

Monitoring Systems Comparison

June 14, 2007

By Scott Stone, scott@theforbingroup.com

© 2007 The Forbin Group, Inc.



TABLE OF CONTENTS

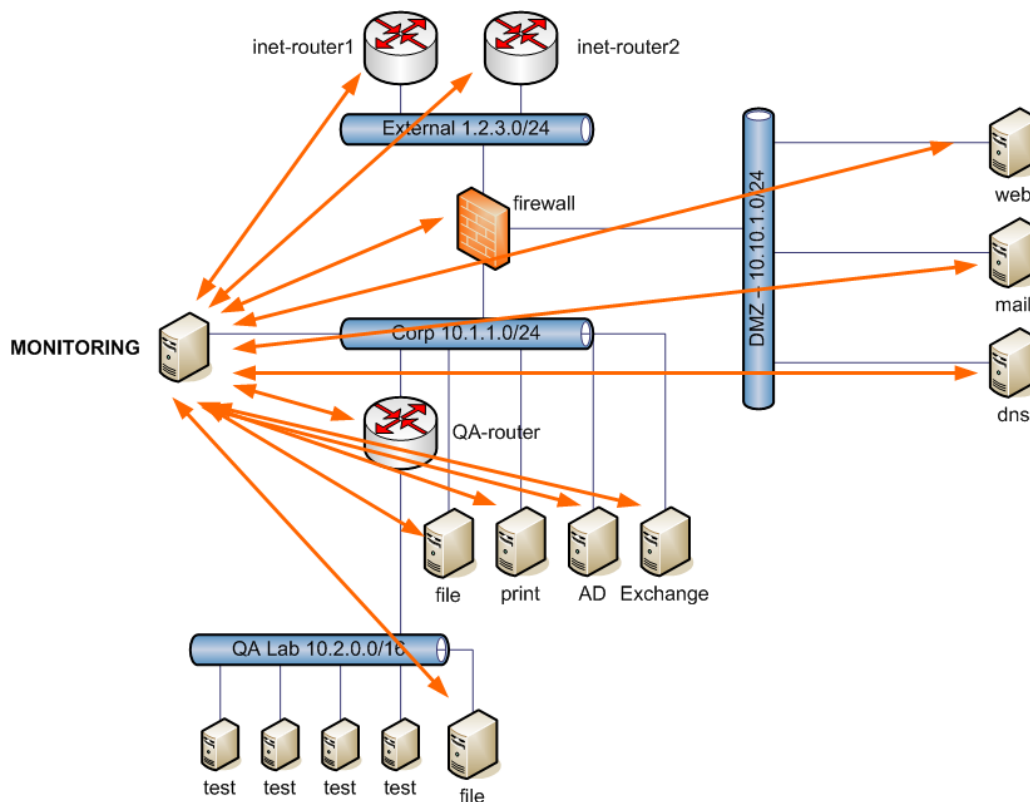
| | | |
|----------|---|----------|
| 1 | MONITORING SYSTEMS COMPARISON..... | 3 |
| 1.1 | BACKGROUND..... | 3 |
| 1.2 | MONITORING SYSTEM CORE FEATURES..... | 4 |
| 1.3 | INSTALLATION AND DEPLOYMENT..... | 6 |
| 1.4 | OPERATING SYSTEM AND PLATFORM SUPPORT | 7 |
| 1.5 | EXTENSIBILITY | 7 |
| 1.6 | DOCUMENTATION | 8 |
| 1.7 | PRICING AND SUPPORT..... | 8 |
| 1.8 | CONCLUSION..... | 9 |

1 Monitoring Systems Comparison

There are many network and systems monitoring solutions on the market today, both free/open-source and commercial. This white paper describes the differences between three of them – Hyperic, Lithium, and Zabbix. Interestingly enough, all three of these have similar “hybrid” licensing models, making them usable both on a free basis and on a commercial/supported basis, depending upon the user’s preference.

1.1 Background

The goal of any network monitoring system is to provide a centralized view of the network and systems so that systems administrators can analyze conditions and prevent/fix problems quickly and efficiently. Generally a separate system is set up to host the monitoring system and is placed in a centrally-located point on the network. Sometimes more than one system is used, in a “distributed cluster” architecture, allowing more than one monitor host to exist but presenting a centralized view of the entire network. A typical installation of a network monitoring system might look like the following:



All three of the monitoring systems compared in this document would be installed in a similar fashion, with one or more centrally located monitoring servers responsible for checking on many servers and network devices. For monitoring the servers, either SNMP (Simple Network Management Protocol) or a proprietary management protocol would be used. For monitoring network devices, typically only SNMP would be utilized.

It is important to note that the firewall and routers depicted above would need to be configured to allow both SNMP traffic and the traffic types used by any proprietary protocols, or the monitoring system will not be able to communicate with the devices and hosts to be monitored. The specific firewall configuration tasks vary depending on which of the three products is chosen, as some of them use proprietary protocols and would require non-standard ports to be opened. All three utilize SNMP, however, so UDP (Universal Datagram Protocol) port 161 would generally always be required, as would port 162 (for SNMP traps).

1.2 Monitoring System Core Features

While all three of these monitoring systems fill essentially the same niche in an enterprise's IT environment, there are several key differences between them in terms of their feature sets.

Hyperic focuses heavily on monitoring application performance. It ships with plug-ins designed to monitor most common applications' performance parameters. Everything from mail servers to web servers to database servers is covered. These applications include, but are not necessarily limited to:

- Apache
- Microsoft IIS
- SunONE Web Server
- WebLogic
- WebSphere
- JBoss
- Geronimo
- Cold Fusion
- JRun
- Microsoft .NET Runtime
- Silverstream
- Tomcat
- Resin
- IBM DB2
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Oracle
- Sybase
- ActiveMQ
- IBM MQ Series
- Microsoft Exchange



- Microsoft Active Directory
- VMWare
- Citrix Metaframe
- LAMP
- LAM-J
- J2EE
- MX4J
- FTP
- SSH
- Sendmail
- Postfix

Best of all, the Hyperic agent will auto-detect the presence of these applications and automatically configure the monitoring parameters for them, based upon reasonable defaults. The administrator can then modify these parameters at will. Hyperic's auto-discovery features are also very well-developed – to deploy Hyperic, one only has to install the console/server software on the management node and then deploy the agents to the nodes to be managed. The code inside the agents will do the proper auto-discovery and automatically register with the server. The only administrator intervention required is when fine-tuning is needed, or when a generic SNMP device needs to be monitored. Neither of these tasks is particularly difficult, given Hyperic's responsive and well-designed web-based user interface. Unlike many Java-based user interfaces, Hyperic's interface is very responsive and does not feel slow or cumbersome. The interface is attractive and is presented as a high-level "dashboard" view when it is first accessed, with the ability to "drill down" to a very fine level of detail if desired. Since it is web-based, all of the interface's features are accessible from any system with a graphical web browser. Systems and services are organized into groups automatically, making it easy to find what the wanted information easily. The graphs of performance data are easy to read and presented in an intuitive fashion, with proper legends and keys provided to interpret the data. "Policy-driven" alerting, log-file monitoring, and configuration change management features are also available in Hyperic when the "Enterprise" edition is purchased. No pre-made reports can be directly generated by this product, but if the information provided by the user interface is insufficient, then the back-end SQL database could be directly queried by a report-generating engine.

Lithium is a simple hardware (host and network device) health and performance monitoring solution utilizing SNMP. It does not have any application monitoring capabilities. It is exclusively an SNMP-based device monitoring solution, and does not cover the same scope as Hyperic does. Lithium comes with several pre-built SNMP profiles for monitoring common network hardware such as Cisco™ routers, Cisco™ switches, Foundry™ switches, Cisco™ PIX™ firewalls, and a few other commonly-used devices. It has two separate user interfaces – one is web based, and the other is a native-OS solution which has more features and is more graphically pleasing. Of the three solutions, Lithium is probably the sparsest in terms of features, since it attempts to be a more "generic" monitoring system that can be used with any

device capable of reporting statistics via SNMP. Lithium has several pre-made reports which can be generated and run, including a 95th-percentile bandwidth usage report. No log-file monitoring or configuration tracking features are offered with this product. Although it has a “free” version, the lion’s share of advanced features (such as being able to communicate with a non-generic SNMP entity) are only available if you purchase the product at a cost of \$198 USD (25 entities) or \$839 USD (unlimited entities).

Zabbix is another good example of quality network monitoring software, although it too does not seem to go as far as Hyperic does with regards to application service monitoring. It is somewhat of a hybrid of the two solutions above in terms of features - It bases its checks on both SNMP and an operating-system-specific “agent”, and can do port-level monitoring of several applications, but does not have a full set of deep application inspection checks like Hyperic does. Auto-Discovery is planned for 1.4, although 1.3 is the current "Beta" version, so 1.4 may not be released for some time. One of the nicest features about Zabbix is its graphing and charting capability. It can create a dependency-based network map showing the physical and logical locations of network assets, and the performance output graphs are clear, concise, and easy to read. Zabbix’ user interface is completely web-based, making all of its features accessible from anywhere. Log-file monitoring and configuration tracking are supported features of this product. Reporting features are similar to Hyperic’s – the user interface provides a lot of information but no pre-made reports. The back-end SQL database could be similarly queried by a reporting engine, however.

1.3 Installation and Deployment

Hyperic has a very simple and straightforward installation procedure. Although it requires a JVM (Java Virtual Machine) to run, this is included in the package. The JVM runs separately from any other JVM which may already be installed on the system, making it completely independent and transparent to the other applications already on the system(s) being monitored. Installing Hyperic is simply a matter of running their pre-supplied install script and, in the case of the agent, telling it the IP address or hostname of the monitoring server that it is supposed to report to. Due to Hyperic’s use of Java, its memory footprint is rather large, and start-up time for both the agent and server is non-trivial. Once it is up and running however, CPU usage is fairly minimal and it is friendly to other JVMs that may be running on either the server or client machines (Hyperic installs its own private JVM, which does increase its disk footprint but greatly reduces the risk of JVM incompatibility issues and crashes).

Lithium is distributed as a .tar.gz file containing RPMs. These RPM packages must be installed manually, and only work on RedHat Enterprise Linux versions 4 and 5, or CentOS versions 4 and 5. In addition to installing the RPM packages manually, the administrator must also install Apache, PostgreSQL, and several PHP modules by hand. After these packages have been installed, there are several more commands that need to be run to create the initial database and configure the PostgreSQL access controls. All of this is reasonably well-documented, with the exception of the access control modifications for PostgreSQL. Once all of this has been completed, you can begin using the web or “Console” interface to configure entities to be monitored. Lithium is written in native, compiled code for either Linux or MacOSX and therefore has a low memory and CPU usage footprint. It starts up quickly and responds near-

instantly to interface requests, even when the server is running on a VMWare™ Server VM (the free version of VMWare). There were no implementation flaws or bugs noticed during testing, and performance remained good throughout all of the usage that the product received.

Zabbix posed some unfortunate technical barriers to installation. There were several incongruities between the installation instructions and reality, both in the steps to be followed and the installation pre-requisites. This is not an installation that can be performed by a novice. This is a process that will prove challenging even to very experienced senior-level systems administrators.

1.4 Operating System and Platform Support

Hyperic supports Linux (any system capable of running a JVM – it is not picky about any one particular Linux distribution over another), Solaris, HP/UX, and Windows for both its server application and its agents. Since Hyperic’s interface is completely web-based, there are no operating system restrictions for accessing it.

Lithium runs on Linux (RHEL4, RHEL5, CentOS4, or CentOS5 only) and MacOSX. Its native user interface can run either on Microsoft™ Windows™ or Apple™ Mac OSX. Since all of Lithium’s checks are SNMP based, it can monitor any platform which is running an SNMP agent. Unfortunately, this means that the monitoring is only as strong as the quality of the SNMP agent running on the host. The systems I was using as test nodes were running an apparently-buggy build of net-snmpd for Linux, in which all of the “tun” interfaces and one of the Ethernet interfaces were continually reported as “operational status: down”. This was not Lithium’s fault, as a basic “snmpwalk” yielded the same information, but Lithium is completely at the mercy of misconfigured or improperly compiled SNMP agents. The web interface can be accessed from any platform, but the web interface is not as feature-rich as the native user interface.

Zabbix runs on Linux, FreeBSD, Mac OSX, Solaris, SCO UNIX, HP/UX, and AIX. It has no Windows agent, but can still monitor Windows hosts through SNMP. Since its user interface is web-based, there are no operating system restrictions for accessing it.

1.5 Extensibility

Hyperic has a comprehensive plug-in development kit (PDK). It requires knowledge of Java, but allows a developer to create a very well-integrated monitoring plug-in for an application package which is not already supported by Hyperic already.

Lithium has some plug-ins available, but are only created by the vendor. There does not appear to be any way for an end-user to extend the functionality in the same way as with the other systems. The free version does not appear to be extensible at all.

Zabbix will allow for the creation of UNIX shell scripts that can be run as external monitors from within the software.

1.6 Documentation

Hyperic does not have very comprehensive documentation. The vendor-supplied documentation is sparse and not intuitively organized. There are community forums for help, however, as is common with many open-source products.

Lithium has recently re-done their website, and documentation is now provided on the site. The installation guide is mostly helpful, although it does assume an intermediate-or-better knowledge of PostgreSQL configuration as well as an advanced-beginner-or-better knowledge of RPM package management in order to follow along. The user guide is peppered with helpful screenshots, although not all of them matched what the software was displaying on our test systems (they were reasonably close, however).

Zabbix has fairly comprehensive documentation included on its website. The product appears to require significant degrees of manual edits to files - which are documented here. However, as was mentioned in the “installation” portion of this document, above, a lot of this information is incorrect. Zabbix’ documentation efforts are, however, more complete than those of the other two products in this comparison.

1.7 Pricing and Support

All three of these products can be used legally for free, and all three of these products have a “payware” version with extra features, available technical support, or both.

Hyperic can be used completely free of charge, with no restrictions. Purchasing the enterprise version gives you log-file analysis, policy-driven reporting, and configuration management features which are not available in the free version, and purchasing the product also entitles you to support. There is also a less expensive option which includes support but no extra features. No pricing numbers were available on the website. The website instructs a potential customer to call for pricing.

Lithium has a more restrictive pricing model. The 10-node version can be used free of charge, but if you wish to monitor more than 10 devices, you must purchase a license. Additionally, only the purchased version supports platform-dependent SNMP monitoring – the free version only allows for talking to a device as a “generic SNMP device”. This is useful if all you wish to do is monitor general availability and interface bandwidth consumed, but not if you wish to do any “deeper” systems checks. A 25-node license will cost \$198, and an unlimited-node license sells for \$839. Support is included when you purchase either the 25-node or unlimited-node license.

Zabbix is similar to Hyperic in that it can be used completely without charge and without restriction. The Zabbix website claims that commercial support packages start at \$495. Apart from the support itself, there are no extra features to be gained by purchasing a support package.

1.8 Conclusion

In conclusion, while all three of these products have their relative strengths and weaknesses, it is the author's opinion that Hyperic is the most complete and useful solution to the problem of network and systems monitoring. Its ability to monitor applications, its auto-discovery capabilities, and its extensible framework make it the most robust and usable product out of the three evaluated here. If a customer opts for the "enterprise" version, they get even more features and functionality in addition to the support package, making it an even more attractive proposition.