

Out-Of-Band Management in the Enterprise

Darel Stokes

Abstract: Out of Band management in the Enterprise has changed from emergency access to serial ports for use when first line management systems and connectivity fail. This technology is now an integral part of any serious attempt to manage the enterprise and offers significant new capability to any management infrastructure. In and Out of Band management systems now stand side-by-side in the infrastructure to guarantee that the corporate assets are always in place to ensure that the enterprise is ready to compete at any level.

Out of Band Management in the Enterprise

What is Out of Band Management?

Out-of-band management is generally defined as a management scheme that does not use the same communication path to communicate between the managing device and the managed elements. Out-of-band management utilizes a serial communication cable attached to the RS-232 console port of a managed device. This connection may require a modem if the distance between the managed devices and the management host is more than a few hundred feet.

In recent years, the definition of Out-of-band management has been extended to include serial console servers, attached to managed-device consoles via RS-232 ports, which provide network access to the consoles of said devices. The serial console servers are often served to more sophisticated software systems that provide functionality such as real-time monitoring, access, and device-learning capabilities.

Finally, with the advent of self-healing networks, out-of-band management can now be thought of as hardware/software solutions that collect information from the monitored systems passively instead of invading the host environment with active components. This information is then passed, through console-servers, to sophisticated monitoring systems that:

- present alerts and visual indicators that an event has occurred,
- collect the information into persistent data stores for further processing,

- have the capability of automatically handling many of the most common failure events,
- provide reporting and analysis capabilities on collected data,
- provide a persistent log of all interactive activity that has occurred on a console.

Benefits of Out of Band Management

No Additional Load on the Monitored System

Effectively monitoring a heavily used network element while overcoming the lack of CPU bandwidth is one of the largest challenges to overcome in the telecommunications industry. Often, a network element's control processor is overwhelmed with requests for monitoring, updating the current configuration, and logging events to a local disk, while is asked for current status by an external command and monitoring package. These software packages are often built in-house and they integrate with components of a vendor-supplied product for communication to whatever external products interface to the enterprise infrastructure.

These challenges often force network designers to implement "change windows" that allow for a finite number of commands to be piped down to the network elements, so that they can be handled properly. This constraint costs the industry valuable time each year because of:

- the finite time window allowed for changes to the network

limiting the number of commands that can be pipelined to each network element,

- the cascade effect on other network elements that depend on, or are aware of, the network element being changed,
- failures in command execution due to errant command construction or topology inconsistencies.

Feature-rich out-of-band management systems, such as ConsoleWorks, can help immensely in this type of environment, without adding detrimental load requirements on the monitored elements. The out-of-band management port of the network element can be connected to a console server. This server is monitored by a system that can learn the load environment of the product and also allow for more flexible update of the configuration.

Event Definition and Detection

An event, for the purpose of this discussion, is defined as a group of characters presented by an application, operating system, BIOS (Basic Input/Output System), hardware component, or environmental monitoring device that is hosted on, or has access to the monitored system. These character groups normally represent activities or circumstances occurring on the system that are of interest to the system administrators, operators, and network support personnel. For example, a system administrator might want to catch the occurrence of an event that includes the string *“system disk 90% full, attempting to continue”* while ignoring a message like *“system clock successfully ticked.”*

An out-of-band monitoring and alerting system, such as ConsoleWorks, uses character recognition techniques including, but not limited to, Regular Expressions, to determine whether the console output of a monitored device contains information that should be recognized as an event. Once an event has been recognized, a series of activities can be configured to occur, such as:

- **Simple logging of the event.** Many events that occur on a system do not need to be acknowledged or acted upon; they simply need to be logged for security or auditing reasons. These events may also be used as input to a billing system such as a “charge per connect” system that might need to count the number of times a user logs onto a system.
- **Alerting an external application of the problem.** External applications may need to perform actions to them in order to successfully respond to a condition that occurs within the system being monitored. Out-of-band management allows the external systems to be alerted without the need for active components to be hosted on the monitored system.
- **Graphically displaying the event.** A monitoring station may need to be alerted to the occurrence of the event, so that human resources can react to the condition that exists. This is useful for messages like, *“there is a fire in the basement.”*
- **Executing a pre-defined action routine that can receive**

intelligence from the actual recognition of the event occurrence. Any number of intelligent algorithmic responses can be coded to deal with messages that can be detected. Take the example above, *“there is a fire in the basement.”* The series of activities could be:

1. Sound an alarm.
2. Alert the fire department.
3. Alert the security department.
4. Turn on the sprinklers in the basement.
5. Close the fire doors.

Secure Access to Monitored Devices

Enterprise architects are increasingly given the task to provide a higher level of security within the corporate network infrastructure when designing command, control and monitoring capabilities that are applied to strategically important assets. Out-of-band management systems meet this challenge by providing secure socket layer (SSL) access from the users’ browser to the management system, as well as secure shell (SSH) access between the management system and the console server(s). These capabilities combine to provide SSL version 2 and 3 protection to the corporate systems allowing only authorized users access. Usernames and passwords are also protected from “sniffing the wire” because the SSL connection is established before the user logs on using his or her access control information.

Immediate Detection of Monitored Events

Most in-band systems rely on polling or trapping techniques to provide status of

an event that has occurred on a monitored device. This technique, while effective, presents a pre-defined delay into the recognition of the event since it has to wait for the pre-configured trap processing or poll interval to elapse before the event is presented to the monitoring system. Out-of-band management systems, relying on character scan techniques, are limited only by the performance of the monitoring software, the electronic capabilities of the console device to relay the information, and the network connectivity between the console servers and the monitoring host. Therefore, it can be said that the only delay presented in an out-of-band solution is the propagation delay presented by the monitored host, the network infrastructure, and the performance of the monitoring system; all of which can be controlled and configured by the system architect.

Capability to Collect Unknown Events and “Learn”

System administrators can discover new events by reviewing the logs of the monitored devices, since all information is logged to a time-stamped log file unique to each device. These character groups can be mined from the log files to create new events. The system scans for these new events when the administrators determine which of the discovered conditions need to be acted upon.

Integration into In-Band Management Infrastructure

In-band management systems, with their own unique man-machine interfaces, are often deployed long before the need for out-of-band management and monitoring requirements are recognized. Replacing

these systems with an out-of-band solution is often prohibitive, simply because of the training involved, the investment in the current solution, and the infrastructure modifications that have been made to integrate the current solution.

These issues do not, however, mitigate the need for out-of-band management, which addresses many of the shortcomings of the currently deployed in-band management infrastructure. Fortunately, out-of-band management systems can be integrated into the in-band infrastructure by simply generating SNMP traps or presenting management information blocks that can be “walked” by an existing SNMP component.

Access to Console When Things Go Terribly Wrong

One of the most powerful capabilities of out-of-band management solutions is the ability to connect to the console of a managed device when everything has gone wrong. A monitored device is in much greater danger of failure with the inability of a successful recovery, if connectivity and communication to it require a minimum functionality of the host operating system.

Out-of-band management only requires that the console device is still responsive, not that the host operating system be in any condition to respond. This fact alone provides a sobering case for out-of-band management: connectivity to the device and a chance of recovery even when the software being hosted on the monitored hardware is partially or fully non-functional.

Collection of Recovery Actions

The actual corrective action steps that were required to bring the failed element back into service are captured in real-time, since the console activity of all monitored elements is stored as it occurs. This capability allows the systems administrator to review the log files and:

- update training materials;
- create automated scripts to recover from such an event;
- review performance the technician who facilitated the recovery; and
- maintain integrity of monitored information even though the host operating system may have ceased to log its own activity.

Action Routines: A New Approach to Automation

“How do I get my operators to recognize the event and act upon it?” is one of the most popular questions asked by infrastructure designers and architects.

Many of the most costly system failures are caused by simple things such as:

- log-file disks filling up;
- memory depletion due to orphaned processes;
- application overload due to insufficient flow-control design in the application;
- unexpected network topology reconfigurations.

These issues can be handled completely, or, in the case of the well-meaning network technician who thought no one was using that router at midnight, they can be alerted upon, and the event can be promptly captured for gentle correction of the offender.

The functionality of action routines is greatly increased when combined with a scheduled event capability. This means that the health of any component, local or remote, can be tested on a predetermined time schedule. If any of these components are found to be inoperable, or unresponsive, events can be generated by the action routines back into management system to alert component failures. This feature greatly enhances the monitoring capability of the out-of-band management system since components can be added almost immediately, without extensive reconfiguration of the management system metadata.

Introduction of Web-Based Out of Band Management

If all of the advantages discussed above are not enough, the most sophisticated out-of-band management tools provide web-based access. This means that the system administrators and operators have access to their management and monitoring capability anywhere they have connectivity and a web browser. Remote connectivity is significantly enhanced with the addition secure communication provided by secure socket layer (SSL) communication between the web server and browser, providing almost hack-proof communication with up to 1024 bit encryption strength. SSL provides the much sought after additional security in the enterprise.

Access to Network Management Throughout the Enterprise

Web based management and monitoring means that the support staff takes their management capability wherever they

go, as long as an intranet-connected, browser-capable client is available to them. This means that the support team will never again have to worry about a management client being successfully installed on a PC or workstation before they can continue their work. If a browser can reach the Network Management Node, the staff can work from home using an internet connection.

No Client Installation Management Headache

Simply mention that you wish to deploy a new client/server application throughout the enterprise and give a desktop support administrator a headache. That is just what your PC support group wants to hear, "We have got one more client application that must be supported, updated, configured, and deployed." Contrast that with the smile that you will elicit when you tell your desktop support team, "All I need is a browser, and it does not matter whether it is Netscape or IE." And imagine the surprise and delight when you tell them that your management tool can receive events from the support Windows desktops and alert the SMS installation that a problem has occurred.

Application Instrumentation via an Application Programmer Interface

Many applications are now distributed over a large number of servers separated by great distances. Each of these application's software components often rely upon the health and behavior of up or down stream components. Many corporations have addressed this issue by implementing workflow systems that cost millions of dollars to purchase, millions more to configure and integrate

into the enterprise, and yet more dollars to maintain.

Out-of-band management systems that present an application programmer interface allow generation of events from applications that may exist on any network element communicating with the monitoring system via TCP/IP. This capability immediately enables monitoring of applications, as well as communication of the current state of the overall process performed in the enterprise. This capability, combined with event action routines, immediately provides a command and control capability that enables seamless control of the corporate data flow, application components, application servers, and the host network elements.

Successful Deployment of Out-of-Band Management Solutions

The most difficult step in selecting an out-of-band management solution for monitoring and control of network and system elements is recognizing the need. System administrators and network architects that have experienced element failures so catastrophic that the host operating system cannot respond do not need convincing. They are the people that have spent seemingly endless hours on the phone to the data center across town, or across the country, trying to find someone to push the magic button in hopes that the system has been configured to restart on power-cycle. Too often they are disappointed to learn that the auto-restart capability configuration is still on the “To do” list.

Recognition of Critical Systems

Systems that absolutely must provide console access to the management

infrastructure must be identified. Their consoles must be connected to console servers, so that the console can be accessed regardless of the state of the host operating systems. It is not a matter of “if” a monitored system will become disabled beyond its ability to respond, but it is a matter of “when” this will happen. Sooner or later, every operating system “wraps itself around its axle,” and can only be recovered via a restart procedure, a power cycle, or commands via a directly connected console.

Identification and Configuration of Significant Events

Once systems consoles have been made accessible to an out-of-band management system, the significant events must be identified and configured. More flexible out-of-band management systems, such as ConsoleWorks, provide prepackaged sets of event definitions that allow the system administrator to start identifying events on monitored systems immediately.

Event handling behavior of the monitoring system can then be tailored to allow for tasks such as, but not limited to, notification of people or other monitoring software that the event has occurred.

Configuration of Event Action Tasks

Once events have been associated with specific systems consoles, and configured properly, action routines may be configured to perform well-known tasks that have been identified by the system administrators. These tasks can be as mundane as moving and/or purging log files or as complicated as adding nodes to an active massively parallel

processing configuration when active nodes reach some percentage of resource utilization.

Event action routines are often used to interface out-of-band management systems into other infrastructure systems including in-band management systems that may need to know what is going on in the enterprise.

Instrumentation of Applications

Existing and planned enterprise applications should be reviewed to determine what processes, notifications, activities, and flow-control components need to be exposed to other applications and management systems. These applications can then be instrumented with the supplied application programmer interface supplied with the out-of-band management system to provide a truly enterprise level integration of all strategic components.

Automatic Reporting Capabilities

Any good management system will allow a large number of versatile and configurable reports to be run against the data received from the monitored systems. This data, while not very useful on a day-to-day basis, presents very interesting and often significant data about system behavior trends in the enterprise. Mining this data with special emphasis on time correlation between monitored systems often presents surprising insights into unexpected positive and negative feedback between network elements. Additionally, reporting can be used to assist in monitoring service level arguments.

Conclusion

Out-of-band management is easily integrated into the enterprise, whether in-band management systems exist or not, giving the enterprise architect a valuable tool to extend the command and control capabilities available to infrastructure operations staff.