Maintaining Non-Stop Services with Multi Layer Monitoring

Lahav Savir
System Architect and CEO of Emind Systems
lahavs@emindsys.com

www.emindsys.com

The approach

- **Non-stop applications can't leave on their own**
- **More complex systems require more monitoring**
- **Proactive system monitoring**
  - Customized monitors
  - Monitor each process, component and application separately and all as a whole
  - Proactive correction of problems before they become noticeable by your customers.
  - Allow application to function at maximum availability
  - SNMP monitoring of application infrastructure
  - Alerting of potential problem or situation prior to accuracy
  - Visual layered display of the entire data center

Monitoring is not just for System Administrators but for Developers as well

The goal for monitoring is to

keep track of the running services 24/7,

find troubles as early as possible and

keep you alerted (only when needed...)

Good monitoring infrastructure provides you a quick and direct troubleshooting abilities via visual representation of the system status

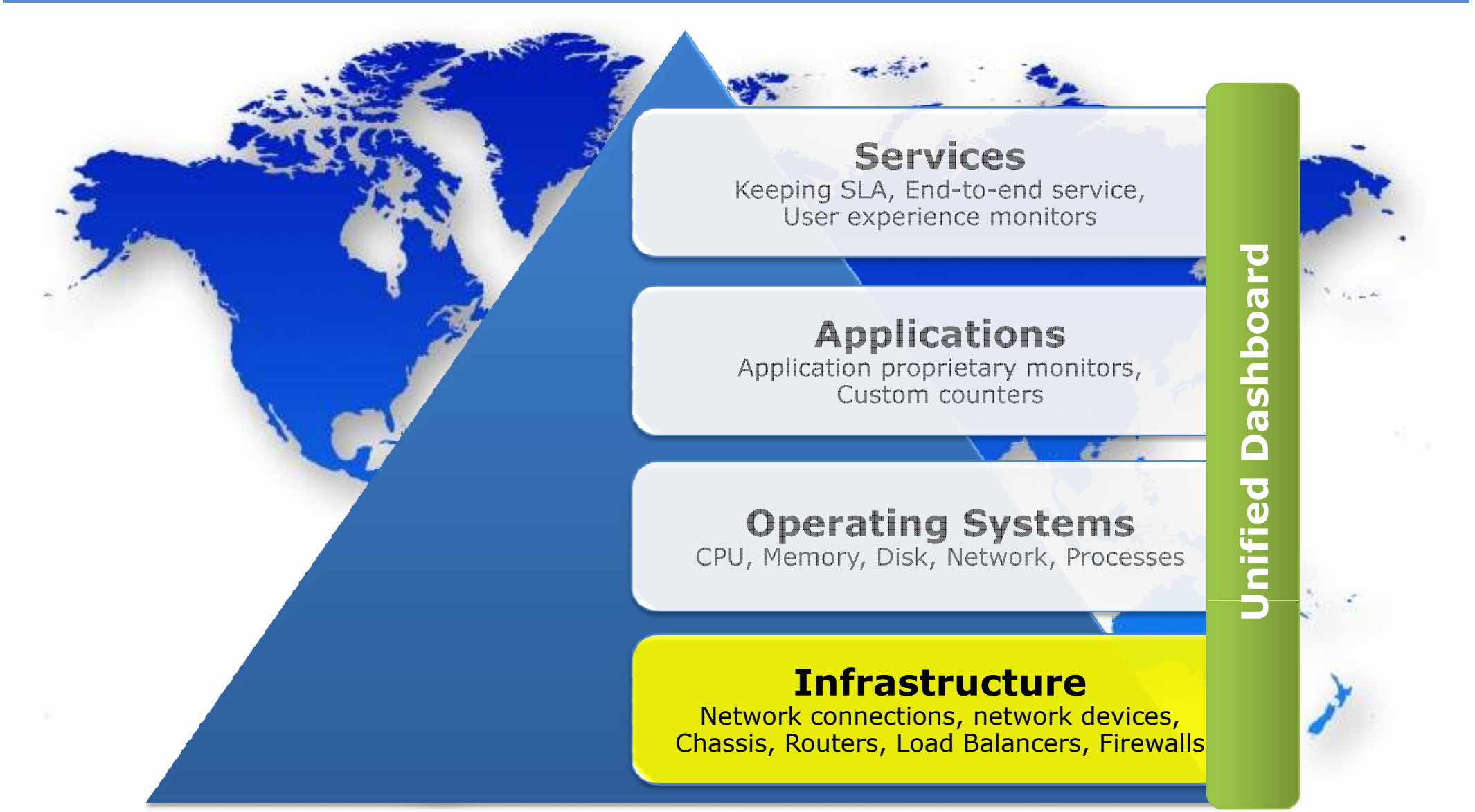
Multi-Layered Monitoring

Visualize the information

- **Use Maps & Views**
  - Visualize the topology
  - Visualize the application flow
  - Focus on different layers
- **Layered views (service & host groups)**
  - Network, Hardware, OS, Application
- **Different roles looking for different info**
- **Graph Service performance**
  - Transactions, Success rates, Cache
- **Aggregated view**
  - Cluster's average

Why multi layer ?

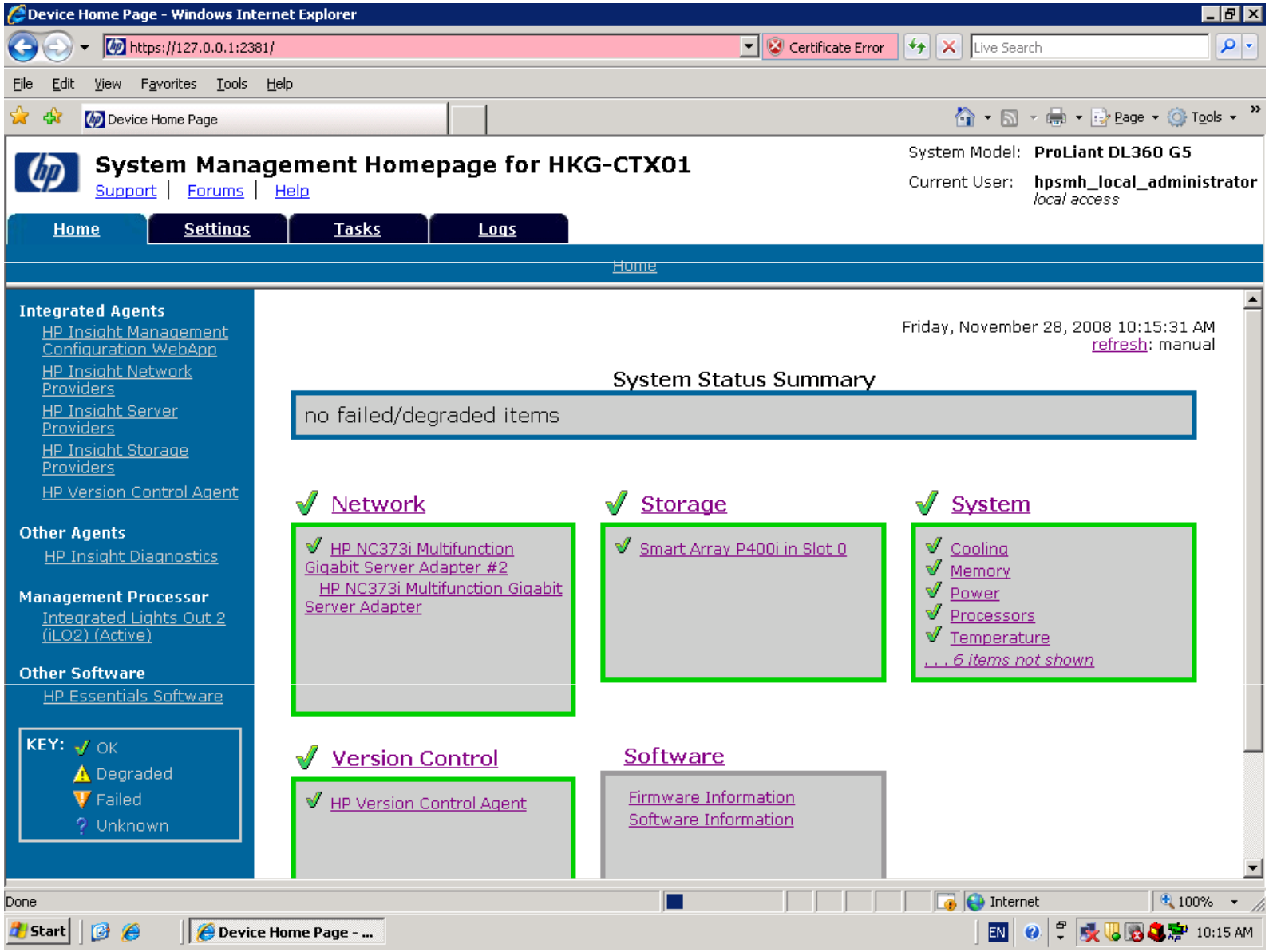
- **Correlated information on one uniform view**
  - Network throughput, CPU usage, Application usage
- **Generate aggregated reports for different machines & layers**
- **Collect information from all nodes**
  - Switches, routers, firewalls, load balancers, storage, servers, applications
- **Collect different types of data**
  - Utilization, throughput, concurrency, cache status
  - Application performance, error rates
- **Objective**
  - Find the root cause via visuals on the dashboard !
  - Be aware of what's going on


Services
Keeping SLA, End-to-end service,
User experience monitors
Applications
Application proprietary monitors,
Custom counters
Operating Systems
CPU, Memory, Disk, Network, Processes
Infrastructure
Network connections, network devices,
Chassis, Routers, Load Balancers, Firewalls
Unified Dashboard

Infrastructure layer

- **Hardware redundancy my be dangerous if you don't keep your eyes on it**
  - Administrators not always seeing the HW
  - Redundant hardware can fool you (until it dies)
- **Vendor specific MIBS / Syslog**
- **Today's hardware provides detailed status interfaces**
  - Power supplies, power usage
  - Fans & temperature
  - Disk controllers & drives
  - Switch ports, interfaces
  - Links, connections

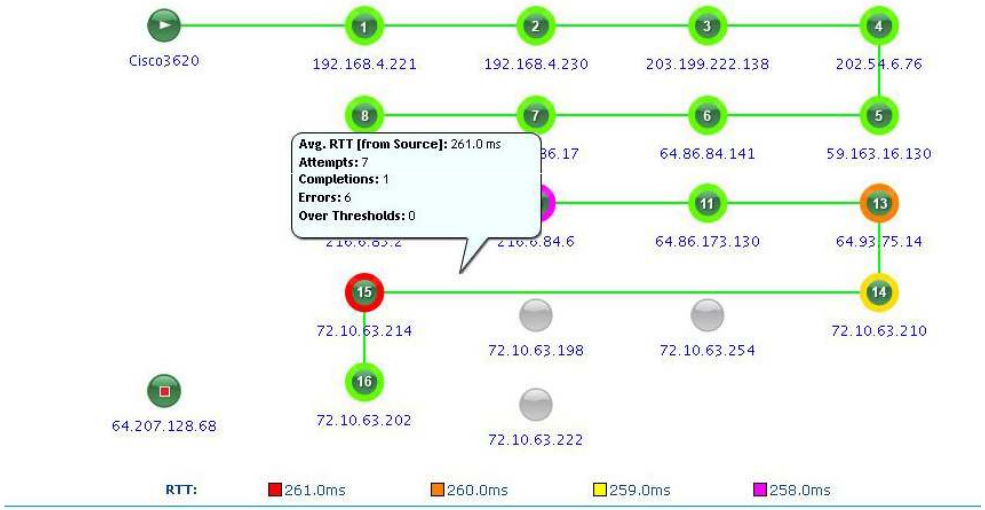
HP HW monitoring



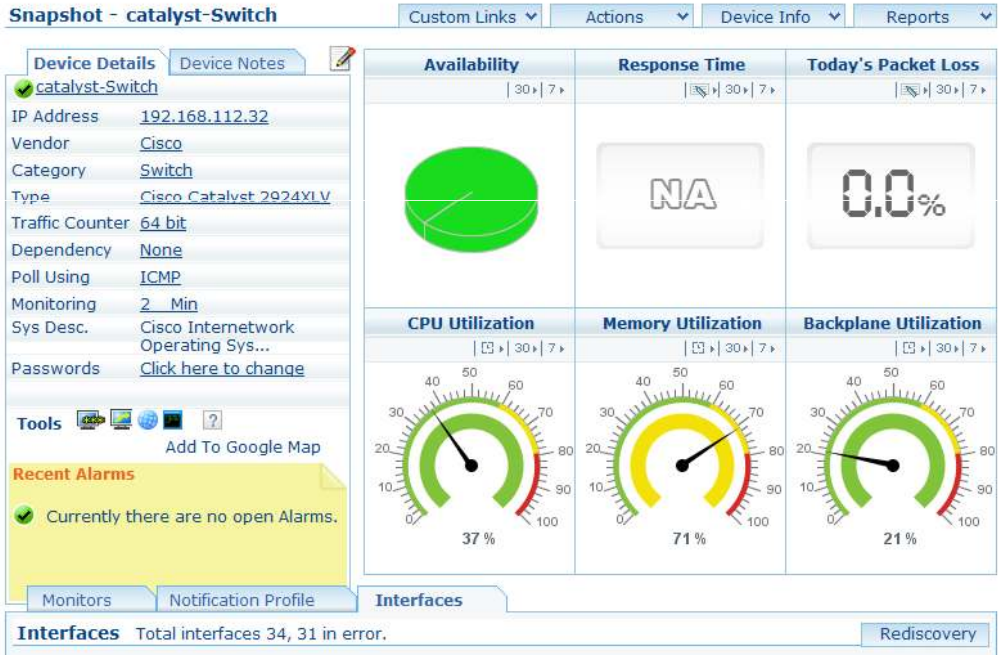
Emind Systems
empowering internet technologies

Network infrastructure health

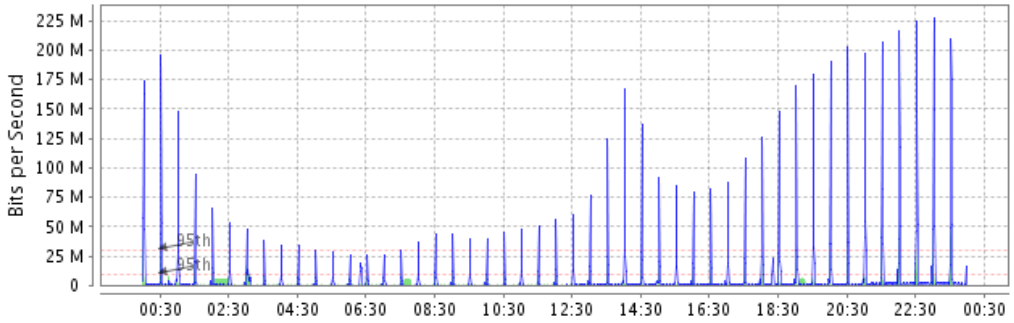
Link Quality



Devices utilization



Network throughput

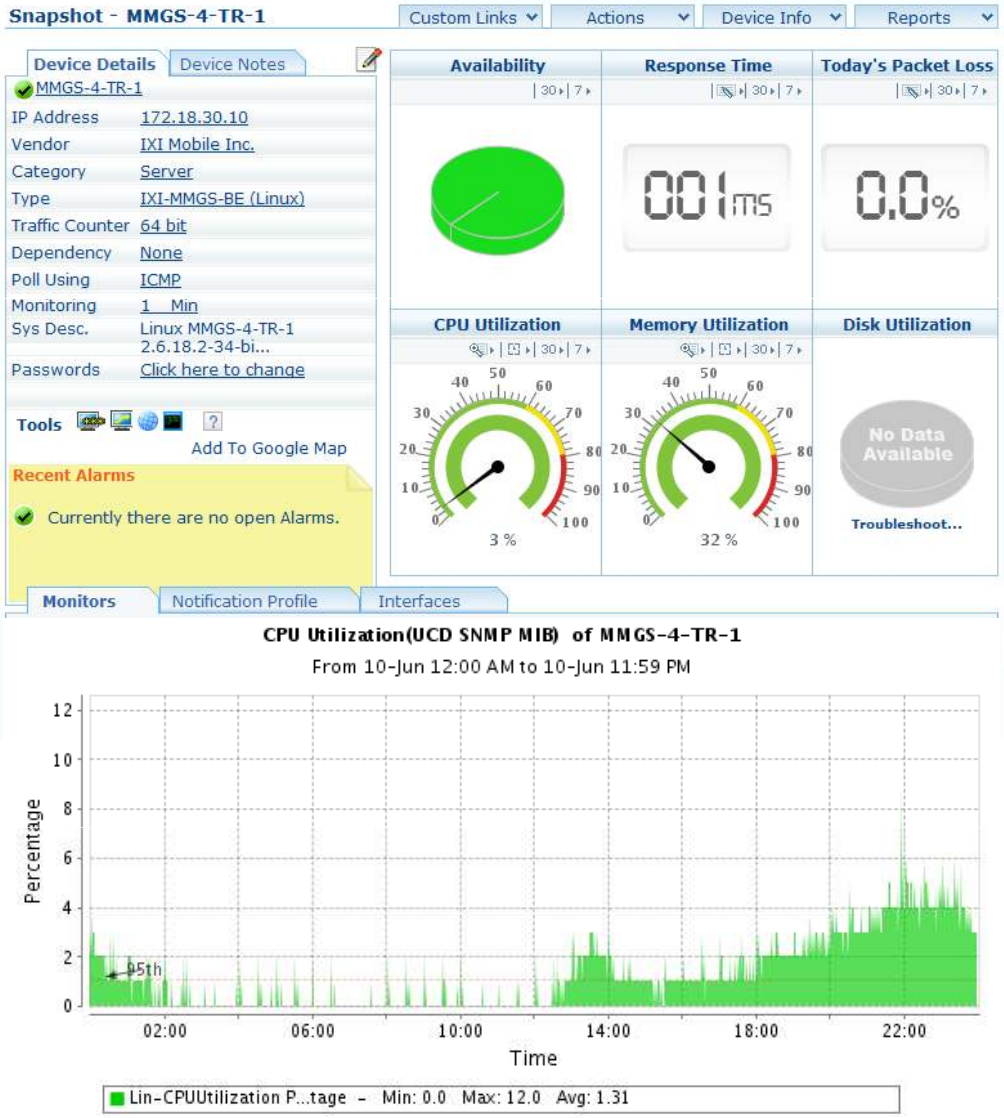


Emind Systems
empowering internet technologies

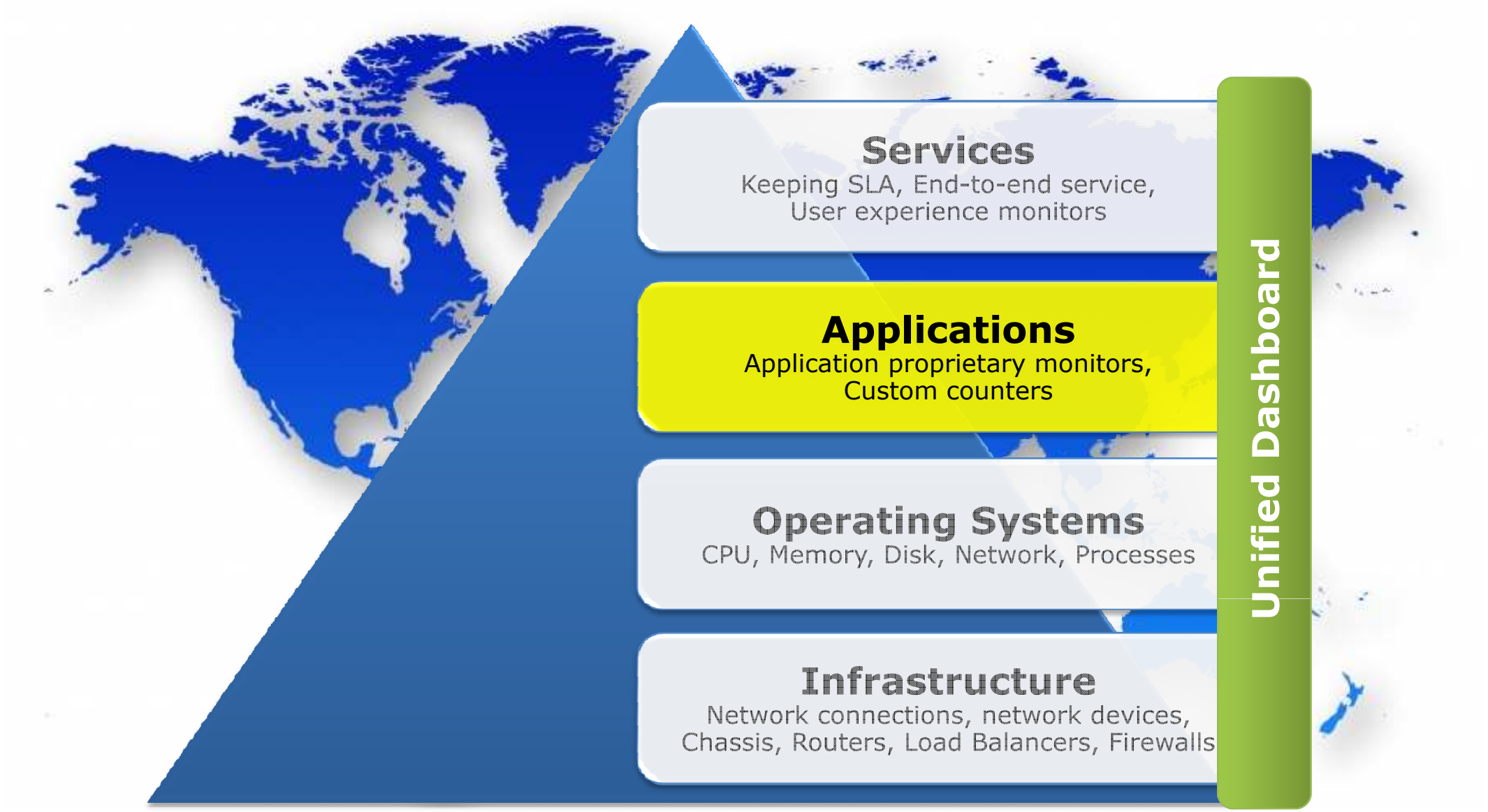

Services
Keeping SLA, End-to-end service,
User experience monitors
Applications
Application proprietary monitors,
Custom counters
Operating Systems
CPU, Memory, Disk, Network, Processes
Infrastructure
Network connections, network devices,
Chassis, Routers, Load Balancers, Firewalls
Unified Dashboard

Operating System health

- **Monitoring of OS essentials**
  - CPU, Memory, Disk I/O, Network traffic, processes, services
- **Use cases**
  - Failure on log cleanup > disks full

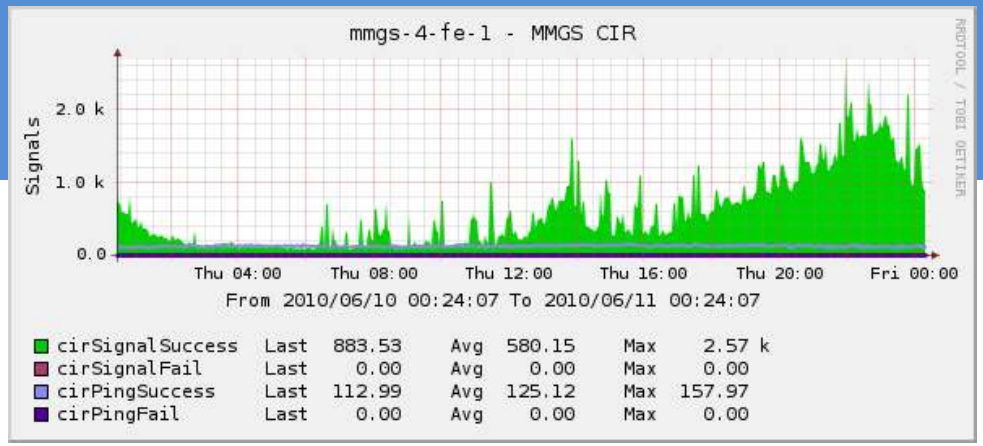


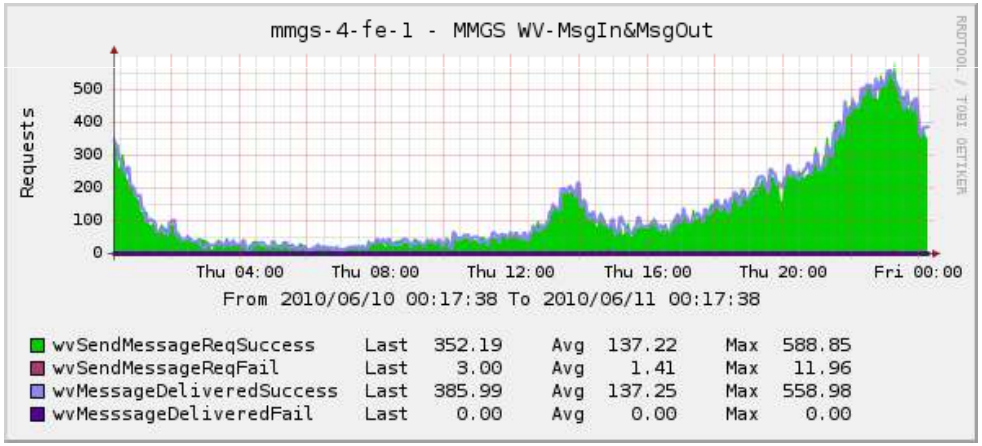
Emind Systems
empowering internet technologies

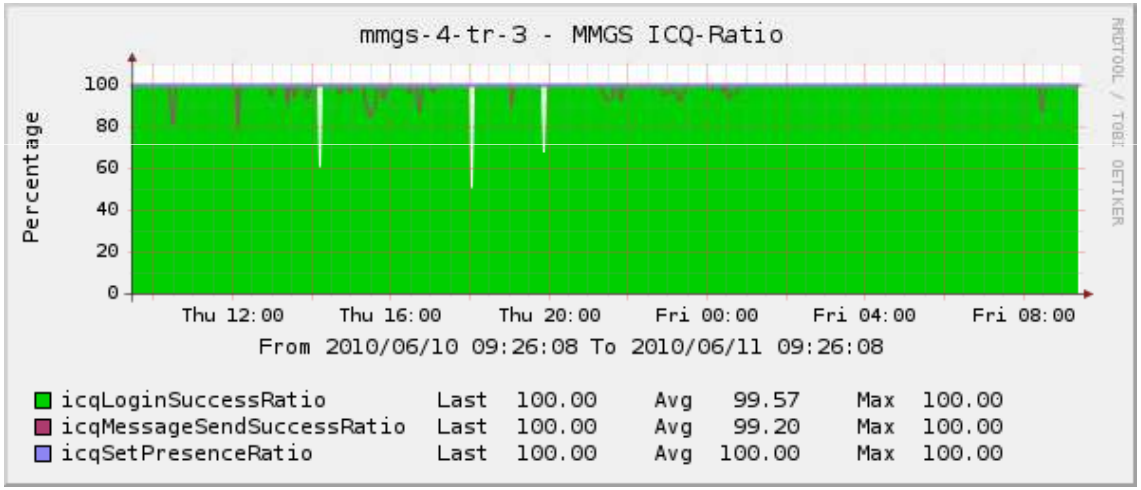

Services
Keeping SLA, End-to-end service,
User experience monitors
Applications
Application proprietary monitors,
Custom counters
Operating Systems
CPU, Memory, Disk, Network, Processes
Infrastructure
Network connections, network devices,
Chassis, Routers, Load Balancers, Firewalls
Unified Dashboard

Applications health

- **Transaction counters**
  - Measure transaction rates
  - Measure counters on input & output
- **% Success rates**
  - Success counters for primary operations

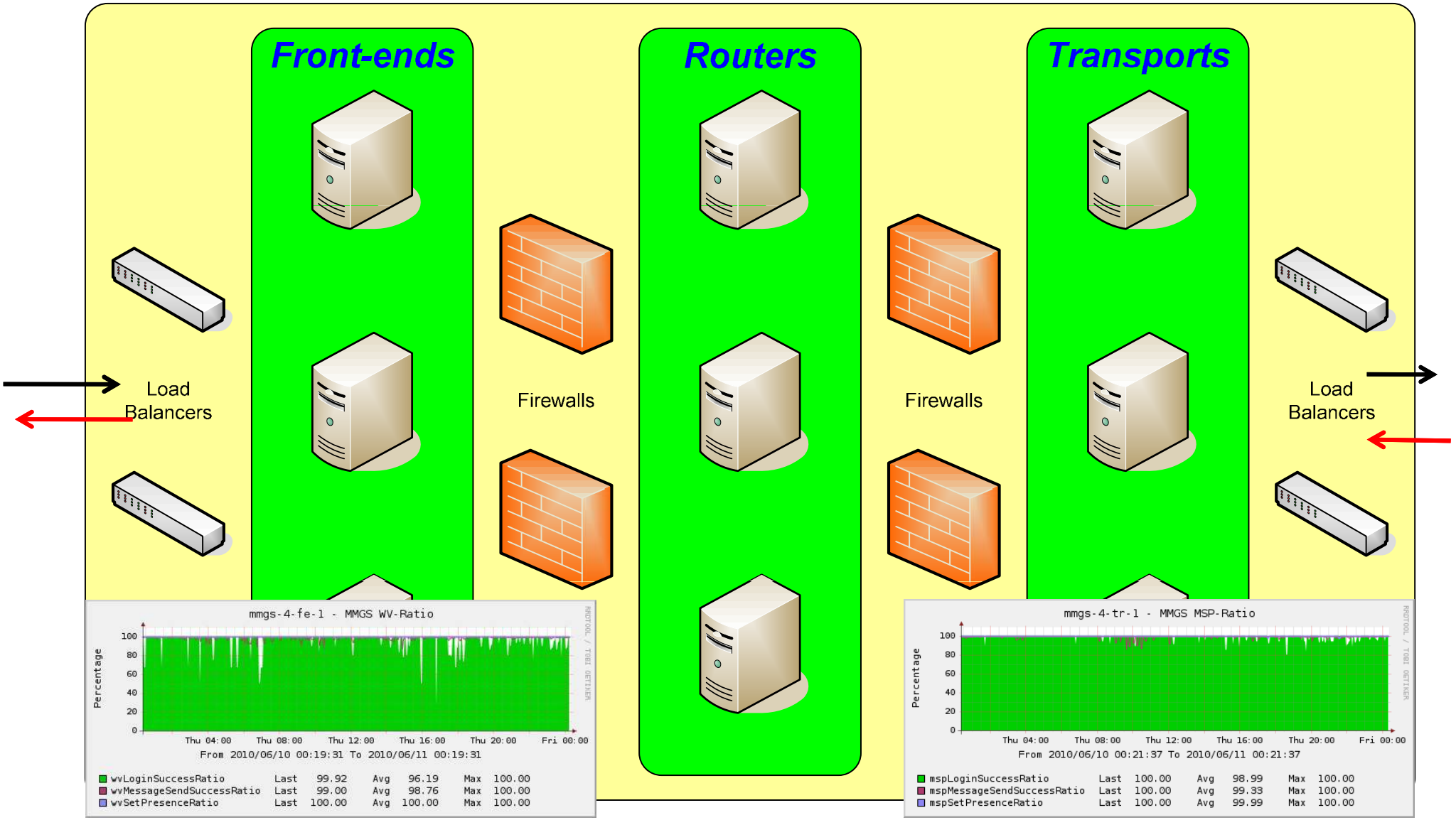






Emind Systems
empowering internet technologies

System input/output monitoring

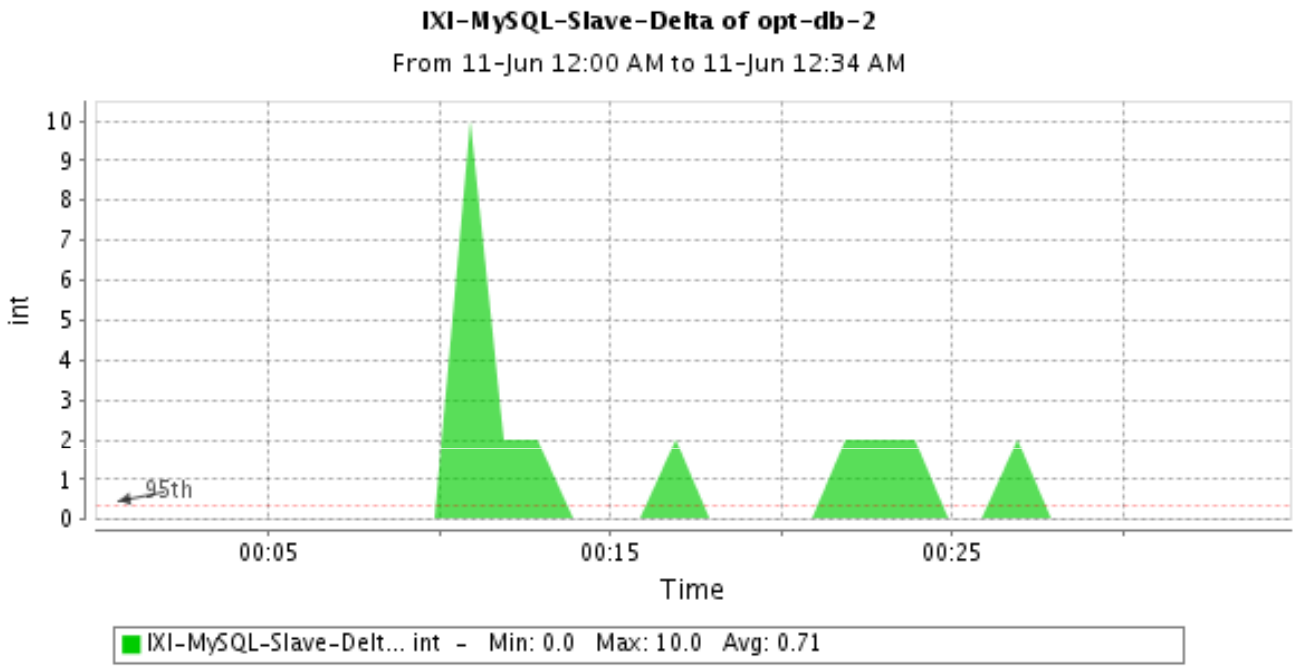


Applications health

- **Queues**
  - Processing backlog
  - Semaphores / throttle usage
- **Latency**
  - Measure the time it takes to process request / data chunk
- **Optimizations**
  - Measure compression rates

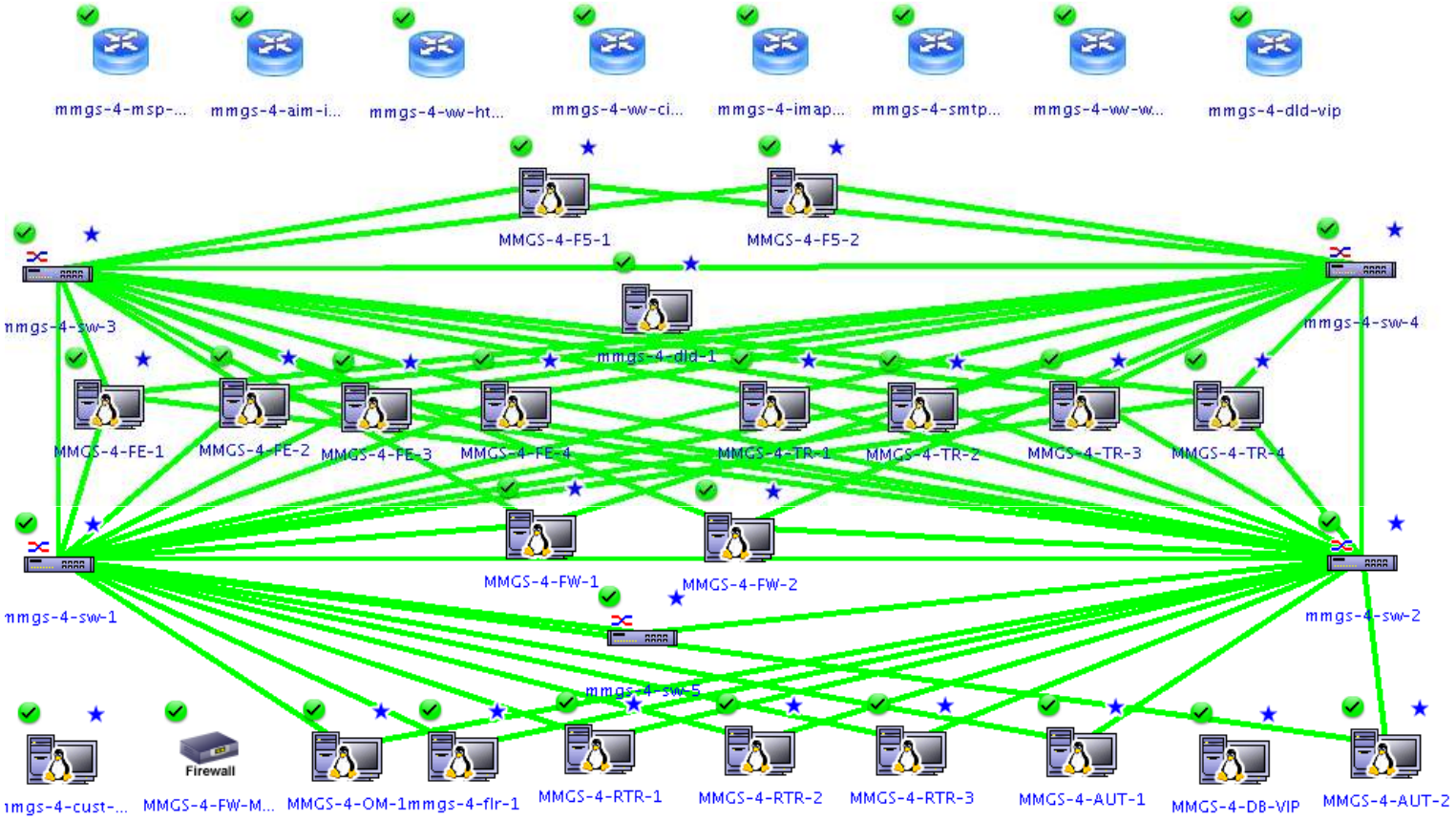
Applications health

- **DB synchronizations**
  - Replication status
  - Replication backlog & delays

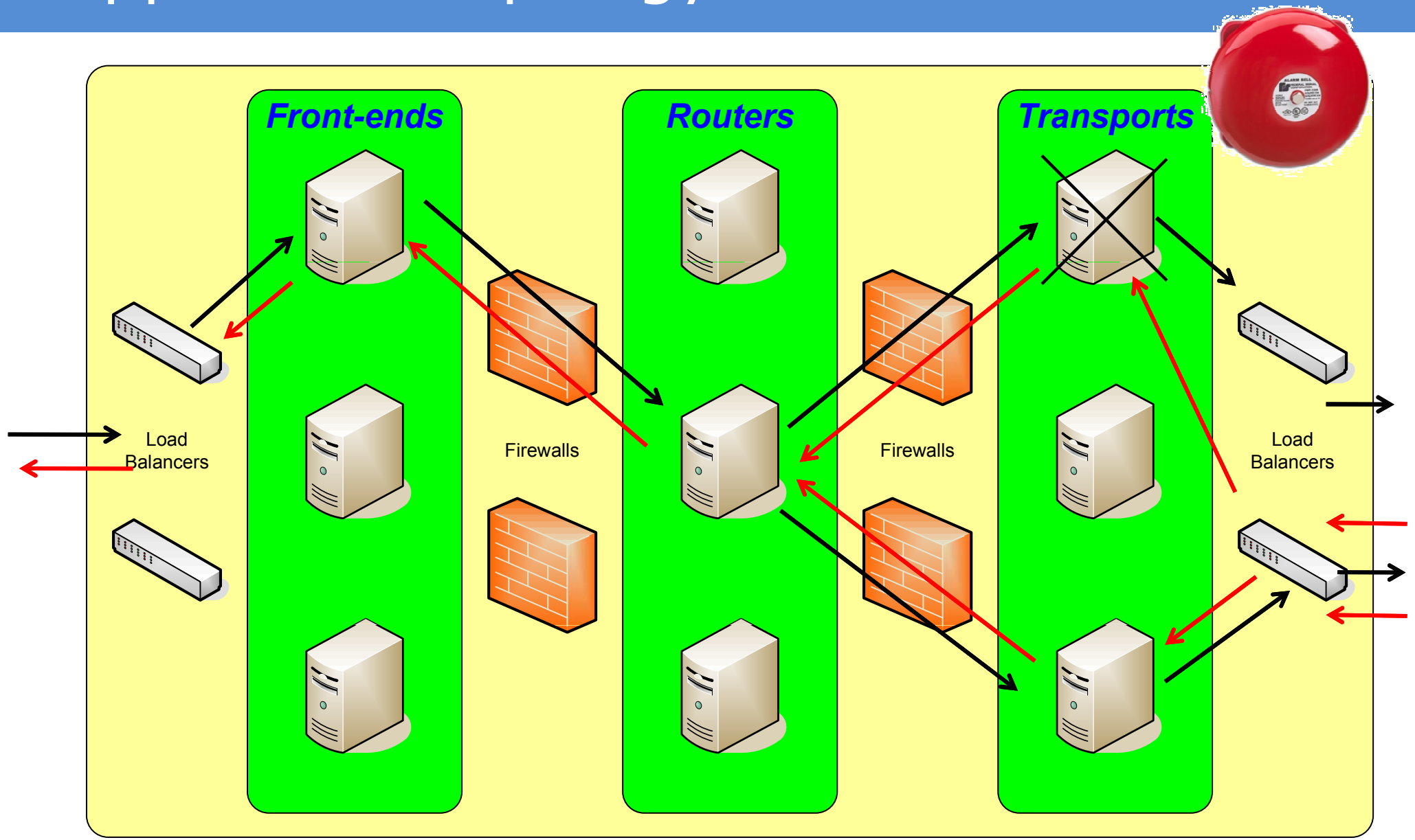


Applications health

- **Cluster & topology monitoring**
  - Track application topology changes
  - Indicate dependencies status



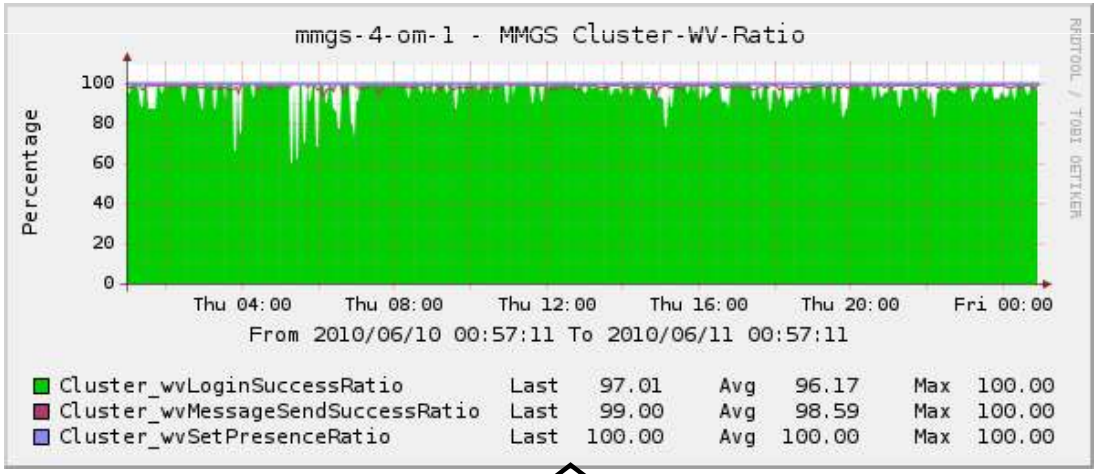
Application topology

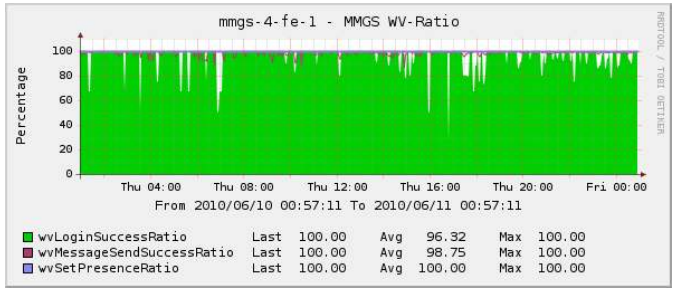


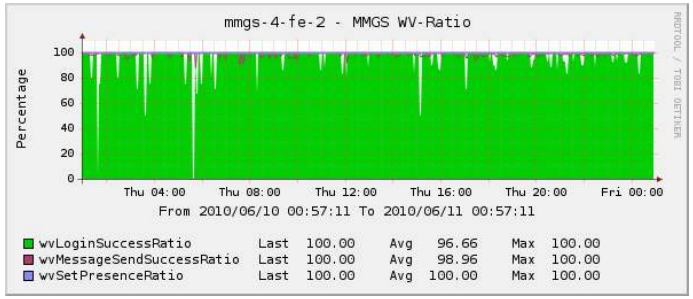

Services
Keeping SLA, End-to-end service,
User experience monitors
Applications
Application proprietary monitors,
Custom counters
Operating Systems
CPU, Memory, Disk, Network, Processes
Infrastructure
Network connections, network devices,
Chassis, Routers, Load Balancers, Firewalls
Unified Dashboard

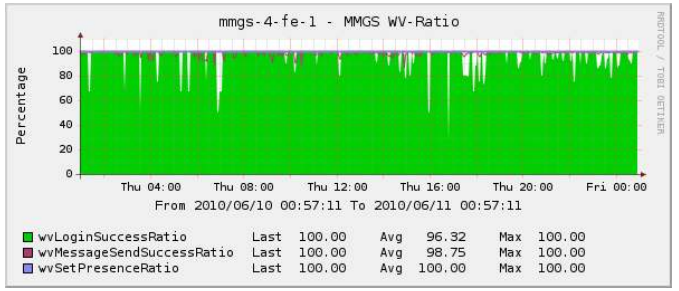
Cluster overall QoS

- **Now it's a cluster, aggregated counters**
- **Want to know what users are experiencing**





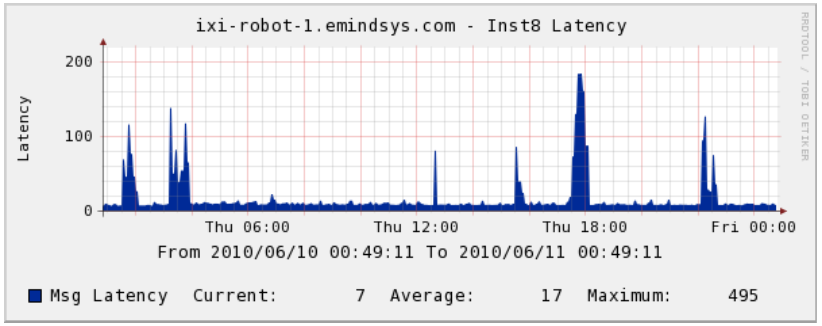


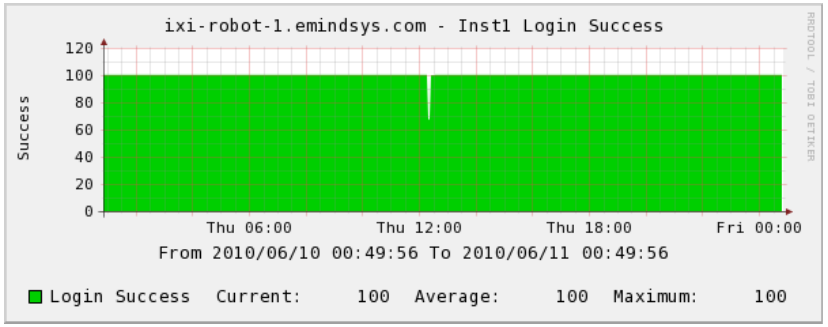


Emind Systems
empowering internet technologies

User Experience & Service QoS

- **Simulate user behavior**
  - Latency
    - How long it takes to login
    - How long it takes to send and receive a message
    - How long it takes to “check out”
  - Success rates
    - What’s the success rate of the user’s operation
  - Download speed
    - What’s the download speed from different locations
    - What’s your Content Delivery Network (CDN) performance





Emind Systems
empowering internet technologies

Recommendations

- **Build a generic monitoring infrastructure with generic tools and interfaces**
- **Use embedded SNMP**
- **Net-snmp is extendable (also for Windows)**
  - PROXY – proxy request to other SNMP agent (embedded)

```
proxy -v 2c -c public 127.0.0.1:50910 1.3.6.1.4.1.15867.2000.3.6
  1.3.6.1.4.1.15867.2000.3.6
```

  - PASS – STDOUT based subagent

```
pass .1.3.6.1.4.1.15867.2001 /bin/sh
  /usr/local/ixi/GenericSubAgent.sh
```

  - EXEC – run a script

```
exec .1.3.6.1.4.1.15867.1100.20.10 axs-imap-test-stat /bin/bash
  /opt/mas/scripts/imap_tester.sh last_state
```

- **SSH / Telnet**

Using Status files

- **Perfect for batch operations**
  - perl, python, php
- **Status file**

```
TIMESTAMP:1276203703
STATUS:0
HOSTNAME:myserver
```

- **Observer**

```
if [ $(get_time_delta ${file}) -gt ${max_d_s} ]; then
     err "Delta is greater than ${max_delta} hours"
     return
Fi
if [ "$(parse_status_file ${file} STATUS)" != "0" ]; then
     err "Last backup status is not 0"
     return
Fi
echo ${ok}
```

Command line based info.

- **Command line applications**
  - DB, Softswitch, Etc.
- **Example**
  - Snmpd.conf

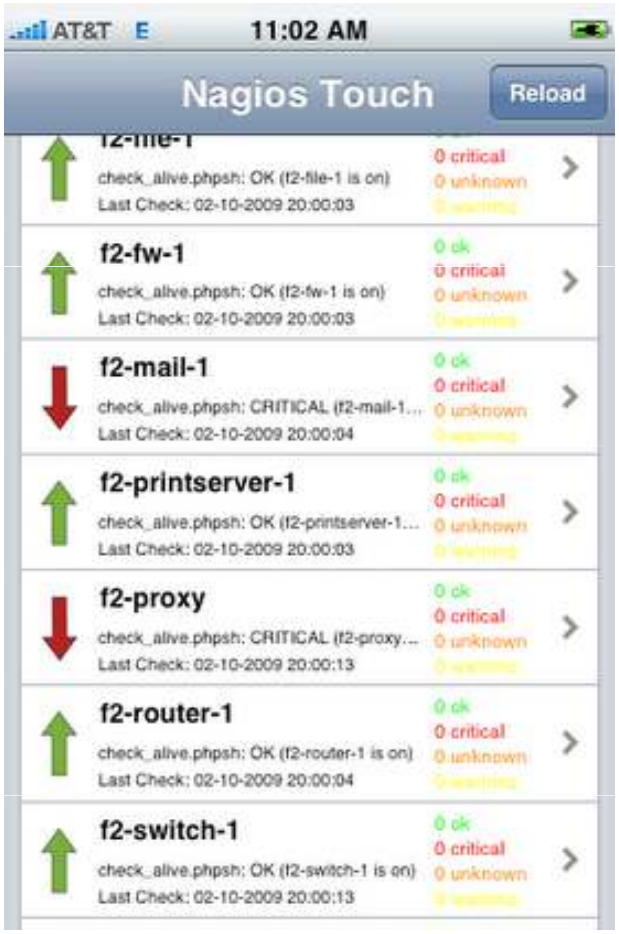
```
pass .1.3.6.1.4.1.15867.1.100 /bin/bash
/usr/local/emind/replication_status.sh
```

  - Run the script `replication_status.sh`
    - Execute SQL Query - `show slave status\G;`
    - Parse the output
    - Return data to snmpd

Important to remember

- **Define your goals, What's right for you ?**
  - Don't over monitor
  - Use methodologies and technologies that fit your network and needs, not the other way around.
- **Build generic interfaces**
  - SNMP
  - Simple command line
  - No proprietary protocols
  - Agnostic to the monitoring tool

Mobile Access



Emind Systems
empowering internet technologies

Leading tools – Open source first…

- **Nagios**
  - Very generic, lot's of public plug-ins
  - Easy to tweak and build it at your own style
- **Zabix**
  - A complete monitoring solution
  - Less customizable
- **Cacti**
  - Graphing (RRD tool)
  - Easy to configure
  - Lot's of public templates

Monitoring on the Cloud

- **Nagios + Dynamic Configuration = Dynagios !**
- **Key features**
  - Auto provisioning
  - Add, Remove, Suspend, Unsuspended
- **Machines are monitored base on their predefined profiles**
- **Machines can join / leave the monitor (purposely)**
  - Join on boot
  - Leave on shutdown
  - If crash happens alert will raise

Commercial tools

Feature	ManageEngine	Orion
OS Requirements	Windows & Linux	Windows
Modular (applications, IP SLA, Netflow, Conf.)	Yes	Yes
Very easy to deploy	Yes	Yes
Multi vendor with lot's of templates	Yes	Yes
Maps	Yes	Yes
Less customizable … but still flexible	Yes	Yes
Est. price for 100 devices	$10k	$15k

Questions?