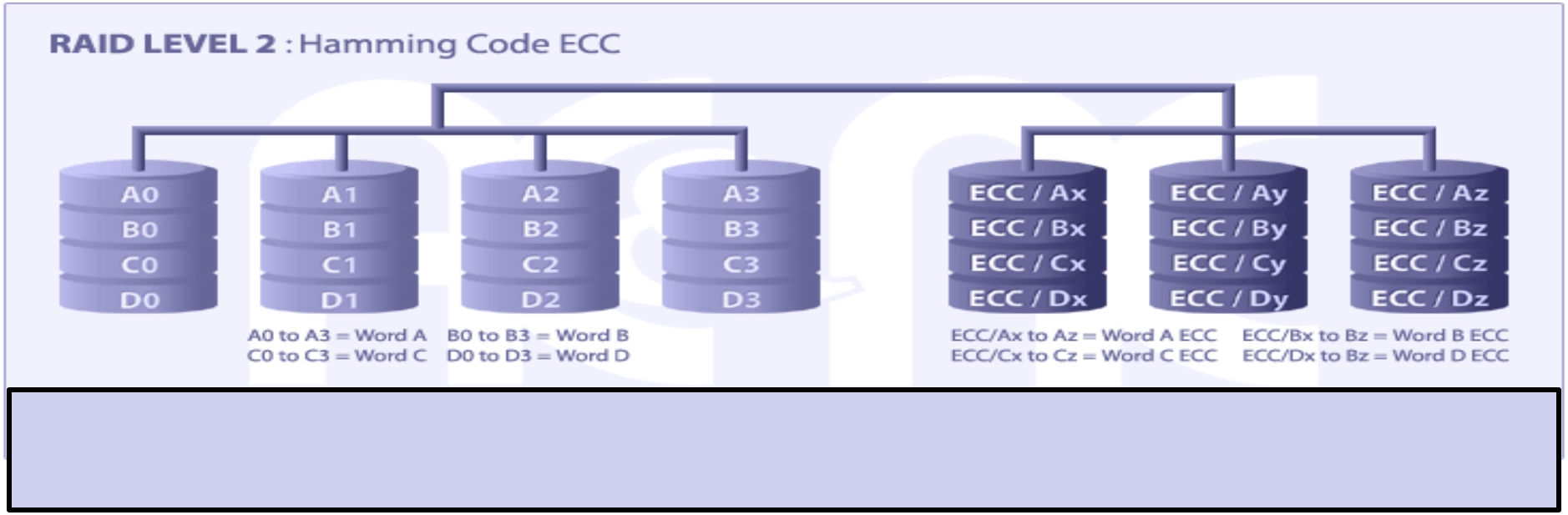
RAID 1

- RAID1 is ‘data mirroring’.
- Two copies of the data are held on two physical disks, and the data is always identical.
- Twice as many disks are required to store the same data when compared to RAID 0.
- Array continues to operate so long as at least one drive is functioning.



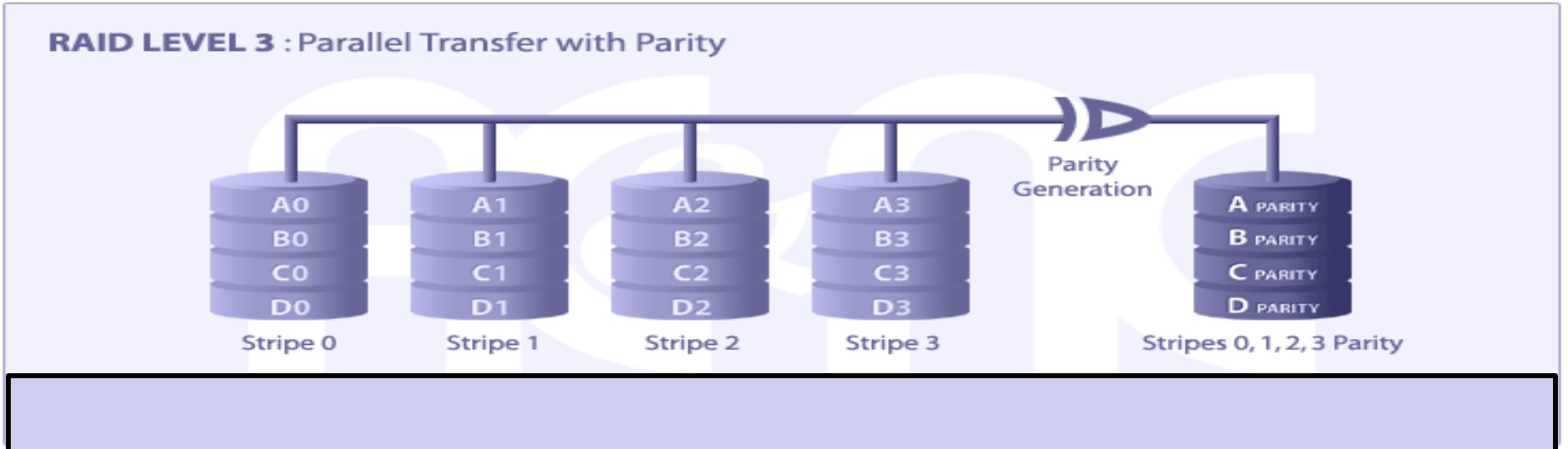
RAID 2

- RAID 2 implements bit stripping with ECC
- Pro: Good performance on both read and write. Good protection. Cheaper than RAID 1
- Con: Hamming code generation is slow, still expensive, no commercial use



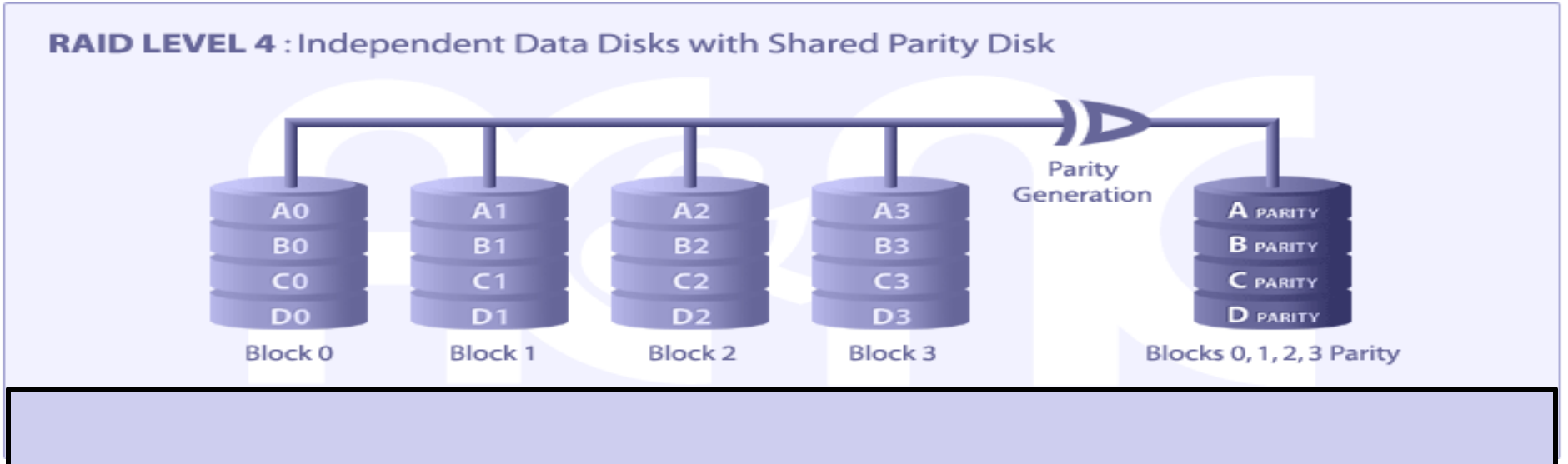
RAID 3

- RAID 3 implements bit stripping with parity disk
- Pro: Very good performance on read, write. Good protection. Efficient.
- Con: Complicated controller design.



RAID 4

- RAID 4 implements data stripping with parity drive.
- Pro: fast on read. Good protection
- Con: VERY slow write speed. Difficult data rebuild. Complex design. Not used in real life

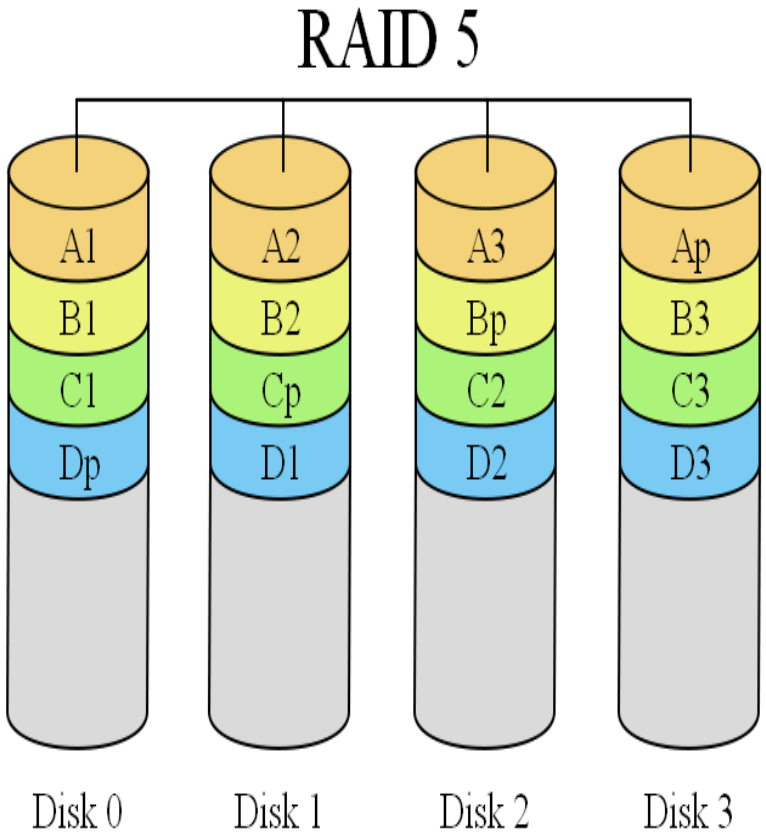


RAID 5

RAID 5 is an ideal combination of good performance, good fault tolerance and high capacity and storage efficiency.

An arrangement of parity and CRC to help rebuilding drive data in case of disk failures.

"Distributed Parity" is the key word here.



RAID-5 Volume (continued)

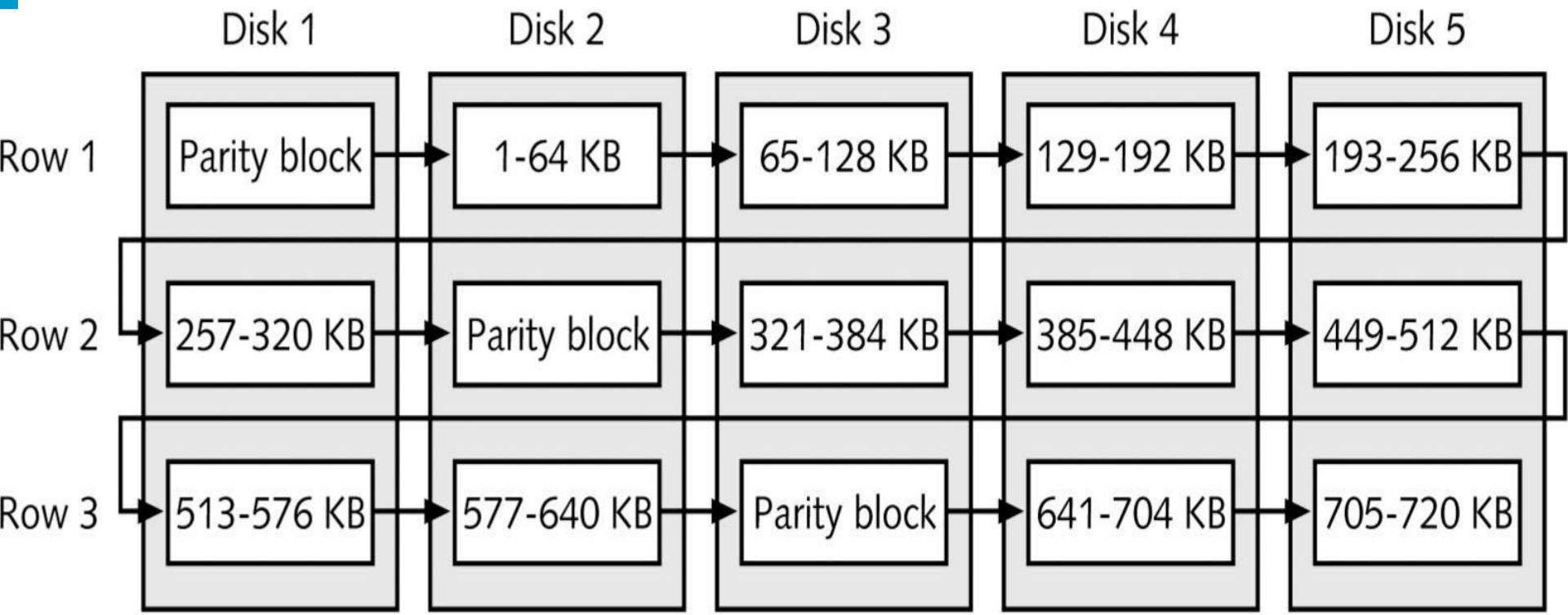


Figure 6-11 Disks in a RAID-5 volume

RAID 6 – Dual Parity RAID

- Two disk failures in a RAID set leads to data unavailability and data loss in single-parity schemes, such as RAID-3, 4, and 5
- Increasing number of drives in an array and increasing drive capacity leads to a higher probability of two disks failing in a RAID set
- RAID-6 protects against two disk failures by maintaining two parities
  - Horizontal parity which is the same as RAID-5 parity
  - Diagonal parity is calculated by taking diagonal sets of data blocks from the RAID set members
- Even-Odd, and Reed-Solomon are two commonly used algorithms for calculating parity in RAID-6

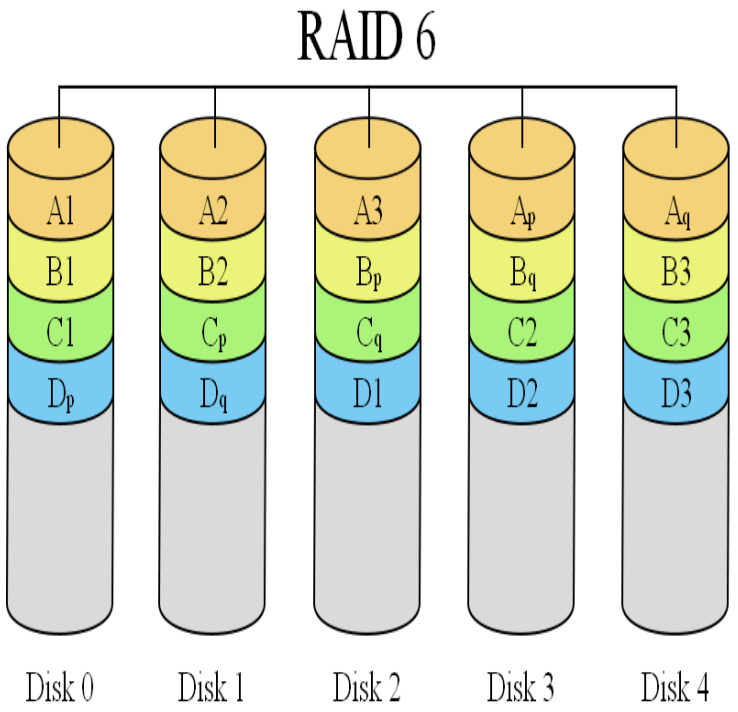
What's happening present day?

RAID 6:

It is seen as the best way to guarantee data integrity as it uses double parity.

Lesser MTBF compared to RAID5.

It has a drawback though of longer write time.

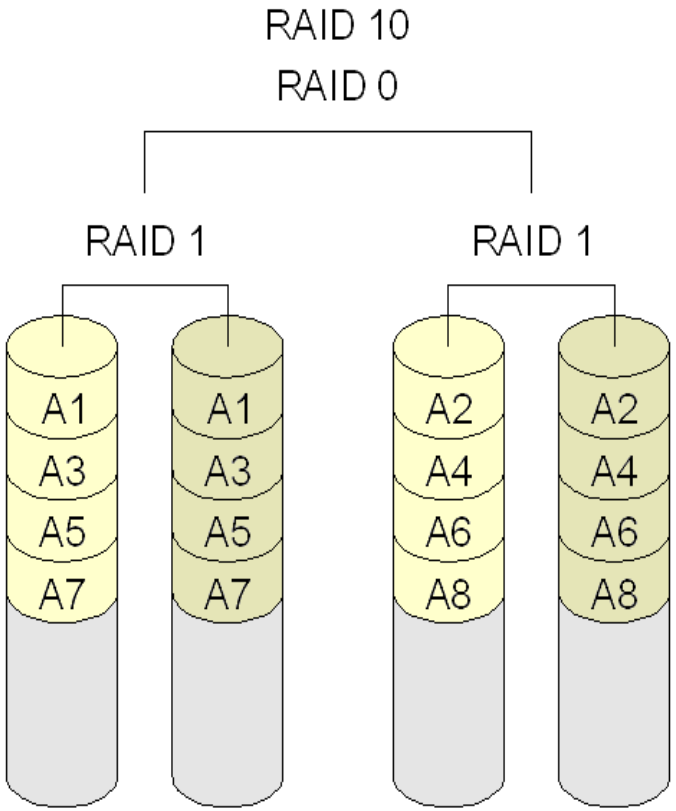


RAID Comparison

RAID	Min Disks	Storage Efficiency %	Cost	Read Performance	Write Performance
0	2	100	Low	Very good for both random and sequential read	Very good
1	2	50	High	Good Better than a single disk	Good Slower than a single disk, as every write must be committed to two disks
3	3	(n-1)*100/n where n= number of disks	Moderate	Good for random reads and very good for sequential reads	Poor to fair for small random writes Good for large, sequential writes
5	3	(n-1)*100/n where n= number of disks	Moderate	Very good for random reads Good for sequential reads	Fair for random write Slower due to parity overhead Fair to good for sequential writes
6	4	(n-2)*100/n where n= number of disks	Moderate but more than RAID 5	Very good for random reads Good for sequential reads	Good for small, random writes (has write penalty)
1+0 and 0+1	4	50	High	Very good	Good

RAID 10

a. Combines RAID 1 and RAID 0.
b. Which means having the pleasure of both - good performance and good failover handling.
c. Also called ‘Nested RAID’.



Implementations

Software based RAID:

- Software implementations are provided by many Operating Systems.
- A software layer sits above the disk device drivers and provides an abstraction layer between the logical drives(RAIDs) and physical drives.
- Server's processor is used to run the RAID software.
- Used for simpler configurations like RAID0 and RAID1.

Implementations

A PCI-bus-based, IDE/ATA hard disk RAID controller, supporting levels 0, 1, and 01.

Hardware based RAID:

- A hardware implementation of RAID requires at least a special-purpose RAID controller.
- On a desktop system this may be built into the motherboard.
- Processor is not used for RAID calculations as a separate controller present.

Road ahead…

- The expanded use of RAID-6 and other dual-parity schemes is a virtual certainty.
- RAID vendors to support "fast rebuild" features that can restore hundreds of gigabytes in just an hour or so!!
- Striping(of data) would extend across RAID groups -- not just across drives within a group.
- Improved disk diagnostic features should offer more reliable predictions of impending drive failures, allowing the rebuild process to begin before an actual fault occurs.