Web Based Monitoring and Management

Comments on Scope and Starting Point

19 February 2003

1 Scope and Purpose:

This unofficial document is submitted to the WBMM working group of the PWG to advance some specific ideas on the scope of the effort and what may be taken as a starting point.

The purpose of the WBMM activity is to address the many circumstances where limited extra-enterprise access to imaging functions for maintenance and support purposes is necessary to properly support the enterprise, to allow effective supply and maintenance of imaging equipment, and to provide usage information for billing purposes. This need to address extra enterprise access to equipment isolated by a firewall is a key requirement distinguishing WBMM from other potentially similar activities such as XMLCONF, WEBDAV, and "remote access", which do not appear to address this problem. This is not to say that these other initiatives may not include ideas that are applicable to WBMM. If my assumptions are correct, this firewall-surmounting problem not only affects the transport, but also the basic operations.

I have included here a set of scenarios that represent my understanding of what the group is addressing and a few scenarios that, to me, are definitely out of scope. I have taken a crack at what seems to be to be an obvious approach, and the implications of this approach.

2 Use Cases

Specific scenarios are an effective way of cutting through the misunderstanding caused by abstract definitions, and checking back to see that those scenarios are effectively addressed is a good method of keeping the development on track. I offer the following as cases to be addressed and a few to not be addressed. There undoubtedly are other that should be included and I continue to solicit candidates.

2.1 Scenarios to be Addressed

I suggest that, as a minimum, these scenarios should be covered:

Scenario 1: *IKA, an office equipment leasing company, leases and services printers and copiers from several manufacturers to a wide range of customers. One specific customer*

is an insurance company, American Casualty Ensurence (ACE). ACE is very concerned with security but also is demanding no more that 0.5% downtime for the equipment. Under different circumstances, IKA would have resident service people checking the equipment, keeping usage figures for billing, and ready to react if a user reported a problem. But because of the security issues, ACE will give service people access only when there is a problem. Security also prevents IKA from access to the ACE network to use standard equipment monitoring programs. Indeed, between traffic and security concerns, ACE does not allow programs using broadcast SNMP to be on its network.

***Scenario 2**: ACE does allow its employees Internet access though an HTTP proxy. However, ACE does not allow any other Internet access including FTP. ACE will allow Ika to communicate status and usage information using the WEB access structure in place, provided that ACE MIS has the ability to monitor the communication. Nothing that reflects anything about the network or the business can be communicated: this includes IP addresses, device names, and of course, any job information.*

***Scenario 3**: DAKON, an office equipment leasing company, sees a market opportunity in the small to mid-sized office market. They believe that if they can get service contracts to maintain the 2-10 printers and copiers characterizing the businesses, they will make money on the consumables and eventually will get to lease equipment to these companies as the equipment in place ages out. In the short term, they need automatic reporting of low supplies and problems for the rapid response they are advertising. In the longer term, they will need to use the web service to get copy counts for billing and the capability of remote update/upgrade.*

***Scenario 4A**: Better Pinter Manufacturing (BMP) is marketing a high-reliability networked printer/copier, and bundling the unit with a supply and service contract. Their information suggests that the profit on supplies will be substantial, and with remote reporting and monitoring, the service aspect should at least break even. They need to set up their customers so that supplies and failure information is quickly communicated to one of their centralizes depot facilities. But the capability must be easy to install, requiring no unusual effort from the often-limited MIS groups. The solution must address concerns about network, equipment and information security from increasingly squeamish companies.*

***Scenario 4B:** BMP has a printer with all the bells and whistles, but at a high end price. Marketing fears that the price will hurt sales, but believes that, if they disable some of the features and sell the product at a lower price, they can make it up later by "upgrading" the units in the field to have full features. Of course, the upgrades need to be easy and must not require either customer service visits or any technical action on the part of the customer. They would like the ability up upgrade device firmware using the Web Monitoring and Management Capability put in place for service and supply maintenance.*

2.2 Out of Scope

I suggest that the following scenarios are at best edge cases and are out of scope.

Joe is holed up in a hotel where he has high-speed internet service.. His secretary calls him up and says that the network printer is not working. Joe wants to access his printer via the Internet so that he can see what is happening.

Despite the fact that it seems an unlikely scenario, WBMM could support this indirectly. An outside service could be monitoring the printer, and provide a website that Joe can access. This website could have a page for Joes printer that indicates printer status, history … whatever. It could even allow Joe to indicate that, on the next contact, some particular set of parameters would be monitored. But this would be outside the scope of WBMM.

Builders Union Limited (BUL), a sales and clearing house for local builders doing house building/ remodeling, with offices in the New England states, has a motley selection of printers and copiers, ranging from large format color printers to low cost inkjets some salesmen smuggle in for convenience. Some devices are networked; some are not. Some are connected to PC's that are networked. The new corporate office manager decides to save money by using the services of Office Supply Company (OSC) to maintain all imaging devices and keep them supplied. In this "blank check" approach, OSC will service the varying base of imaging devices at BUL using WEB services.

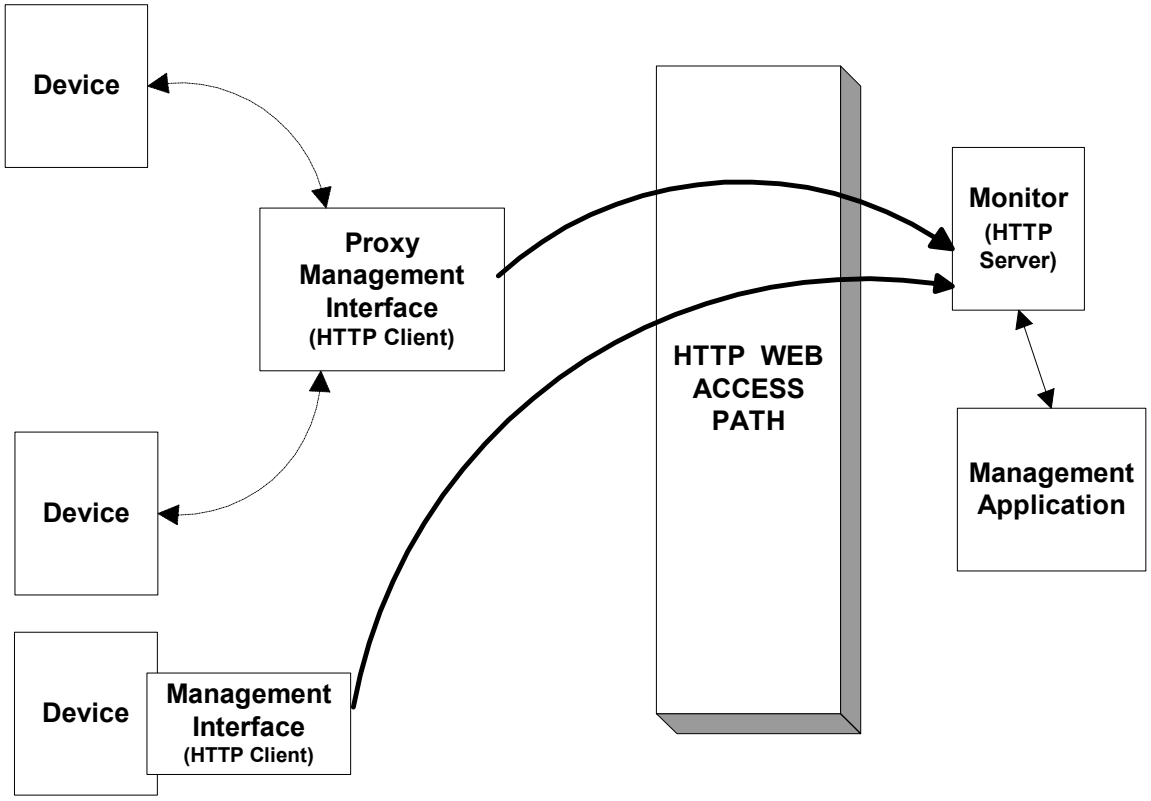
This is a nightmare scenario. OSC cannot maintain non-network connected copiers using WEB services (unless they equip them with radio or modem links). And BUL would not like the bill for servicing a varying base of imaging units, which included providing fresh ink cartridges for printers that salesmen brought in from home for the day. There needs to be some process by which the devices to be serviced are identified. And this should be independent of the basic monitoring and management capability. I suggest that the method of identification is out of scope.

3 The Starting Point

The following "neutral" terminology will be used to facilitate discussion

1. The equipment or service being monitored/managed is the "Device"
2. The function allowing remote monitoring/management is the Management Interface or "MI", where the MI can be in the Device or outside of the Device.
3. The entity doing the monitoring/managing is the "Monitor".

The relations are schematically represented in the attached diagram.



3.1 The Accessible Path

The primary consideration is that most enterprises have a firewall, and allowing internet access to imaging units is not an option because of the perceived increased vulnerability of the network, the effort necessary in special handing the device connections, and the potential for abuse of the devices themselves.

What is in place however is a usually well-protected channel from the enterprise to the Internet to allow employee access to the WWW. Intuitively, it appears that the use of this existing path offers the best solution. This is perhaps jumping ahead, but it would be useful if we could agree to this as a key point in the solution.

If we use this path, it means that the connections must be initiated by the MI, not the Monitor.. Therefore, by usual terminology, the MI is the client and the Monitor is the server.

3.1.1 Implications

This structure has ramifications on the modes of operation.

A. Since the Monitor is a Server:

1. there must be some other interface between the Monitor and whatever consumes the data. I consider this interface out of scope, although general characteristic of this type of interface may be considered in the data form.

2. the interface between the MI and the Monitor is not intended for direct human consumption

B. The MI must be set up to contact a specific Monitor according to a program or on operator command.. Monitors cannot contact a site and "sniff" for MIs.

C. There will be a limited number of specific Monitors that an MI will need to contact, and these will be set up by some process that is out of scope. Contacts will not be "cold" The MI will "know" what Monitor it is to communicate with. The ability to handle "unknown" contacts should be considered only in terms of lockout to prevent security breaches. The establishing of a relationship between an MI and a Monitor is out of scope. I suggest that there is no need for an MI to be able to discover a monitor.

D. When the MI does contact the Monitor, in the most general case, the Monitor must be able to:

1. request immediate operations to be performed related to the device, perhaps including:
    a. get object
    b. set object
    c. transfer file
2. set up a series of instructions in the MI, including:
    a. when to next contact the monitor for instructions
    b. what parameters to monitor and actions to take, per Device (e.g., alert reports, update code when not busy, etc)
    c. what data to gather and when to report this data back to the monitor
    d. delayed or timed initiation of file transfers

3.1.2 Operations

3.1.2.1 Initial Reports

The MI must make a connection to the designated Monitor when it is first brought up, whenever there is a change in configuration, when power is restored after a power off, and whenever the MI may have lost the last instructions. In this report (as in all reports), the MI must identify itself, including a series of parameters that may include identification, location and date-time. In the case of a proxy MI servicing multiple devices, this initial report must include the number and nominal identification of each of the devices registered in the proxy for monitoring.

After providing the initial report, the MI must be prepared to receive instructions.

3.1.2.2 Basic Operations

Certainly, an RPC approach could be used, or a complex set of instructions. But, as indicated above, functionally the necessary set of commands appears to be

a. get object (object ID)
b. set object (object ID, value)
c. transfer file (file name, transfer mode)

and perhaps

d. get object group (group ID)

We have used an OID prefix as a group ID, meaning get all objects with that prefix. This acts both as a indexing mechanism and a flexible get bulk. But the get object group could also just apply to a named group. I am inclined to not include the naming of objects in the WBMM activity, or at least, not restricting naming to a given scheme

3.1.2.3 Compound Operations

In many cases, the Monitor will want to have a report only if an object's value represents some sort of problem. Therefore, there should be an operation that amounts to "get object, compare and report" or sense object:

a. sense object (range, in range/out range) and
b. sense object group (range, in range/out range)

when all objects of the group are of the same data type and the same range class, such as the severity index in the prtMib alerts table.

It is unclear if a sense object group with array of range values would be necessary. It is unclear if a special commands would be necessary for comparison of bit mapped values, or strings.

3.1.2.4 Time Argument

Elaborating on the operations, I would collapse the "immediate" commands into special cases of the timed or periodic instructions. That is, there would be a serial of operations and compound operations with time arguments of

1. NOW,
2. THEN (time-date), or
3. EVERY (period or repeated time).

"EVERY" could be every ten seconds (period), every hour at ten minutes after the hour (repeated time), or every month on the last day of the month at 23:55 hours (repeated time)

3.1.2.5 Moderation

Particularly for alerts, the Monitor will want to receive a report when the alert occurred, and when the alerting condition was removed. It is unlikely that a report will be tolerated ever time the condition was observed. So I suggest that that form of moderation be inherent. There may also be a certain amount of filtering desired, so that a condition must exist for N poles before it is reported, or must be gone for M poles before it is reported resolved. There may be the desire to not report secondary conditions during a major alert

condition (e.g., report off line, tray out, open door etc during a paper jam). It is not clear of special instruction parameters should be defined to allow specification of these types of conditional responses.

3.1.2.6 Extraordinary Conditions

Particularly for proxy MI's, some events should cause alert reports, perhaps without specific instructions. Such conditions would be verified failure of the device to respond to polls (not just one lost query), and perhaps invalid responses. The an example of the latter, might be no such object responses to an SNMP request for some object being monitored.

3.2 Inter-Enterprise Management

It has been suggested that the Monitor could also be internal to the enterprise. Although there is some potential commonality, the constraints on an internal Monitor are much less and the requirements of management information are typically much more extensive. In addition, there presently is a well-established and well-supported method of intra-enterprise device management. At this point, I suggest that the WBMM working group seek to maintain compatibility with inter-enterprise management efforts to the extent that such compatibility does not compromise the primary purpose of remote management.