August 15, 2002

Monitoring the Physical Environment of Distributed Systems

Jean-Pierre Garbani

Catalyst

A client inquiry

Question

What products are able to monitor the facility environment of unattended distributed systems?

Answer

The aftermath of Sept.11, 2001 has added physical threats to IT infrastructure components to the long list of potential problems faced by an IT operation. Due to their long history, data centers have been very apt at monitoring and controlling their physical environment. Distributed systems, on the other hand, are more resilient to office conditions and are often left unattended and uncontrolled, especially in remote divisions or branches of midsize and large corporations. While the "logical" status of software and hardware is most often monitored remotely at the network operation center (NOC) level, the "physical" environment relies on the building and facility equipment and is usually not monitored constantly.

The typical physical threats to an infrastructure component, whether a networking component, a storage element or a server are of three main categories:

- The immediate facility conditions, including temperature, humidity, presence of water, smoke or fire
- The internal conditions, such as component temperature
- The detection of intrusion in a local office or other room containing mission-critical equipments

Most of the time servers and other components placed in a remote office do not receive all of the attention dedicated to a data center. The cost of using traditional data center equipments to support this type of distributed systems would be prohibitive and not in line with the value of the equipment so protected.

Several products can monitor these unattended infrastructures. Usually built as a small appliance, products by **NetBotz** (www.netbotz.com), **Wilson** (RLE Falcon, www.wilsonengineered.com/RLE_Base_Package.htm) and **Phonetics** (Sensaphone: www.sensaphone.com) are now available to monitor the physical environment of unattended components. These products are typically priced at less than $1,000 and can be networked using an Ethernet port. They include a Web server that allows a direct viewing of parameters from a browser, and an SNMP agent that can forward alerts and alarms to a NOC console. Alarms and alerts can also be transmitted by pager or e-mail.

NetBotz appears to have taken the lead by including several features not seen in other products. The appliance can be a wall mountable unit or in a rack unit and can be used to monitor the external or internal environment of different computing equipment. Netbotz proposes a central system that can be used as a monitoring center. Snapshots from an incorporated camera can be uploaded either periodically or following an alert provoked by an intrusion detection device, for example.

It is clear that the level of awareness of potential threats to remote and unattended infrastructure components has been considerably raised after Sept. 11. Remote monitoring of the physical environment has become, consequently, a must have rather than a nice to have. Organizations with remote offices should actively consider adding environment monitoring appliances to the NOC data and event collection. Of the products proposed on today's market that are price compatible with small to midsize offices, NetBotz offers a distinct advantage through its centralized management server and the inclusion of a snapshot camera to its distributed appliance. The added function does not consume a lot of bandwidth (snapshot of five frames) and could prove valuable in sorting false alarms from true problems.