Computer Security

Infrastructure Security

Prof. Jean-Noël Colin
jean-noel.colin@unamur.be
Office #306

University of Namur
Computer Science Faculty

www.unamur.be

UNIVERSITÉ
DE NAMUR

Agenda

- Introduction
- Component-level security
- System-level security
- Network security
- Hosting
- Site redundancy
- Monitoring
- Contracts

Infrastructure

- What is infrastructure?
    - computers, smartphones, tablets, microcontrollers
    - storage
    - backup devices
    - printers, scanners
    - network devices
    - IoT devices
    - ...
    - hosting facilities
- Murphy’s law
    - “if something can go wrong, it eventually will!” (most likely Fri. 4.00pm)

Introduction

Infrastructure getting more and more complex

- Moore’s law
  - Kryder dans Scientific American, 2005:

	Annual growth (%)
CPU complexity	50%
Memory capacity	60%
Memory access speed	10%
Disk capacity	60%
Disk access speed	25%
Network speed	40%

- capacity and performance of components grow at different pace, with impact on the global architectures (software and hardware)

Infrastructure security objectives

- Confidentiality? Integrity?
  - not the first concern (more important at higher levels)
- Availability
  - business continuity
    - IT supports business ⇒ IT continuity
  - avoid unexpected downtime
    - reliable hardware
    - maintainable hardware: hot swappable devices, non-disruptive firmware upgrade
    - error detection and correction (ex: Single Error Correcting, Double Error Detecting)
    - automatic reconfiguration

Availability

- Risk-based approach to define expected availability level
- Disruption can be caused by
  - planned maintenance (upgrade)
  - failure
- How to measure availability?
  - MTBF – Mean Time Between Failure
  - MTTR – Mean Time To Repair
  - availability = $\frac{\text{MTBF}}{\text{MTBF+MTTR}}$
  - easier to improve MTTR then MTBF
    - high quality hardware/reseller
    - support/maintenance contract
  - what does MTBF mean? 1.2Mhrs MTBF (136 years!)

Availability

- How to measure availability? (cont'd)
  - AFR – Annualized Failure Rate: proportion of devices of the same type that are expected to fail yearly, on a global scale
  - $\lambda_{annualized} = \lambda.8760$
    - $\lambda = \frac{1}{MTBF}$ (the failure rate)
    - 8760 = number of hours in one year
  - ex. Seagate Barracuda ES.2 Serial ATA:
    - MTBF: 1.2 Million hours
    - AFR: $\lambda_{annualized} = \frac{1}{1.200.000}.8760 = 0{,}73\%$

Threats

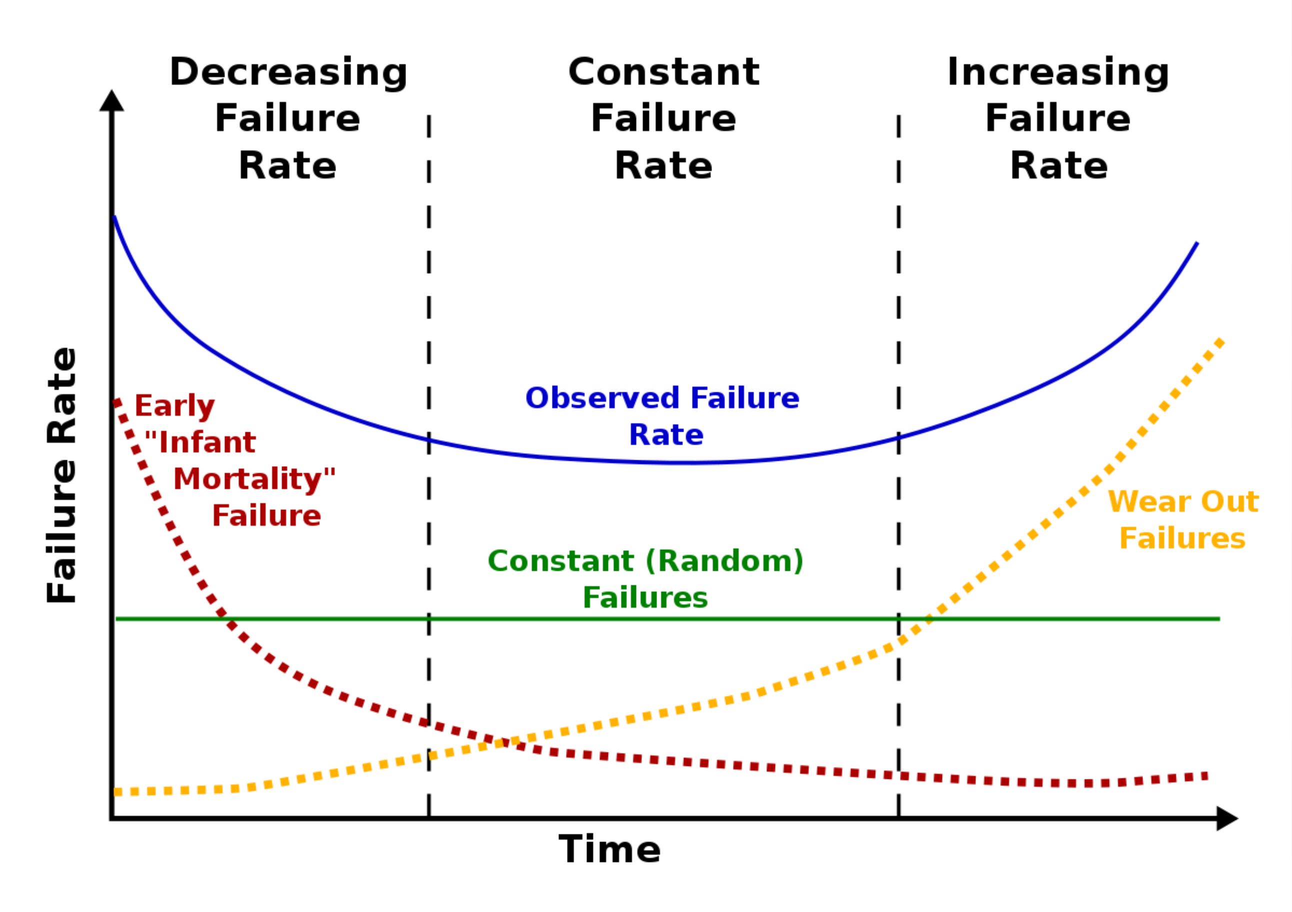
- Voluntary damage
- Failure
- Human error
- Natural disaster

General principles

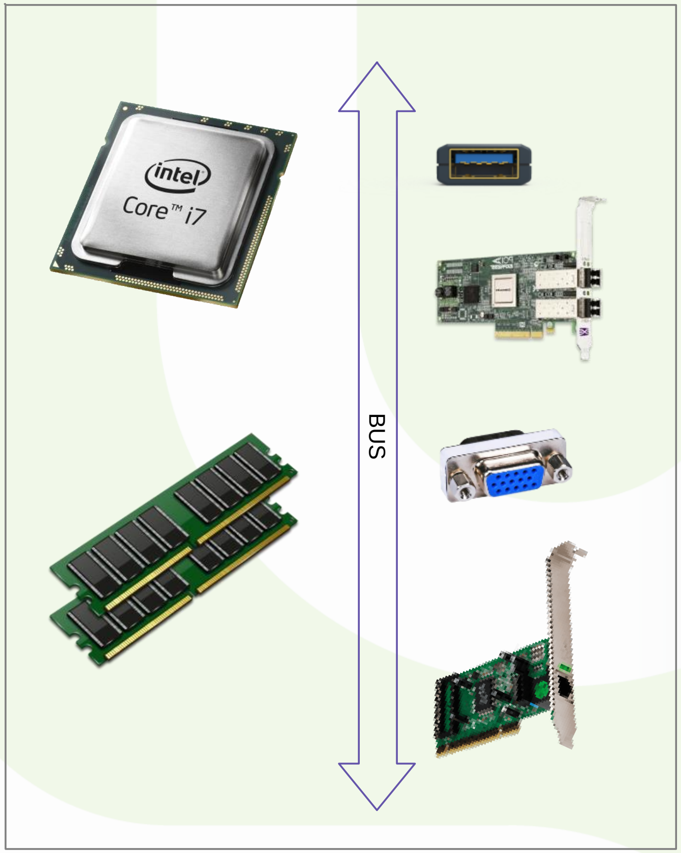
- Robustness
  - do not make things over-complex: as simple as possible, as complex as necessary
  - minimize failure likelihood
  - keep system manageable
- Redundancy
  - avoid ‘Single Points of Failure’
  - at all levels: environment, system, component, device, connection...
- It is not enough to duplicate...
  - failure detection and management
  - failover management
  - replicate state to allow fast restart

Component-level security

Hardware reliability



Simplified view of a computer

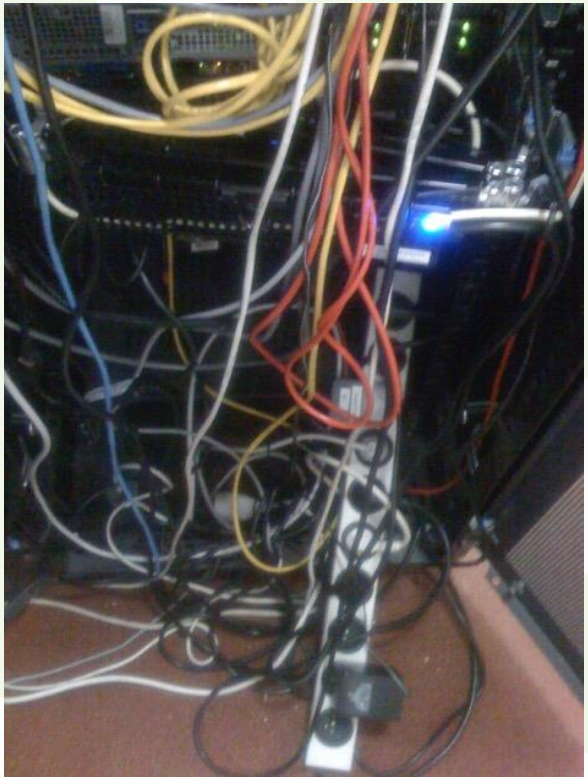


Component redundancy

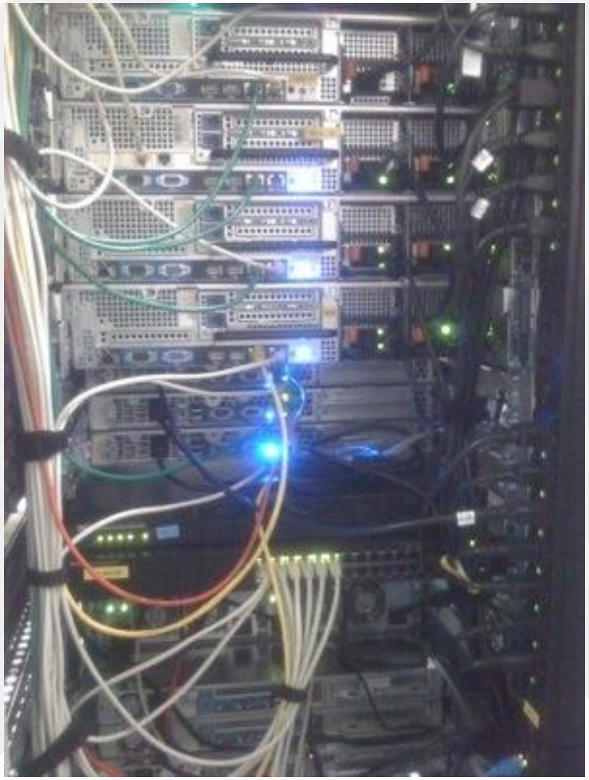
- CPU
  - multiple CPU/CPU boards
  - hot swappable
- Memory
  - detection/correction mechanisms
  - “memory scrubbing”
- I/O interface
  - multiple interfaces provide higher bandwith (i.e. trunking)
  - in case of failure, transfer in degraded mode
  - manual or automatic failover
- Cabling
  - length, labeling, placement

Cabling

😠



😊



Component redundancy

- Power supply
  - redundant power supply: n + 1, n + 2
  - up to power source
  - Uninterruptible Power Supply (UPS) for temporary outage
  - multiple providers and paths
  - generator
- Hardware interventions...
  - ...can cause more trouble than they aim to solve
  - require
    - care
    - training
    - tools (ex: anti-static mat and wristband)

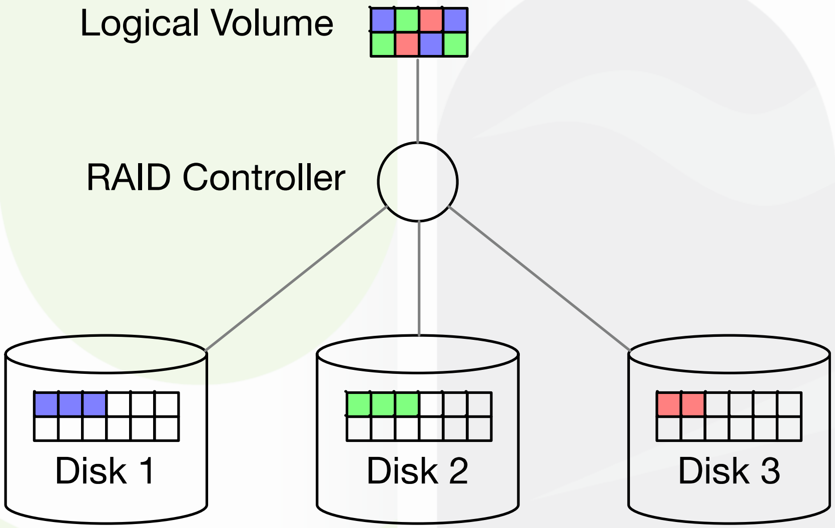
Data storage

- Different types of support
  - variable capacity
  - variable durability
  - variable security
  - mobile parts ⇒ higher failure rate
- Same redundancy principle
  - Duplicate units, devices, support types, connections, localization
- Disk-level: RAID
  - Redundant Array of Inexpensive Disks (vs. SLED – Single Large Expensive Disk)
  - defines logical (virtual) volumes on top of physical disks
  - several raid levels
  - combines 3 mechanisms
    - mirroring
    - striping
    - parity control

RAID

- Raid 0 - Striping
  - no redundancy
  - load spread over multiple physical disks
  - allows to create volumes larger than single physical disk
  - two parameters
    - #disks (stripe width)
    - #Bytes per chunk (stripe size)
  - hard to optimize
    - too small: load spread over all disks, but files split across multiple chunks
    - too large: overhead for file access is low, but disk load is not even
  - one disk fails ⇒ data lost

Raid 0 - Striping

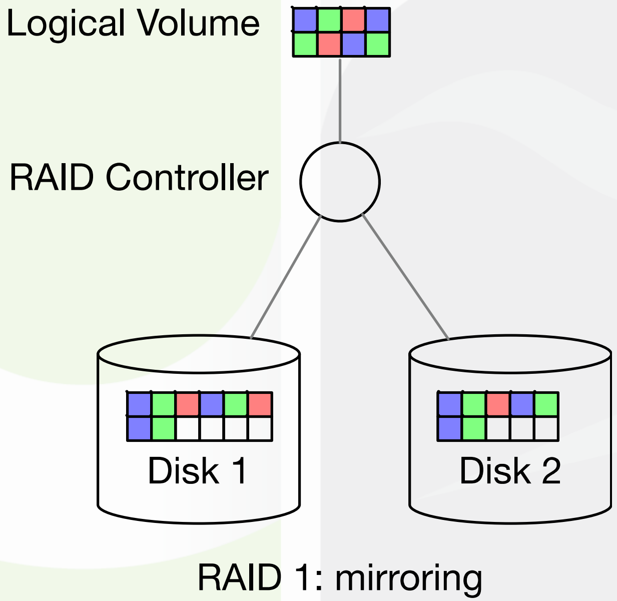


RAID 0: striping

RAID

- Raid 1 - Mirroring
  - data redundancy
    - disks 1 and 2 are in perfect sync
  - possible concurrent read
  - slower write
  - storage efficiency: 50% (two way mirror)
  - in case of failure: replace defective disk and rebuild mirror

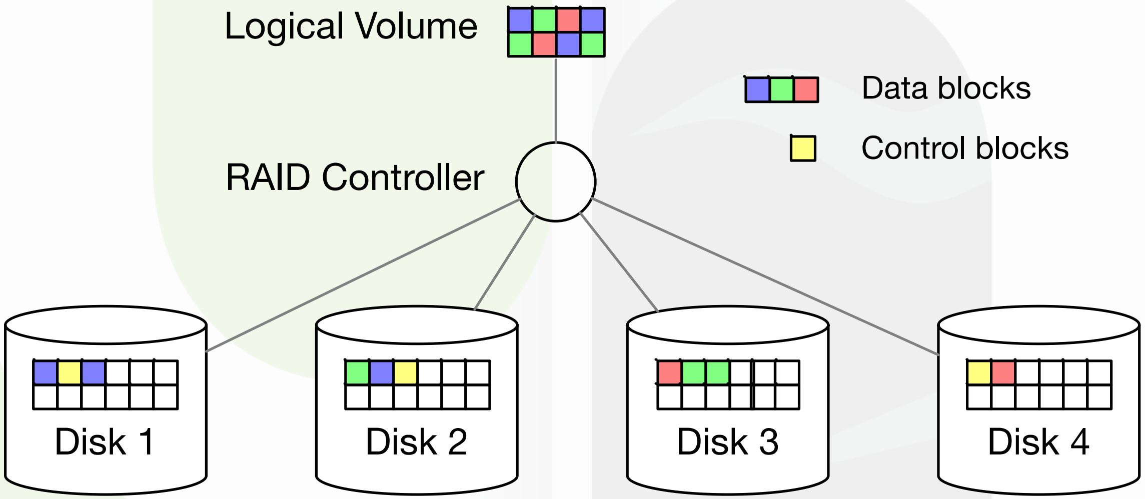
Raid 1 - Mirroring



RAID

- Raid 5 – Striping + parity check
  - n-way RAID 5:
    - n-1 data chunk + 1 parity chunk
  - possible concurrent read
  - slow write
    - write data chunk + parity chunk (requires data chunks read)
  - storage efficiency: (n−1)/n
  - in case of failure: replace defective unit and rebuild lost chunks (requires reading entire stripe)

Raid 5 – Striping + parity check



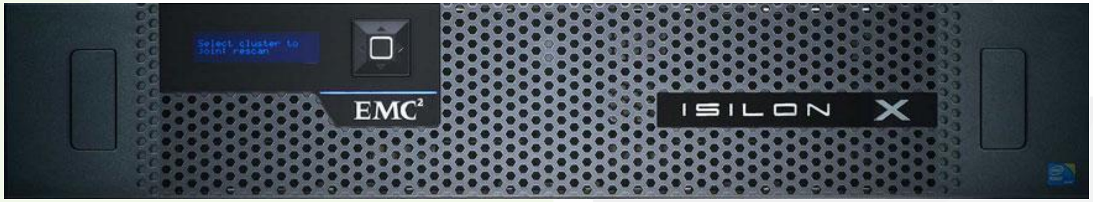
RAID 5: data + control block

RAID

- Other RAID levels
  - Raid 0+1 – mirror of stripesmiroir de stripes
  - Raid 1+0 – stripe of mirrors
  - RAID 6 – extension of RAID 5 to allow loss of 2 disks (uses 2 blocks of parity)
- RAID controllers
  - software vs hardware controller
  - different performance level/cost
  - ex. Veritas Volume Manager, LVM, DiskSuite...

Storage units

- Dedicated solutions (CPU, RAM, storage)
- Advanced functionality
  - snapshot
    - Split mirror or Copy on write
  - Remote copy
- EMC, Oracle/StorageTek,...



EMC Isilon X210: up to 48TB

Storage units

Oracle ZS5- series
up to 11.5PB (10^{15}B)

Storage units

System-level security

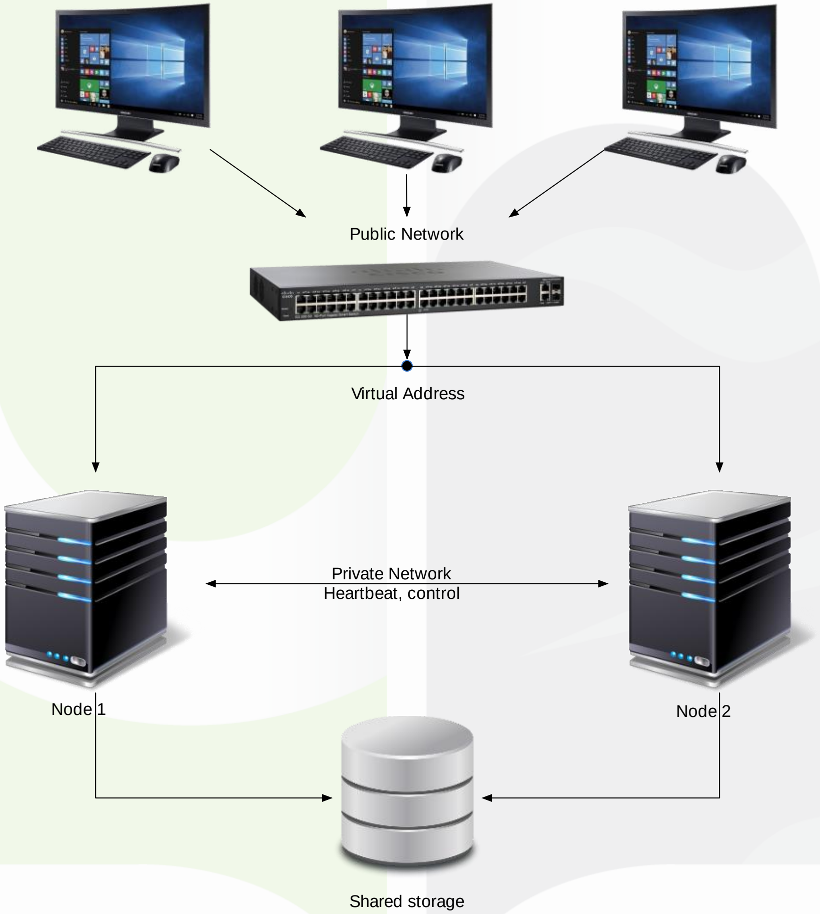
Virtualization

- Virtualization is a very old concept
  - idea: share a physical resource between multiple clients by creating virtual resources on top of it
  - i.e. timesharing, virtual memory, logical volumes, VLAN...
- Motivations
  - cost-effectiveness
  - consolidation
  - hosting space
  - manageability
  - energy saving

High availability

- System redundancy
  - solution to failure that affect more than one component or SPOF (sub-system, OS...)
  - possible DRP solution
- Service virtualization: service is running on top of a logical host that sits on top of a cluster of physical machines. In case of a machine failure, others in the cluster take over
- Cluster types
  - Failover
    - service fails over from the failed node to a healthy one
  - Load balancing
    - service executed on a pool of similar systems; in case of a machine failure, others in the pool take over

Failover


Public Network
Virtual Address
Private Network
Heartbeat, control
Node 1
Node 2
Shared storage

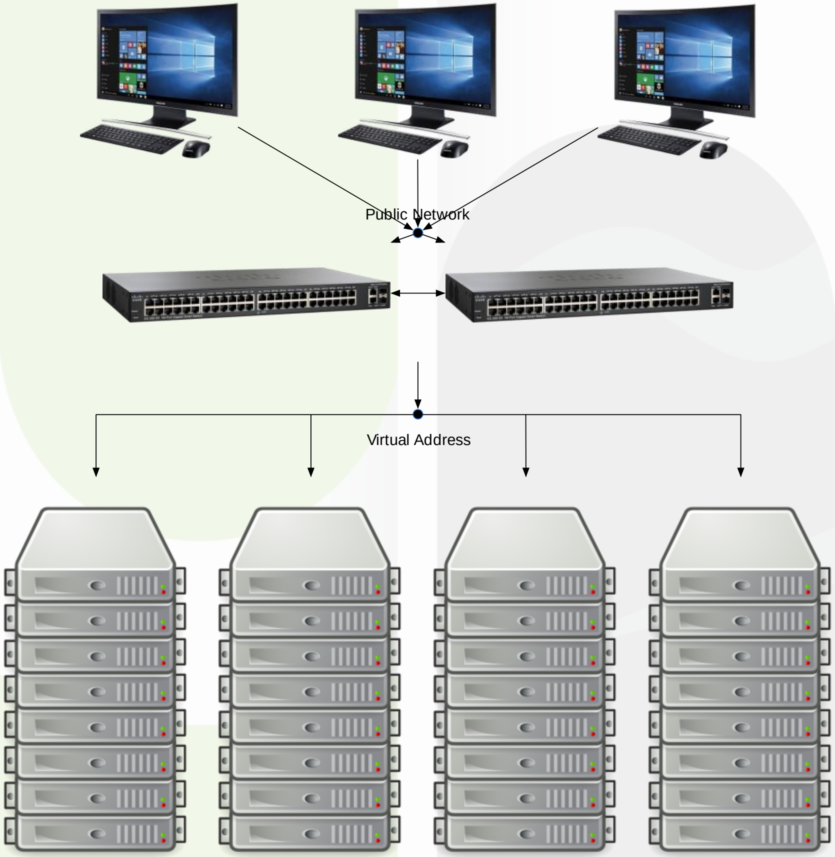
Failover

- Cluster configuration
  - shared state
  - inter-node communication
    - heartbeat
    - quorum device
- Service integration
  - provide scripts to start/stop/check service
  - define necessary resources: logical volumes, IP address...
  - preferred node
- Failover
  - manage timeout, ping-pong
- Identify service dependencies

Load-balancing

- For stateless services: webservers, directory services (LDAP, AD, DNS...)
- Based on server farm
- Spread the load across the farm nodes
- Load distribution algorithm can be as simple as round-robin or more complex, for instance taking into account machine or request characteristics
  - DNS Load balancing, IP load balancing, reverse proxies

Load-balancing



Network-level security

Network security

- Availability
  - once again: redundancy
    - NIC – network interface card
    - network segment
    - providers
    - connection channels
- Access control
  - Network is the gateway to the server and the organization
  - Firewall
    - packet filtering
    - stateful packet inspection (SPI)
    - deep packet inspection (encrypted channel?)
    - application firewall
  - Control connecting devices

Network security

- Confidentiality, integrity
  - use encrypted channels
  - according to network layer
    - PGP/gpg (email), DomainKeys and SenderID/Sender Policy Framework (SMTP), DNSSEC
    - SSL/TLS
    - IPSec
      - Authentification (AH – Authentication Header) et confidentialit´e (ESP – Encapsulation Security Payload)
      - Mode transport : paquet initial enrichi des informations AH ou ESP
      - Mode tunnel : encapsulation IP-dans-IP
    - VPN: secure tunnel between workstation and organization network
      - nomad users
      - third-party access

Network security

- Network isolation
  - split internal networks into several isolated sub-networks
  - network segregation: DMZ
  - 3 networks
    - LAN (internal)
    - WAN (external - internet)
    - DMZ (demilitarized zone)
  - 3 flows
    - LAN → WAN
    - WAN → DMZ
    - LAN → DMZ
  - use multiple firewalls to separate networks
- Integrated solution: CASB – Cloud Access Security Broker
  - “CASBs provide a consistent and convenient point of control over user activity and user data in a growing set of SaaS and other cloud-based applications.” (Gartner Magic Quadrant for Cloud Access Security Brokers)

Hosting

Datacenter

Datacenter

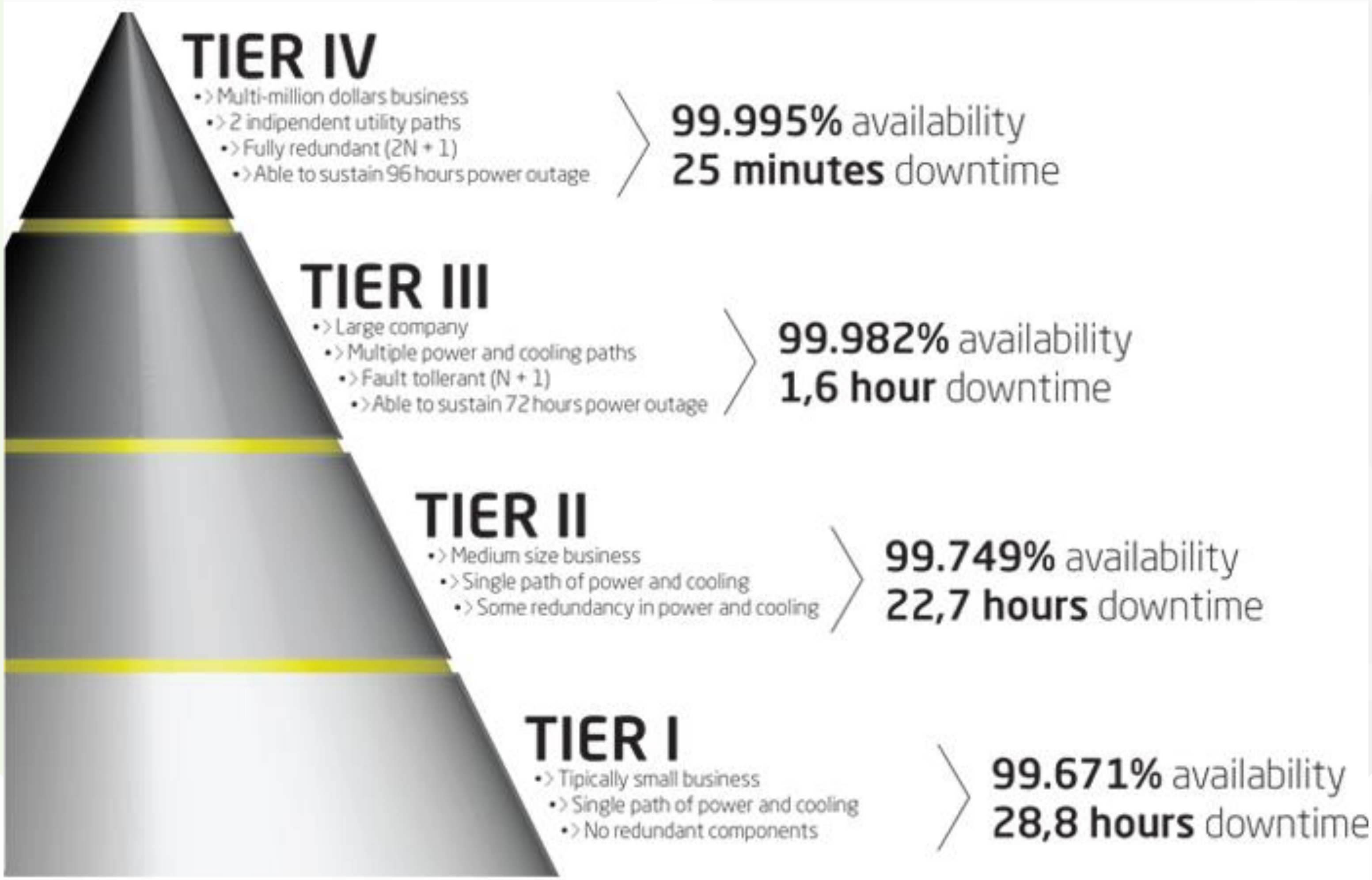
Datacenter

- Complete hosting solution offering all required facilities
  - elevated ground, cabling, access control
- HVAC - Heat, Ventilation, Air Conditioning
  - system density increases heating
  - rack placement
  - optimize air flow in the room (cool corridor)
  - temperature (American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)
    - 20° to 24°C (2005)
    - 18 to 27°C (2011)
    - Class A2 (35°C) or even A3 (40°C) and A4 (45°C)
- HVAC system is of critical importance: proper sizing and redundancy!

Datacenter

- Fire
  - detect: (redundant) probes
  - CO_2, Halon, FM-200, Inergen
- Power supply
  - redundant connections (and providers?)
  - UPS for short interruptions
  - diesel generators for long outage
  - do not power all systems at once
  - test the full procedure regularly
- Identify system dependencies for root cause analysis (what is the impact of...?)

Datacenter



TIER IV

- > Multi-million dollars business
- > 2 indipendent utility paths
- > Fully redundant (2N + 1)
- > Able to sustain 96 hours power outage

99.995% availability
25 minutes downtime

TIER III

- > Large company
- > Multiple power and cooling paths
- > Fault tollerant (N + 1)
- > Able to sustain 72 hours power outage

99.982% availability
1,6 hour downtime

TIER II

- > Medium size business
- > Single path of power and cooling
- > Some redundancy in power and cooling

99.749% availability
22,7 hours downtime

TIER I

- > Tipically small business
- > Single path of power and cooling
- > No redundant components

99.671% availability
28,8 hours downtime

Source :https://uptimeinstitute.com/TierCertification/certMaps.php

Datacenter

- Management procedures
  - ITIL – Information Technology Infrastructure Library
    - IT Service Delivery
    - IT Service Support
    - Service desk, Incident Management, Problem Management, Configuration Management, Change Management, Release Management
- Dedicated staff

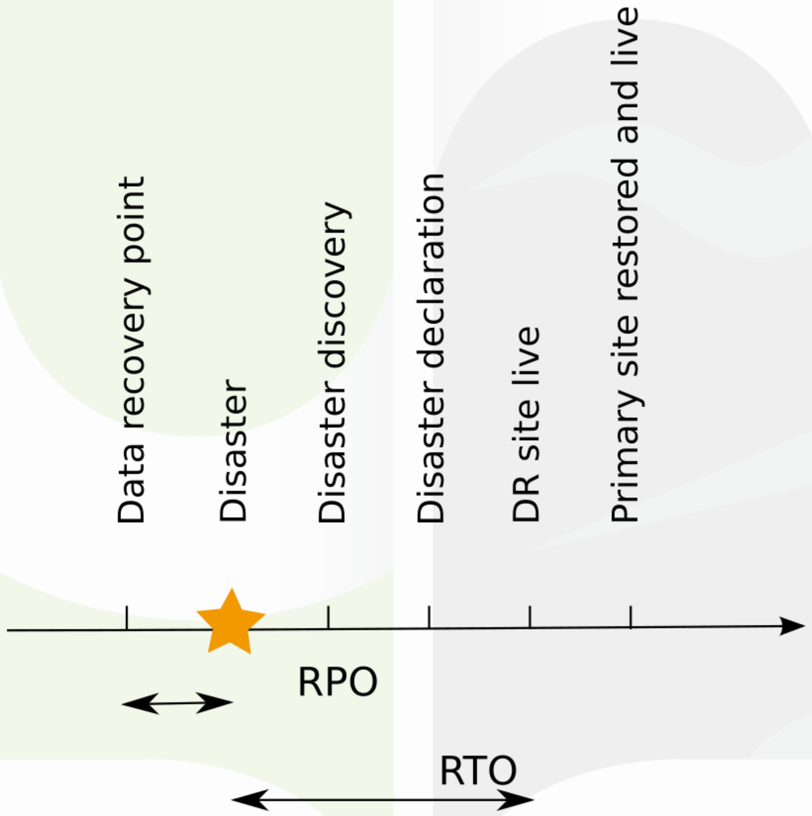
Disaster recovery

Disaster Recovery

- DRP or BCP?
- Goal: handle major incident
  - natural disaster (flooding, typhoon, earthquake...)
  - accident, fire
  - attack, sabotage, terrorism
  - massive data or system corruption
- Solution: duplicate operation site
  - and define procedures...
- Identify scope of DRP
  - not all services are concerned!
  - risk-based approach
  - prioritize services
  - identify resources required

Disaster Recovery

- Incident, recovery, RTO, RPO



Disaster Recovery vs High Availability

- DR is business driven: strong involvement of business side: not an IT problem only!
- Longer outage
- Larger impact
  - number and size of components/systems
- Higher risk and cost
- DR requires extensive procedures
- DR is not a fully automatic process

Disaster Recovery

- General approach
  - Objective and scope definition
  - System identification
  - Definition of parameters (RTO, RPO), staff and responsibilities
  - High-level design of the solution (principles)
  - Technical design of the solution (technologies)
  - Implementation of the solution
  - Elaboration of procedures
  - Training
  - Test, Test, Test!
  - Evaluate and improve

Disaster Recovery

- Primary and backup (DR) site
  - owned by the organization?
  - partner’s location via mutual agreement?
  - outsourced?
  - where to place DR site?
    - not too close, not too far!
    - avoid similar risks
- Site synchronization
  - hot stand-by
    - DR site is an exact copy of primary site
  - cold stand-by
    - requires data restore on DR infrastructure
    - hint: store backups on DR site for quicker restore
  - hybrid approach: activity split on primary and backup sites; in case of incident, the healthy site takes over

Disaster Recovery

- Long distance synchronization
  - asynchronous mirroring
  - backup/restore
  - log shipping
  - long distance cluster
  - file synchronization (rsync)

Monitoring & alerting

Monitoring and alerting

- Should something (seem to) go wrong? Make sure you get informed!
  - decide what to monitor
  - decide where to put the probes to avoid impact the system performance
  - fine tune the monitoring system to avoid false positive/false negative; adapt threshold
  - many existing tools
    - Patrol, OpenView, Nagios...
- Send alert
  - email
  - SMS
  - organize support team
  - define and document reporting and escalation procedures

Contracts

Contracts …

- Vendor selection: check the following
  - re. products
    - flexible, modular, up-to-date product line
    - credible roadmap
    - Interoperability
    - site visit
  - re. organization
    - existing partnerships
    - local team/resources
    - support organization
- Support contract
  - with hardware and software vendors
  - different levels of support and price
  - of critical importance for business-critical systems

SLA – Service Level Agreement

- defines the service
- defines requirements in terms of availability
    - incl. performance aspects
    - max. outage duration over the period
    - max. cumulative outage duration over the period
    - max. outage per incident
    - max. number of incident over the period
- differentiate between failure severity (minor/major outage)
- define planned maintenance slots
- define responsibility and procedures
- define communication and escalation mechanisms
- define penalties in case of failure to meet requirements
- can be concluded with external partners or internally between departments
- do not over- (under-)estimate your needs

Conclusion

- Protecting the infrastructure requires a manifold approach
  - Technical
  - Organizational
  - Contractual
- Redundancy as the main way of ensuring availability
- Refer to ISO 27002 Clauses 11-13, 16