If we knew everything about everything in our technical environments, we could provide our customers with the perfect experience. However, not only is this goal impossible in practice, it is also theoretically impossible. We have not only the opportunity but the obligation to make choices in designing the monitoring and management of our technical environments. In order to deliver our customers the best possible experience, we need to understand their requirements, and use this as the basis for making such informed choices.

This is true for all information technology projects: the heart of project management is the balance between the three competing needs of cost, time and functionality. But in the Internet world the need to make choices is even clearer. The Internet itself is based on a choice that makes it different to traditional telephony. A telephone call will be connected, or not. The service will be available, or busy. The Internet’s core design, however, takes a different approach. Even the most limited or tenuous connection will allow small amounts of information to flow. That can play havoc with a video or voice message, or may be fully sufficient for non-time-critical applications such as e-mail.

Few areas require more choices than performance monitoring, and this applies to web portals as much as other services and applications. No provider wants a technology issue to impact their customers. Given the sophistication (and cost) of modern systems, it seems that nothing should. The promise is simple using modern monitoring tools. Several vendors now promise that businesses can view one or more dashboards that show the state of a service, warning of any current or potential customer impacts, and allowing immediate issue identification and resolution.

Unfortunately, as with many areas in technology, the reality is far more complex. Choices are not only available, but forced onto application owners who expect to know everything about everything. In the next few paragraphs I will spell out a range of choices which I have personally faced in technology service management. This is not a complete list, but gives a reason for pondering before expecting a monitoring miracle.

The first group of choices relates to what gets monitored.

- Synthetic transactions or user monitoring: There are two quite distinct ways of
measuring the customer experience of a service or application. The first of these involves tracking the traffic of one or many users. A particular transaction may be identified and then timed as it goes through a system. If the technical and non-technical problems of tagging individual users can be addressed, there is still a significant weakness in this approach: Service failures often occur overnight due to changes, batch processes and other events outside of regular working hours. The use of transaction monitoring cannot determine if a service is working until customers attempt to use the service, which may not occur until the start of a business day, several hours after an incident has crippled a service. A second and quite different approach is to execute “synthetic”, or artificial, transactions. By measuring the response time to service requests, the application is able to determine delays in various parts of the service and the wider network that will impact customers. A significant challenge to the synthetic transactions approach is security. The system initiating the synthetic transaction will require all accesses required by a real user, and for value transactions the system will therefore need to be appropriately secured. Yet to be effective the system will need to initiate the transactions from areas outside of the central protected IT environment: Just because the synthetic transaction generated within your computer center gets a great response, this says little for a struggling client several thousand kilometers away.

- All access paths or common access paths: Closely related to the previous point is the balance between understanding what a typical user may be experiencing, and understanding what every user is experiencing. For an on-line service, the latter would require direct monitoring of every packet exchanged with every single user. This is because of the nature of the Internet’s protocol, TCP/IP. There are no permanent paths used by users: they can change packet by packet (or many times a second). For a service provider in the real world this would be impossible. Increasing the number of access points and paths also rapidly increases the application’s cost.
- Complete data or longitudinal data: Gigabit routers have existed for many years. The thought of storing all data going through a device which counts its traffic in billions of items per second for anything longer that a few minutes is difficult to imagine. Yet many business managers like to think that they can keep an exact record of everything (not just key transactions) indefinitely. Determining the right level of abstraction in storing information is key to effective problem resolution.
- Automated actions or determinate actions: For over a decade it has been feasible to manage network configuration by allowing service management software to roam a network, interrogating devices and providing either their details or maps based on these details to network managers. This can achieve huge time savings, and provide a level of detail otherwise difficult to attain. Yet allowing software to roam a network searching for devices, and possibly even making decisions about these devices (for example, preparing reports on their status and validity) is a step towards the creation of a non-deterministic network, where the outcome of an action will not necessarily be known in advance. Regardless of the additional delay, effort and difficulty, an organisation which places significant dependence on its networks (such as a bank) may prefer to be able to track the responsibility for every configuration and reporting decision to a specific person, time and place. Automation would then be limited to software that compares on the one hand what and where all devices are supposed to be, and on the other hand, all devices that participate in a network.
Another set of choices relates to reporting. Possible reports include among others:

- A record in an incident management system: This could include a unique identifier, a time-stamp, an author, a title, a short description, a long description, attached information, a log, a set of events, a link to other records, a set of proposed actions, a history of actual actions, text descriptions, numerical descriptions, and many other fields.

- An alert regarding an incident: This could be a brief message listing a subset of the incident record sufficient to provide a simple understanding of the alert. It could be character limited, for example to fit into an SMS message. It will often be a dense and cryptic reference, meaningful only to a particular specialist.

- A brief summary of such a record or alert: While key staff are working with alerts to identify and resolve an incident, information about the incident will also be sought for escalation or communication purposes. Here again brevity is important, but a cryptic message will be of limited value.

- A detailed log: While the primary purpose of incident management is the rapid recovery of a service, for root cause analysis and problem management large volumes of data may be captured.

- A summary in a daily or monthly incident report: Grouping together the various incidents occurring in a large information technology environment is necessary for reporting and tracking of key indicators, which may feed into service level reporting, key performance indicators, reporting dashboards, and other management tools.

The purpose of the report will determine what should be reported. In practice there are at least four different stakeholder groups with quite distinct information requirements:

- The operational view: Providing a reliable and continuous service is an operational task. There may be one or more operational centres around the globe providing 24-hour support, or just a single staff member in a small company with responsibility to keep a service running during business hours. Their task is to get the service back up. They will use the standard tools available to them to rerun batch jobs, transfer to disaster recovery environments, restart processes, and call on the next line of support. They need information to do their own jobs, and if this isn’t enough, they also need to be able to identify which of many in-house or external technology support teams they should turn to. They are interested in processes and options available to them, and the alerts or reports they receive to help them in their tasks will be designed with this in mind.

- The technical view: Fixing a technology incident is a technical task, with several specialties often divided among the relevant teams. In any significant incident it is common for two or more issues to be involved, and several or many technical areas of expertise may be required to rapidly identify (or eliminate) particular paths for investigation. While a programmer, database administrator, data communications engineer or middleware specialist may be fairly confident that a problem is or isn’t their particular responsibility, incident recovery is not an exact process. Common technology errors such as a failed disk drive or power supply may be self-diagnosed. When technology specialists are engaged, the problem is often beyond the commonplace. In these circumstances, unlike in the case of the operational view, it won’t be standardised reports and regular processes that resolve the incident. The report with the most value may be entirely incomprehensible even to technologists in other fields.

- The business view: Here is concern over the specific impact of an incident on customers, with an understanding of which customers are most important, and a desire...
to minimise both overall and high value customer impacts. Knowing which rule corrupted the firewall will be worse than useless, and understanding which team is working on the problem will be of only limited interest. They will be more interested in knowing how long an incident is likely to last. They will be very interested in the names of specific customers or customer segments affected by the incident.

- The assurance view: Finally, the service will often be linked to contractual or regulatory obligations. There may be a limit on the number of minutes a service is unavailable before service level penalties are incurred. These limits may sit within annual or monthly allowances, may relate to the time of day, may vary for different services, and may be bound by internal company guidelines. For service levels the penalty may be purely financial, while for regulatory obligations a significant outage may result in the loss of license to operate at all.

Each of these audiences will have their own requirements for incident notification. For example:

- Message detail: As soon as an incident has occurred, the business view will be interested in the impact on customers. The other views should be aware of the impact order of magnitude, but the technical view will be looking for hardware, system and application alerts that help isolate the problem. These will probably be incomprehensible to the others. Operations will be more interested in management of the recovery, including any temporary workarounds for customers, rather than the specific technical activities.
- Message format: Closely related to the detail of the message is the way it is formatted. An attractive dashboard may provide a valuable business view. (However, unlike a text alert, a dashboard needs to be constantly monitored if it is the primary means of communicating alert status.) A text alert will be much more useful to a technical support staff member, particularly if it is able to identify the specific device, platform or other item having difficulties.
- Message thresholds: In general it is far more valuable for operational and technical staff to receive advance notice of any breaches of thresholds relating to services than for business staff. For example, information that a database has just passed a capacity threshold (such as “80 per cent”) requiring action is of no interest to business staff.
- Impacted groupings: The technical view will focus on all the applications that pass through a particular firewall or server. Server names will be meaningful to them, network diagrams will provide key relationships, and the extent of the incident will be understood in terms of technology. As operations works to resolve an incident, the range of internal impacted groups who need to be engaged or informed will be of major significance. In the business view, the impacted hardware or other technical element will be meaningless, while key focus will be on knowing in advance which customers or customer groupings will be impacted.
- Correlation: In a major incident, there may be many impacted systems and customers. An effective incident management system will group these together and report on impacted groups (e.g., all ATMs in a specific region) rather than provide a separate report for each item that has been impacted. Here again, correlation providing meaningful business information will be quite different to that providing meaningful technical information.
- Drilling down: Sophisticated incident management reporting tools will allow a user to drill down to gain additional information regarding the area of interest. While a technical specialist will be interested that a particular card in a device has
failed, a business concern could focus on which a list of branches in a region have been impacted and for how long.

- Reporting frequency: It is within the capacity of modern technology to provide reports at a rate which will overwhelm human capacity. I am aware of one incident when a faulty device reported its error state 27,000 times in a matter of seconds. While this was an incident in itself, frequency of reports may vary greatly for the same incident depending on the user’s purpose.

For each of these items, the reporting will vary. An implementation which provides alerting or a dashboard in terms meaningful to one group but not the others will fail to meet actual needs. Understanding the different views, and who needs to know what sort of information, is critical to having a meaningful set of messages.

- Loss of service or degraded service: Finally, there is one significant decision which applies to every point made above. Are we concerned just with loss of service, or also with degraded service? Degraded service can refer to delays affecting each transaction, or to loss of some but not all elements in a network (such as the ATMs in a particular region). Alerting a company’s CEO to the loss of connection to all retail outlets makes sense, whereas the loss of one ATM out of 1,000 may be a “business as usual” activity. An additional second for delay experienced for every on-line transaction may be a minor irritation, while a 30 second delay would render most web sites unusable. Where it the cross-over point?

These choices are not insurmountable. With a clear understanding of exactly what we want, we can choose a set of deliverables that are both useful and meaningful. Using a framework such as IT Infrastructure Library (ITIL) to help us understand our service goals and develop our service definitions, we can substantially improve the customer experience. Modern monitoring tools let us get the data we want, once we understand what that data is and how we will use it. Choices don’t have to be a plague, but we do have to make them, if we are to genuinely help the customer.

Greg Adamson
Co-Editor-in-Chief
IJWP