What is IT Infrastructure Monitoring?

IT infrastructure monitoring is the deployment of a built-in knowledge base to automatically diagnose performance and availability problems across the technology stack before productivity compromised. Full-stack IT Infrastructure monitoring includes:

- Hardware – Physical Health
- Operating System – Utilization and depletion
- Network – Bandwidth consumption and errors
- Application – Performance and availability

Because IT Infrastructures are often comprised of multiple locations that encompass both private, public, and hybrid cloud deployments, the challenge IT faces is how to quickly identify and correlate problems before they affect end-users and ultimately the productivity of the organization.

IT Infrastructure monitoring becomes more complex as IT infrastructures become both denser and dispersed. Significantly larger quantities of server data and the need to analyze that data *quickly* can only be accomplished with automation. This allows IT personnel to spend their limited resources on advancing high value initiatives rather than chasing down avoidable server issues.

Learn the Best Practices for implementing automated server monitoring across large scale, diverse IT infrastructures.

Download the whitepaper:
Best Practices for Server Monitoring

IT Infrastructure Monitoring Design

Longitude is constructed to be lightweight and quick to administer. An agentless architecture means the discovery and monitoring of your technology stack is speedy and non-intrusive. In addition to the simple Web interface, an easily mastered command line interface allows user to rapidly embed Longitude into existing automation or to create their own with scripts. Keeping Longitude *low touch* means IT can focus their efforts on the most pressing issues.

The following outline is a list of items to take into account when implementing an IT Infrastructure monitoring system:

What should you monitor?

- Hardware – IBM Director, Insight Manager, and OpenManage
- Operating Systems – Windows, Unix, and Linux
- Virtualization – VMware and Hyper-V
- Network – SNMP enabled devices
- Applications – Database, Messaging, and Web

What constitutes a problem?

- Hardware errors
- Poor provisioning of Windows and *Nix resources (CPU, Memory, Storage, IO Capacity)
- Misallocation of virtual resources (Hosts, Virtual Machines, Network, Storage)
- Excessive network utilization and error rates
- Application problems as identified by built-in knowledge base

What should you do when a problem is identified?

- Automate an OS command or script to fix the problem if possible
- Prioritize and escalate high severity alerts with text messages or email alerts
- Dashboard performance / availability based on user-definable criteria

What kind of reporting should be in place?

- Analytics – Performance trends and patterns
- Capacity Planning – Rightsizing of IT Infrastructure
- Service Level Agreement – Baseline behavior and identify IT Infrastructure components that deviate from the norm
- Problems – show alert history

Next Steps...

Contact
Privacy Policy
FAQs
Support