Problem Analysis

# Intro

The issue with network problems, hardware failures and intrusions is that they can happen at essentially any time. There is nothing stopping an air conditioner from failing at 3am when everybody is happily in bed, just as much as there is nothing stopping a power supply from popping a capacitor when all the best electrical engineers in the world are standing right next to it. This boils down to informing the right people of the problem and having it dealt with as soon as possible.

There are many ways to mitigate various issues, such as failing over to a different system or, if the system is non-essential, simply shutting it down until a technician can deal with it, but in many cases an issue will require the near-immediate attention or decision of a technician.

For example, if an under-sea routing connection between the United Kingdom and Iceland was cut or otherwise damaged, where would data be redirected to? It is possible that a technician would have to make a split-second decision to redirect connections going to Iceland to instead go via France, then Denmark and finally to Iceland. Instead, they could choose to redirect from the United Kingdom to the United States, then Greenland and finally to Iceland.

This example only works if the technician was made aware of the issue. If alerting systems did not exist, or were sub-par and required constant supervision, it could go hours or even days before a flaw in a system was noticed. A single line in a log file thousands of kilobytes large just isn’t the kind of warning system needed for large operations with important infrastructure.

For this analysis we will be assuming a medium size business of 200 or so people, their own in-house server room and two dedicated server technicians who work in the office from 9-5. They have a pretty common setup, with networked environmental sensors which can set off alerts in the case of high temperature or humidity issues in their server room. Unfortunately, cheaper environmental sensors have only one method of informing out-of-office, or otherwise engaged technicians: Email.

Email has issues. It can be slow, unreliable, unwieldy, can be hard to configure correctly and is generally not a fantastic tool for urgent reports of problems. In the case that it suddenly starts rising by tens of degrees in the server room, automated systems may not be able to deal with this before morning. The technicians need to be informed immediately, and just like our single line in a log file, a single email in a technicians already-clogged inbox will not wake them from their slumber. They need to be given a choice immediately, do they start shutting down non-essential systems until somebody can get on site to try and cool down the room? Do they leave it, knowing somebody can be there to turn on the back-up air conditioner in five minutes? Once given a choice, the technician needs to be able to choose one immediately based on the information they have been provided, assuming they have even seen the information and the servers haven’t already hit thermal cutoff points by the time they get in at 9am.

Technicians need a proper urgent alerts system, with real choices that can take affect immediately, regardless of any slow mail servers or struggling to VPN in to access crucial control panels on overheating servers. If not environmental problems, technicians need to know about potential security issues, and be able to query data about their firewall and resource usages on servers on the fly on a platform capable of running anywhere – Weather it be on a large screen in the office, a mobile on the go, or a laptop at home.

# Existing Tools

Talking about existing tools could be a problem as I haven’t researched many – My last 4 reviews should be about information systems

{{Table comparing tools}

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Nagios |  |  |
| Webmin |  |  |
| RSAT |  |  |
| Icinga (Has a cool rest API) |  |  |
| OpenNMS |  |  |

{{Table comparing sub-tools, tools that the tools use to report stuff}}

|  |  |
| --- | --- |
|  |  |
| E-Mail |  |
| SMS |  |
| Phone Call (Automated) |  |
| Web page |  |
| Log files |  |
| Instant Message |  |

{{Response types? – How can you remotely deal with issues once being informed}}

|  |  |
| --- | --- |
| VPN |  |
| Remote desktop |  |
|  |  |
|  |  |
|  |  |

{{Some theoretical stuff based on my lit reviews}}

{{Specific weaknesses from tables}}

{{List/identify weaknesses I’d like to address}}