L12: Documentation, Maintenance, and Monitoring
1. Write down 2-3 problems in the documenting process (use only one sentence!)

2. Find people with similar thoughts, form teams (3-5 members)

3. Agree on the single most important problem, describe it in one sentence, then you are expected to explain the problem in 1 minute

4. Re-organize (if you find some other teams' key problem more important)

5. Offer solutions for this key problem – 1-2 minutes to explain the solution
Maintenance
(Hooldus)

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

regularity
- regular – based on a schedule
- irregular – based on a need

criticality
- routine
- sensitive
- major
Maintenance

desired/known state

entropy

maintenance

unknown state
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
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
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
Documenting the Maintenance

Post-maintenance

• keep maintenance log/record
  – activities performed, results
  – time of maintenance
  – persons responsible

• test and monitor for unwanted side effects
Software Maintenance

software updates...
- security updates
- bug fixes
- functionality updates

..and other procedures
- configuring
- log maintenance
- package audit
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
Hardware Maintenance

• details containing moving parts...
• changing the 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
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
User Account Maintenance

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

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

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

...but if something works, ... :)

Ulrich Norbisrath (http://ulno.net)
University of Tartu

Systems Administration
http://sysadmin.ulno.net
Monitoring (seire)

Objective of the monitoring process is to constantly and systematically provide structured information about the state of the system.
Monitoring

various monitoring objectives
• (real-time) overview
• incident discovery
  – including alarms & notifications
• support for problem management
• support for planning
  – including capacity management
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
physical environment
keep irrelevant information “on the background”
  - relevancy may change in time
Monitoring: accuracy and interval

• when interpreting the monitoring data, you must know the measuring accuracy (mõõtetäpsus)

• the second “dimension” of accuracy is the interval (intervall): the amount of time between two measurements

• shorter interval gives better overview but...

• ...also increases the load. Find a compromise
Monitoring Scale (*skaala*)

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 Scale: a negative example
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
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
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
    • dynamic intervals
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 Tools

tools shipped with operating systems
  • monitoring the base resources
  • `top`, `iostat`, `Windows Task Manager`, ...
  • usually not enough

specialized monitoring software
  • Nagios, Munin, Ganglia, arpwatch
  • usually can be extended with plug-in's
Monitoring Output

we need a clear overview!
and..

we need detailed information on resources!

so:

• gather and keep detailed information, but also generate visual output:
  - graphs, diagrams, maps, ...
Acting Based on Monitoring Results

long-term monitoring:
• historic
  - planning the changes and capacities
  - reporting and documenting
  - risk management
  - maintenance
• real-time
  - incident discovery and alerting
  - pro-active monitoring
Acting Based on Monitoring Results

short-term (operative) monitoring:

• solving incidents and problems
• detail changes
• testing and maintenance