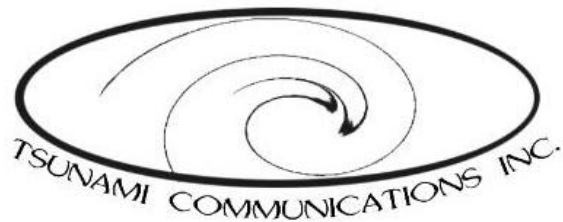


Tsunami Communications Inc. Whitepaper on:

## Planning to Monitor a Windows 2000+ Network on a Shoestring Budget

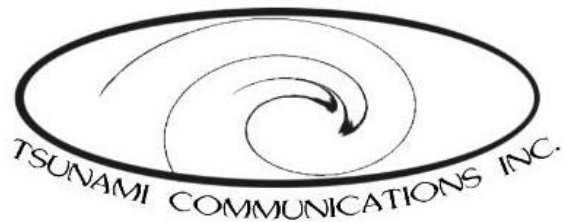
Prepared by: Jason J Kennedy  
May 31, 2004

Version 1.1  
Last Revised: 6/10/04



## Table of Contents

Introduction.....	3
Approach .....	3
Setting Your Scope .....	3
Defining Your Parameters.....	5
Up/Down .....	5
Processor.....	5
Memory .....	5
Disk.....	5
Services .....	5
Event Logs.....	6
Choosing Your Technologies .....	6
Simple Network Management Protocol (SNMP) .....	6
Windows Management Interface (WMI) .....	6
Conclusions .....	7



## Introduction

Microsoft Windows technology is prevalent in small to mid-sized companies, but the systems and processes to effectively monitor that technology rarely are. It is important to state that there are varying degrees of systems management, and in this paper we are specifically addressing the lowest common denominator – getting some quick results from a minimal investment in time & money. The more effort (and greater cost) you can afford up front, the more complete architecture you can implement, but these tips are to help get a foot in the systems management door – an entry level solution that can be built upon.

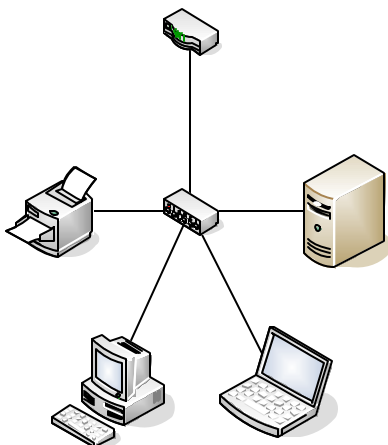
## Approach

### Setting Your Scope

Do you already know what you want to achieve with systems management? It's important to set some clear, achievable, and defined goals for your systems management implementation. Take the time up front in the work to nail these objectives and set your scope, so you can have some measure as to when you know you've accomplished what you've set out to do. Another important part of the scope is to define what systems you wish to manage.

For the purpose of this paper, we are specifically addressing Windows 2000+ server networks, but those networks are probably linked together by network devices. If your networking gear is manageable (see the "Choosing Your Technologies" section) then you'll be able to manage the servers and the links between them. For that reason, we will also include standard network attached printers & network devices (routers, switches, hubs).

Standard practice is to manage all systems "upstream" of the desktops. The following diagram illustrates the components in an average small-to-medium sized business.





At the top of the diagram, we show the router, the device which provides access to the Internet or other corporate networks. At the centre is the switch (or in some cases, hub) that interconnects all the devices at any particular physical location (office). To the right is a server, the left, a printer, and at the bottom a PC & laptop representing any number of personal computing devices on the network.

So consider “upstream” devices to be anything in the diagram above the personal computing devices, or, any device connected to the switch (or hub) except for personal computing devices.

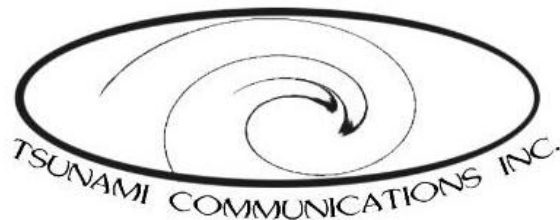
Ultimately, you will have to decide whether or not to manage any particular devices on your network – factors that may weigh into the decision are:

- Manageability – is the device actually manageable? If so, how readily?
- Importance – how critical is the device to your overall network? Are there other devices people could readily use? Is this a shared network device (server, printer, etc...)? How sensitive is the data or application(s) on the machine to the operation of your organization?
- Profile – who is the key user of the device? Do they require higher “uptime” than other users?

Once you’ve determined what you want to achieve, and have a list of which devices to monitor, make sure you document this all. Put together a document that summarizes your systems monitoring goals – it doesn’t need to be elaborate, but it should be clear & specific. Next you should create an inventory of the devices to be monitored. It is a useful exercise to make use of a spreadsheet that keeps this list well organized. The following example shows a good example of the kinds of data you’ll want to collect on your network devices to be monitored.

Device Name	IP Address	Make	Model	OS	Patches/Vers

In summary you will be best off to start into this process by using some business & technical criteria that make sense to your organization to select & inventory the pool of network attached devices to be monitored, and document your goals & inventory.



## **Defining Your Parameters**

Having determined what you expect to achieve, and being certain which devices (or “nodes”) you wish to monitor, you can move forwards to the next step, which would be to determine what specifically you will be monitoring on each device. This is a more complex task than it sounds, but can be broken into easy tasks. Start with “the basics” which can apply to any network attached device, but we will focus on the Microsoft servers:

### *Up/Down*

Also known as a “ping test” this is used to determine if the server is available on the network – but of itself is not highly useful other than to approximate whether the server is “generally” available rather than fully functional.

### *Processor*

Monitoring the usage of the processor can be confusing with all the options available. There are many options for monitoring the processor(s) in a Windows system, and the right ones for your situation can be determined through research, experimentation, and consulting with experienced Microsoft experts. It’s very valuable to be able to know if your processor(s) are over (or under!) utilized for an extended period of time. It’s also important to be able to watch the trending of processor(s) utilization over time, so you can see if you need to take any actions to address performance issues.

### *Memory*

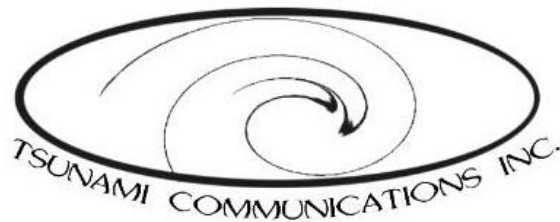
Much like processor utilization, it’s vital to be aware of how the memory in your Windows server is being used – physical & virtual memory. This includes observing the use of paging (moving information from physical memory to virtual memory) which can significantly slow down server performance. Again, you will want to watch for thresholds to be crossed at “danger points” and be aware of long-term trends so you know if you need to add memory, or take some other corrective action.

### *Disk*

It’s quite easy for server disk to get used up without knowing about it until it’s too late. Watching for disk usage thresholds to be crossed, and tracking the consumption of disk space over time are highly valuable metrics to observe. A key with this is to enable disk monitoring by running “diskperf –y” and then rebooting. This will consume slightly more system resources (processor & memory) but is worth the minor expense for the value provided.

### *Services*

Each Windows server will have key services that need to be watched – it will depend upon the purpose of the server to know which services to monitor. The services should be carefully observed to make certain they stay running. Often you may want to set the services



to try and automatically restart if they should fail the first time, and if they continue to fail to alert the support people for the server. The set of services monitored will likely be different, on different servers – print servers, domain controllers, database servers, application servers, web servers, etc... an experienced systems management professional can point you in the right direction.

### *Event Logs*

While it can be extremely useful to monitor the information populated into the system, application, and security event logs on a Microsoft server, it can be overly burdensome to be notified of *every* event. It is highly useful to know what key words to watch for and alarm on relevant instances, not every single event.

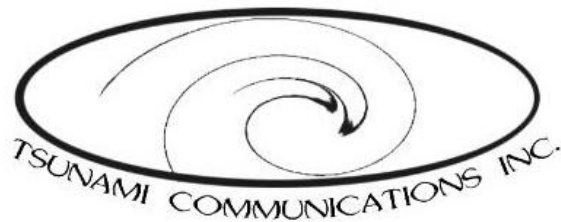
## **Choosing Your Technologies**

### *Simple Network Management Protocol (SNMP)*

SNMP is the technology used to monitor those “other devices” on your network, but can also be leveraged to watch over the Windows servers. It is not the native protocol for managing Windows systems, but there are ways of configuring your Windows systems to take advantage of this universal management standard. Chiefly though, SNMP would be used to manage routers, switches, and network attached printers (and any other “SNMP enabled” devices) on your network with the use of a systems management application that makes use of SNMP. Numerous applications are available that make use of SNMP, and range in features and functions from low-end solutions to enterprise-class software. An experienced consultant can guide you to the right tool for your environment.

### *Windows Management Interface (WMI)*

The link to WMI is via the “perfmon” set of performance monitoring tools. The most common way to access this imbedded Microsoft technology on any Windows server is by use of the “Perfmon” application. WMI is the acknowledged standard for measuring system resource (processor, disk, memory, etc.) utilization on Windows servers, and is leveraged by almost every Windows management application. WMI data can be accessed locally on the server by perfmon or agent software that makes local WMI calls, or remotely by applications that can communicate over the network directly to the perfmon statistics gathered on the Windows server. There are benefits to either method of gathering the WMI data, but some risks inherent as well. Once again, it’s beneficial to lean on the expertise of a professional who’s worked with these technologies and can provide technical leadership in this area.



## Conclusions

The steps outlined in this paper address how to plan for cost-conscious alert & performance management (two of the important first levels of systems management in the Tsunami model). Putting together a plan before starting in on even an entry level solution will save time, money, and technical challenges in the future. Start by defining your objectives, and your scope – know what you're doing and why, and what measurable objective benefit you expect to see at the end of the process. Next make your inventory, and ensure that those nodes (network-attached devices) to be monitored are configured to meet any management pre-requisites. Carefully choose the metrics that fit your objectives and scope. Don't create more work for yourself than you need to! Finally, choose the technology that best meets your needs and you're ready to pick a product and roll forwards.

This document is provided for general information and educational purposes only and is not intended to replace professional advice and services or the maintenance of any systems. In no event will Tsunami Communications Inc. be held liable for any decision made or action taken in reliance upon the information provided through this web site or any published documents.