

New Job

At management school I was given the following advice "When you arrive at a new job you get fired for what you do, not what you don't".

It is also sound advice for systems administrators. Making sweeping changes to existing systems, and breaking them, certainly will get you noticed, but unfortunately not in a positive way. As we all want to earn our wages, the question is what should you do when you take over administration for a new site, and where should you start.

In general I start with the monitoring of services and machines. Monitoring services is important, central to systems administration, and "mostly harmless". If you don't know the system is working, then it might as well not be working; and very likely, some time in the future it won't be. And not until the phone rings with an irate boss or customer at the other end, will you know it is not working. It is very reassuring to both customers and co-workers for you to be able to answer the phone with "we know there is a problem", - and what it is, rather than be taken wholly by surprise.

Monitoring is also "mostly harmless" as, in general, it is not customer facing, and can be fitted in between fire-fighting and learning the systems.

Monitoring is also an excellent orientation to both systems and services; it forces the administrator to inventory physical servers, virtual servers, network infrastructure and services and start working out the dependencies between the servers, services and infrastructure.

Finally, done right, monitoring saves you time and makes you appear cleverer than you are. IF you add tests to your monitoring system for the faults you encounter, then the next time the fault occurs you can save diagnostic effort which is often in short supply at 2AM in the morning.

When starting out at a new site you are likely to encounter 3 situations: well maintained monitoring, monitoring in disrepair and nothing.

If you encounter working, well maintained monitoring that describes the relationships between infrastructure and services then you have effectively been given living documentation of the site, and what the previous administrator thought was important. Study it, maintain it and it will look after you.

Monitoring in disrepair will still give you hints about the history of the organisation, and provide some insight into the infrastructure.

A site with nothing represents a chance to do the job right. Create a living description of the systems, services and infrastructure present in the organisation. Furthermore, mapping dependencies helps make you aware of what happens in failures and prepares you for future fire fighting.

When choosing a monitoring system it is important to identify what the monitoring system is to be used for and how it will be used.

In general, I separate monitoring into 2 classes: monitoring you use for optimisation (monitoring for performance), and monitoring to alert you to disaster (monitoring for function).

Monitoring for performance is useful for predicting failure and improving service delivery. It is generally information-rich and may not reveal much at a glance.

Monitoring for function essentially tests if a service is working acceptably eg a web page returns within 10 seconds might be acceptable and one that takes 2 minutes is not.

In a crisis, information flow is critical to reacting well to the situation. Information can be pushed - sent to the responder (eg emailed or smsed) or pulled - the responder seeks out information (eg goes to a web site). It is quite easy to overwhelm a responder by pushing too much information on to them. It is, however, essential to allow the responder to seek out any information they might require.

When choosing a monitoring system for use in responding to a crisis, it is vital that the monitoring limits the amount of information it forces on the user. Dependencies between services are critical to limiting information flow. A simple example of a dependency is a web site running on a server. If the server is down, then the web site will fail. In a crisis caused by a failing router, receiving messages about each failed web site and server could easily distract the administrator from the important information that the router has failed.

During day to day operations, the detailed information, provided by performance monitoring comes to the forefront. This information could include load averages, IO delays, network round trip times and throughput. This type of information is useful in identifying hot spots, and allowing reconfiguration of workloads to optimize performance.

At the end of the day, working on monitoring is far from doing nothing; on the contrary, it is a critical performance multiplier for system administrator.

By Maurice Castro