

*Did you ever get caught by surprise because of a network problem and had downtime as a result? What about monitoring your network?*

Network downtime or network related problems cause up to 37 hours of down time per person each year. Do you have unexpected network downtime that costs you money? Do you have the proper monitoring tools in place to reduce these costs?

**E**ven the smallest company has got several network devices in their organization. In many cases those devices are installed wired and then they are forgotten. It may be possible that you never have any problems. But what if your organization is larger or it is growing? Does your network infrastructure grow with it? Or do you just wait until end users start complaining and then take action? Or what if the devices have reached the end of life and are not performing anymore as they should have or have malfunctioning parts or are simply obsolete?

Maybe it is time then to think about monitoring your network in a structural way. This can be done with many tools that are available in the market or even with applications which are available for free, if you plan to do some small simple monitoring. Knowing what is going on in your network infrastructure can help determining the problem and solve it faster than just guessing and start changing settings or replacing devices.

### **Preventive monitoring**

In the good old times we maintained the saying 'if it isn't broken, don't fix it' and so it became true that most network administrators didn't take any actions until something actually was going wrong. End users, who started complaining about lack of speed or broken connections, were normally the reason that made people move and search for a cause and a solution. In the meantime expensive end users where waiting in front of their lifeless machines until the network problem was solved, which often wasn't a case of minutes, but more like hours or days.

Therefore, modern network monitoring tools are not anymore the small handy tool which you can plug whenever something goes wrong, they are advanced systems

which continuously monitor your network environments, traffic, availability, interface status etc. They take care that whenever something happens, that is not supposed to, alerts are being sent to persons who are directly responsible and not to the long line of end users to network administrators.

### What and which devices do we need to monitor?

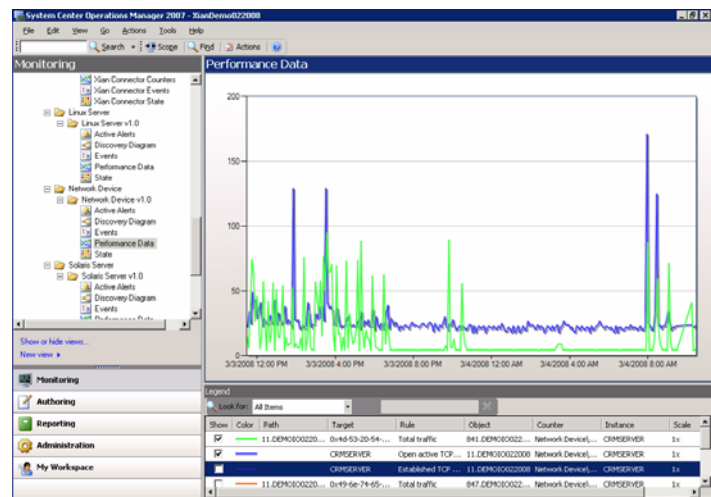
So you have decided to start monitoring your network. What is the next step? Well, first take care that you know what you want to monitor. This is not as easy as it seems, and people tend to start monitoring without giving it a good thought in advance. Even for the smallest network environment it is important to make a small analysis and plan before you start. Next we will discuss a simple standard procedure to help defining what and how to monitor your network.

First ask yourself the following questions:

- What kind of problems did you see in your network in the past?
- Which network devices were involved in those problems?
- Do you know if your devices are reaching end of life?
- Are you currently having problems with network speed and downtime?
- Do you have availability issues?

Then define the next monitoring fields:

- Where in your company are the critical servers and connections?
- Are there special end user activities which need profound monitoring?
- What are the quality standards demanded by the CIO office?
- Are there any other contracts which demand special monitoring?
- Where are the real costs of network problems (for example downtime)



*Performance data from Jalasoftware Xian Io objects in System Center Operations Manager 2007*

Once you have answered the questions above you can start selecting those devices which comply. Very often these are switches, routers and firewalls but in many cases you can also think on VPN Concentrators, Wireless devices, or UPS's. Then it is time what you want to monitor on your devices. There are many options on that side, so try to focus on those data and alerts that can catch problems, analyzed above.

Active Alerts (41)					
Source	Name	Resolution State	Created	Age	
Severity: Critical (40)					
FastEthernet0/6 (7)	Total traffic Alert	New	3/5/2008 2:12:52 PM	1 Minute	
FastEthernet0/15 (16)	Total traffic Alert	New	3/5/2008 2:12:51 PM	1 Minute	
FastEthernet0/1 (2)	Total traffic Alert	New	3/5/2008 2:08:30 PM	6 Minutes	
LinuxDemo	Device Availability Alert	New	3/5/2008 8:48:30 AM	5 Hours, 26 Min...	
demoIo022008.jalasoft.local	SQL Server Broker disabled	New	3/4/2008 12:32:55 PM	1 Day, 1 Hour, ...	
Machine with linux	VM Heartbeat Alert	New	2/22/2008 7:39:47 AM	12 Days, 6 Hour...	

*The Jalasoft Xian Io Alerts appearing in Microsoft System Center Operations Manager 2007*

So, what kind of aspects of your devices should you think of to start monitoring?

- Device Availability
- Interface operational status
- Interface traffic (normal, errors, discarded packets)
- CPU usage
- System uptime
- TCP connections
- Memory pools
- Temperature (UPS)
- Fan status

Monitoring some of these aspects needs of course a fine-tuning and for that reason it is better to start retrieving only performance data from a specific counter and select an alerting threshold on a later stage. Most applications have the option to do that. Other rules like interface operational status can be configured directly with a threshold. However, be sure to choose the right interfaces and that you only select those which are up and actually used. A useful tip, even for those cases is to collect performance data before setting up the thresholds.

**“It is easy to monitor your network, and you can save yourself a lot of troubles!”**

#### *Availability*

Monitoring the availability of a device should never be missing on any scenario. An availability rule verifies if the connection between the monitoring software and device is up and running. Also in many cases, it can retrieve counters like response time and its status. A rule like this will easily allow you to get the first impression of the network health.

#### *Interface Operational Status*

Every interface might be affected somehow one day. This can be an unplugged cable, cable breach, broken or disabled interface. Especially if we take into account that core

switches interfaces might go down. A simple monitor can check this for you and even extensive reporting helps you guarantee quality.

#### *Interface Traffic*

Excessive traffic due to increasing number of users, errors and discarded packets stress the need to monitor to be able to take preventive measures or to define bottlenecks in time. A simple threshold on your traffic can warn you.

#### *CPU load*

A very simple aspect and with a value that normally will not vary too much, unless something is wrong. A higher CPU load suggests more work for a switch which is not always normal

#### *System Uptime*

Normally the network devices system uptime grows gradually, unless a power failure stops the device or it is reset. Therefore it is important to be warned when the system uptime goes to zero, but also when the system uptime goes over a certain value for example to do annual maintenance.

#### *TCP connections*

Open, active, failed, established TCP connections can be an important indicator of the performance and the security of your network. A simple rule can warn you when these numbers get too high.

#### *Memory pools*

Performance issues on the switch or the network can be caused by the state of the switch in relation with the memory. Many rules are possible but a simple rule which at least monitors the free available memory can already warn you when the first symptoms appear.

#### *Temperature*

In the case of UPS but also switches and routers, many suppliers offer the possibility to monitor the temperature. It is needless to say that a high temperature can cause serious problems.

#### *Fan status*

Fans don't work forever and are often one of the first components to give up. Although in many devices there are failovers available, to have an alert when it goes down isn't excessive luxury.

Of course there are many other rules offered by monitoring applications but with the list above you will have a good start. However take the following common mistakes into account before you decide on your monitoring strategy.

- Do not monitor all your devices
- Do not monitor all your interfaces or processes

- Do certainly not put alert thresholds on everything
- Try to use reasonable intervals to prevent performance problems due to the monitoring.

Of course you are free to ignore those, but then be prepared for a flood of alerts from your devices and interfaces and a fast growing performance data Database. If you have a system to forward any alert to your emails, you definitely need to be careful with what you monitor.

### Notifications

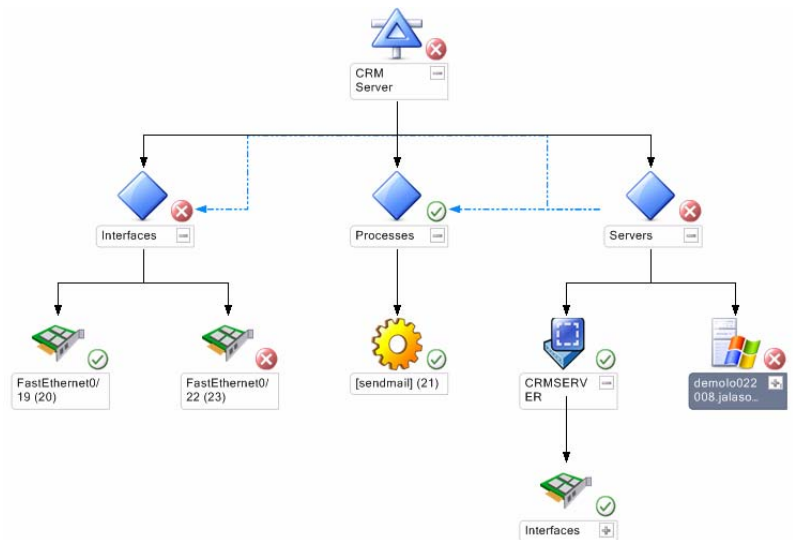
Once you have all the data and alerts, there are many possibilities to use this information. The alerts can be forwarded to your email, sms, messenger, etc. taking care that you are aware of anything that goes out of the ordinary wherever you are. Also some applications have the option to forward alerts to different persons. You can send your network alerts to the network administrator and alerts related with Linux to your Server or Linux administrator.

### “Who does not want to see the state of network and servers in one single console?”

Just in case, do take into account that alert forwarding needs a network connection and if a critical part of your network is down, alerts might not go out. Exactly for those situations it is useful to have your monitoring system at a strategic location where hardly anything can cause problems. Another option is to create a test alert that runs on a specific interval and guarantees the notification system is working correctly.

### Solutions

A very well integrated solution to monitor your network, applications and servers is the combination of Jalasoft Xian Network Manager Io with Microsoft System Center Operations Manager 2007. In a very user friendly and single console environment, you are able to monitor your windows servers, Linux servers, virtual servers, switches, routers and many other network devices. On the Xian Io side you can easily add network devices and set up rules. All without any complicated scripting, just a matter of drag and drop the rules. Xian Io comes with about 100 build in rules per device type!



*A distributed application with Jalasoft Xian Io objects in System Center Operations Manager 2007*

A very useful feature which Xian Io and Operations Manager 2007 offer is Distributed Applications (DA). The base idea of this feature is that you combine different objects which are all related with the same application. For example you want to monitor your CRM server. In a DA you can add the different switch interfaces which the server uses, the windows server or even specific processes of a Linux machine. Whenever something goes wrong that might affect your CRM Application, an alert is visible on the specific object which is causing the problem. So a root cause analysis has become even easier. This can significantly help you taking preventive actions when something is about to go wrong or at least you are able to find the cause faster and reduce the downtime of your network and end users.

### **Syslog monitoring with Xian Io and Operations Manager 2007**

For those who are familiar with Syslog, they know that a Syslog message can report a serious and important event but they also know that it is easy to be flooded with other not important syslog alerts and it is not always that easy to configure since it has to take place on the device which is sending the syslog. However, since basically all network devices (and even applications) support syslog, it should not be forgotten when monitoring your network. An interesting advantage compared to SNMP monitoring is that alerts arrive asynchronous and you do not depend on your interval.

But what can we do about those large flows of syslog alerts? Connecting to the device and change it, is complicated and in most cases different for each device. That is why Xian Io can work as a syslog catcher and filter before forwarding the alert to Operations Manager 2007. Enabling this in Xian Io is very simple, you only need to take care that the device is sending the syslog alerts and create a simple keyword based filter on the Xian Io side. With that you will only receive important alerts and then take action fast without been annoyed with many alerts you do not want to see.

#### **More Information:**

Jalasoft Corporation

[www.jalasoft.com](http://www.jalasoft.com)

Phone +1 888 402 6717

sales@jalasoft.com