

LogicMonitor
ARCHITECTURE WHITE PAPER



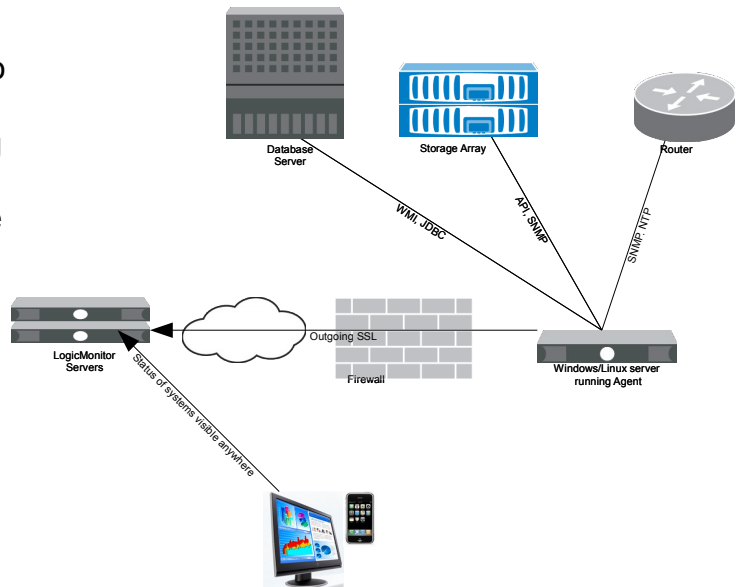
*Examining the architecture of a
“Software as a Service” monitoring system.*

Today, comprehensive, reliable and accessible monitoring of web services infrastructure and internal I.T. systems is no longer a luxury – it has become a business necessity. Whether to meet internal I.T. SLA's, or to identify performance, scalability or hardware problems before they impact customers, comprehensive monitoring and trending has been proven essential. However, given the tight staffing levels of many I.T. environments, they are often scrambling to meet immediate demands, and implementing and maintaining monitoring systems is often low on the priority list. This state often persists until a service affecting outage occurs, which monitoring could have prevented. LogicMonitor's unique hosted solution provides an easy and scalable way for enterprises to be up and running with effective monitoring and trending with a minimal investment of time and no hardware resources required, and its ongoing device attribute discovery ensures your monitoring stays up to date, even in the face of frequent changes.

How it Works

The LogicMonitor system is composed to 3 functional components:

- The LogicMonitor service, running on highly available machines in secured datacenters, provides the user interface, configuration management, and all the back end processing and storage.
- The agent or agents, running on systems inside the enterprise's firewalls.
- The monitored systems.



Configuration Management

All configuration and administration takes place via an authenticated web browser session, from any Internet connected computer. Configuration consists of defining hosts to be monitored, what to monitor on them, the appropriate alerts and thresholds, and the escalation lists for who to contact in the event of an alert. With device discovery, and extensive best practices datasources defined, however, most LogicMonitor users find that little configuration is necessary other than adding hosts and defining alert escalation destinations.

The LogicMonitor service will create the appropriate configuration for the agents based on the configuration done through the web user interface.

Agents

Agents are deployed inside the enterprise's datacenters. They may be deployed on a dedicated machine, or on a server currently in use. The only requirement is that the agent be able to make an outgoing SSL connection on port 443 to the

LogicMonitor service on the Internet, and be able to monitor the systems assigned to it. (The monitoring may occur over snmp, http, icmp, WMI, JDBC, etc, so the appropriate protocol must be permitted between the agent and the targets.) Because of this, no firewall modifications are needed at most deployments, regardless of the current firewall, NAT or proxy policies.

The agent connects to the LogicMonitor service over SSL in order to pull down its configuration of what systems to monitor, and how; to check for updates; and to post back the data it has collected. Agents also perform ActiveDiscovery on a regular basis – reporting back to the service when a new volume is added to a storage system, for example.

The agent itself is very lightweight in terms of CPU and memory usage.¹ A dedicated agent can easily scale to monitor thousands of systems, depending on the kind and frequency of monitoring desired (some data collection methods, such as applying complicated regular expressions to parse JDBC or HTML output, consume more CPU per datum.)

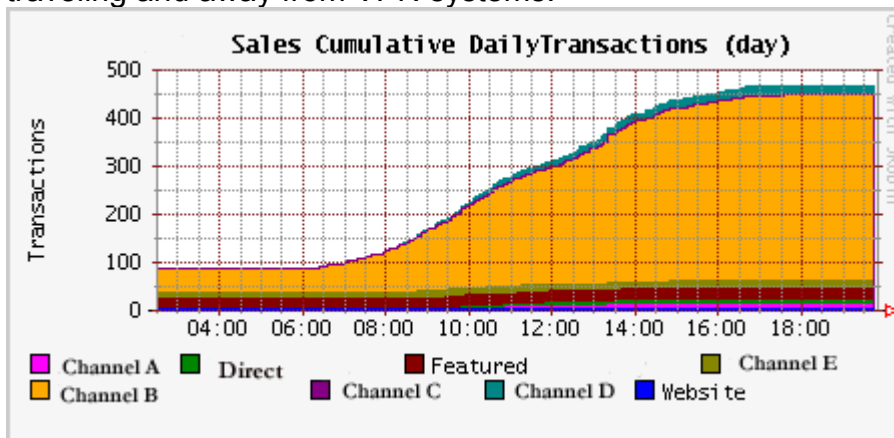
Multiple agents may be deployed, either to scale data collection, or for internal firewall policies. (For example, if no traffic is permitted into the corporate finance network, a separate agent can be installed on one of the existing machines on that subnet, while another agent collects data from non-finance machines.)

In the event of a network issue between the agents and the LogicMonitor service, the central service will escalate an alert that the agent has not reported back, but the agents will continue collecting data and buffering it locally. In this way, the trending data will be complete once the network connectivity is restored.

Monitoring and Trending

All alert status, reports, monitoring and trending is securely visible from any web browser after a user has been authenticated appropriately. This eliminates any problems with accessibility of monitoring information when staff is off site or after hours, but still has to respond to alerts.

It also allows business managers to keep current on graphed metrics, even when traveling and away from VPN systems.



¹ For example, in one deployment, one agent is collecting 32,000 datapoints per minute, using about 30% CPU of a single 1.6 Ghz core.

Alerts are sent directly from the highly available central service via email or SMS, and soon, direct to phone via text to speech and IVR technologies.

Security

LogicMonitor uses standard web based security protocols. All data to or from agents and users is encrypted with 128 bit SSL encryption. The agents have no listening sockets, and only make outgoing network connections. The agents authenticate both themselves and the central server to ensure your data stays private.

Enterprises have full control over administering user access to their service, creating and revoking users with different privilege levels.

Conclusion

LogicMonitor provides enterprises with a scalable, simple to deploy monitoring, alerting and trending system, with great flexibility and customization capabilities. It's unique Software as a Service model delivers these capabilities with no hardware requirements, no systems administration overhead, high availability, and no changes required to the existing infrastructure.

For more information, or for a free trial, go to <http://www.logicmonitor.com/>