System Administration

Maintenance
Monitoring

http://courses.cs.ut.ee/2012/syshald/
Outline

- No test results yet! Next week?
- Maintenance
- Monitoring
Maintenance

- Objective of the maintenance process is to constantly keep the system in desired state
- Maintenance is often handled in a similar way as change
Maintenance (2)

• Maintenance can be divided by
  – Regularity
    • regular – based on schedule
    • irregular – based on need
  – Criticality
    • Routine – low failure probability
    • Sensitive – significant failure probability
    • Major – system is about to fail without maintenance
Maintenance

entropy

maintenance

desired/known state

unknown state
Maintenance (4)

• Planning the Maintenance
  - Pre-maintenance
    • maintenance procedures must be pre-planned
    • prerequisites and risks must be accounted for
    • there must be a back-out plan
    • in some sites, critical maintenance must be approved by a committee
Maintenance (5)

• Communicating the Maintenance
  - some maintenance procedures require downtime
  - customers are informed about sensitive and critical maintenance
    • even if it is regular
  - no need to inform about routine maintenance
  - two-step communication
    • long-term pre-announcement
    • repeat just before maintenance
Maintenance (6)

• Automating the Maintenance
  - many maintenance procedures can be (semi-)automated
  - more flexible schedule
    • procedures can be run at any moment
  - Faster procedures
    • time spent on developing the procedure is quickly compensated
  - reduces the risk of human errors
Maintenance (7)

• Documenting the Maintenance
• Post-maintenance
  - keep maintenance log/record
    • activities performed, results
    • time of maintenance
    • persons responsible
  - test and monitor for unwanted side effects
Maintenance (8)

- Software Maintenance
  - software updates
    - security updates
    - bug fixes
    - functionality updates
  - other procedures
    - configuring
    - log maintenance
    - package audit
Maintenance (9)

• Software Updates
  - (semi-)automatic updates for masses, manual updates for critical systems
  - mass updates must be tested, but fully automated (with no testing) updates are still way better than no updates
  - take extra caution when updating software on critical systems
Maintenance (10)

• Hardware Maintenance
  - details containing moving parts...
  - changing the BIOS, RAID-controller, etc. batteries
  - firmware updates
  - hardware errors are not visible to end-user in redundant systems
    • disaster waiting to happen
    • mitigate the risk by monitoring
    • routine maintenance only, if done right
Maintenance (11)

• Hardware Maintenance
  - specific skills required
    • maintenance manuals from manufacturer
    • specialist know-how
    • specialist experience
  - you are dealing with physical objects
    • you cannot just “take back” any step
    • risk of injury
Maintenance (12)

- User Account Maintenance
  - operations
    - creating
    - setting the permissions and roles
    - changing (re-setting) the password
    - blocking and removing
Maintenance

- User Account Maintenance
  - high security risks
  - have fixed set of authorized persons to perform user account maintenance
  - maintenance procedures and rules must be specific, strict and must not be changed by the persons performing them
  - User Account Maintenance vs. Identity Management
Maintenance (14)

- maintenance is a “soft” form of risk management
  - helps to avoid incidents and disasters
  - mitigates the effects
- costs less than disaster recovery
- stress levels are way lower compared to disaster recovery

rule of thumb: if it is not broken, don't fix it
Monitoring

- objective of the monitoring process is to constantly and systematically provide structured information about the state of the system
Monitoring (2)

- various monitoring objectives
  - (real-time) overview
  - incident discovery
    - including alarms & notifications
  - support for problem management
  - support for planning
    - including capacity management
Monitoring (3)

• Monitoring Coverage
  - always cover the base resources:
    • storage
    • CPU load (computing power)
    • network (bandwidth)
  - critical resources specific to the system
  - services offered by the system
Monitoring (4)

- Monitoring Coverage
  - physical environment
  - keep irrelevant information “on the background”
  - relevancy may change in time
Monitoring (5)

• Accuracy and interval
  – when interpreting the monitoring data, you must know the measuring accuracy
  – the second “dimension” of accuracy is the interval: the amount of time between two measurements
  – shorter interval gives better overview
    • but...
  – ...also increases the load. Find a compromise
  – Monitoring software defaults are often good
Monitoring (6)

- Measurement Scale
  - scale – the range for presenting the monitoring results
  - it is not always desirable to have scale covering all the possible measurement values
  - upper and lower limits are set, values outside the scale are “cut”
  - scale does not have to be linear
Monitoring (7)

- Monitoring Scale: a negative example

- Logarithmic scale would be better
Monitoring (8)

- Short-term (Operative) Monitoring
  - manually started by the system administrator
  - limited duration
  - more values measured (possibly with higher accuracy)
  - shorter interval
  - used during incident and problem resolution
  - higher load for the system
Monitoring (9)

• Short-term Monitoring cycle
  – 1. monitor, collect results
  – 2. analyze
  – 3. try to apply the analysis results in the problem solving process
  – 4. if no success, go to 1
Monitoring (10)

- Long-term Monitoring
  - fully automated
  - longer intervals
  - Lower load on the system
  - can be divided to:
    - historical monitoring
      - for planning, capacity management, reporting
    - real-time monitoring
      - for early discovery and alerting
Monitoring (11)

- Service Monitoring
  - service availability monitoring
    - is the query being answered
    - is the query being answered as expected
    - is the query being answered in expected time
  
- availability monitoring systems are often run separately from base resource monitoring systems
Monitoring (12)

• Monitoring Tools
  – tools shipped with operating systems
  – monitoring the base resources
    • \textit{top, iotop, Windows Task Manager, ...}
  – usually not enough
  – specialized monitoring software
    • Nagios, Munin, Ganglia, arpwatch
  – usually can be extended with plug-in's
Monitoring (13)

• Monitoring Output
  - we need a clear overview
    • and..
  - we need detailed information on resources
  - gather and keep detailed information, but also generate visual output:
    • graphs, diagrams, maps, ...
    • Use automated tools for this
Monitoring (14)

- Long-term monitoring results give us ability for:
  - historic:
    - planning the changes and capacities
    - reporting and documenting
    - risk management
    - maintenance
  - real-time
    - incident discovery and alerting
    - pro-active monitoring
Monitoring (15)

• Short-term monitoring results give us ability for:
  - solving incidents and problems
  - detail changes
  - testing and maintenance
Activity (15-20 min)

- From groups of 5
- Familiarize with “unit testing” concept from software development
- Discuss whether this concept is directly usable in system availability monitoring. Pros and cons.
- Present!
Activity (15-20 min)

• When developing software
  – Is it wise to write tests for functional units also?
    • Functional unit is set of classes/modules/etc. which perform an activity described in single functional requirement
  – Is it wise to combine functional unit tests to single application/framework?

• When administrating a system
  – Could we make use of functional units test framework on system availability monitoring?
Activity (15-20 min)

- Potential side-effects of demanding functional unit test code from software vendor/developer
  - Developer actually has to write tests!
  - Software will probably cost more
  - Software will probably have less bugs
  - Software will probably have better uptime due to thorough availability monitoring
Questions?