Title: Standards-based Secure Management of Networks, Systems, Applications and Services using SNMPv3 and HP OpenView

Session #: 325

Speaker: David Reid and Steve Blizzard

Company: SNMP Research
Topics

• Summary of Current Situation
• The Internet Standard Management Framework
• Management of Networks, Systems, Applications, and Services
• SNMPv3 with Security and Administration
• HP OpenView NNM and SNMPv3
• Management of Networks, Systems, Applications, and Services revisited
• Examples
Current Situation

- Management solutions based on IETF standards have been deployed pervasively for network monitoring using SNMP, standard MIB objects, and enterprise MIB objects
- OpenView NNM is widely deployed as the heart of management “ecosystems”, in conjunction with many integrated management tools
- Not as widely used for configuration and control due to lack of security
- Most system and application management tools are proprietary
Deficiencies of current tools

• SNMPv1 and v2c are not secure, therefore:
  – Not used for configuration
  – Not used for system and application management
  – Not configured for acknowledged informs
• System and application monitoring products are frequently not interoperable, even from same vendor
• Proprietary solutions do not support selecting “best of breed” building block components
• Discontinuity in adding system management to network management infrastructure
• No elegant way to encapsulate home-grown management tools in standards-based framework
The Internet Standard Management Framework

• Built around the Simple Network Management Protocol

• More than merely a protocol for moving management data - a complete framework, defined by Internet standards and consisting of:
  – A data definition language – the Structure of Management Information (SMI)
  – Definitions of management information (Protocol Independent) - Instrumentation described in the Management Information Base (MIB)
  – Protocol definition (MIB Independent) for SNMPv3
Increasing Scope

- The SNMP Management Framework has traditionally been used most widely for network management.
- The scope of SNMP-based management is increasing:
  - Not only traditional network management.
  - Management of the systems connected to the network.
  - Management of the applications running on those systems.
  - Management of the services provided by those applications.
- System and Application Management may be the most rapidly growing portion of the management software market.
Value of Standards-based Solutions

• Interoperability between products from different vendors
• Enables selection of best of breed components
• Internet standards process results in a high-level of completeness and robustness
• End-users may deploy management solutions in pragmatic building-block, step-by-step solutions, instead of higher-risk enterprise-wide management re-architectures
Standardization Process

• SNMPv3 with security and administration is now an IETF to “full standard”.
• The IETF also moved SNMPv1 and SNMPv2c to historic status.
  – While vendors will continue to support SNMPv1 and SNMPv2c for some time to come, SNMPv3 should be used for Internet management, as it provides security and administration that was not previously available.
Management of Network, Systems, Applications and Services

• These divisions are often arbitrary: often it is difficult to distinguish between systems and applications

• Is management of a service level application application management or system management

• Is a web server an application or a managed network service

• “No matter where you are standing, the application is the layer above you”

• Users care primarily about the services delivered by these applications
Management of Network, Systems, Applications and Services

• Two parts of the problem:
  – knowing (definition and instrumentation)
  – telling (import and export): extensible agents

• Systems and Applications can be designed for manageability

• But often are not, at least in a truly open way
Two implementation options

• Non-invasive: watch the external behavior of processes from the outside
• Invasive or fully-integrated: watch the internal behavior of applications from the “inside”
• Each has a time and place and they are not mutually exclusive
Non-invasive management

• It is often not timely or practical to add instrumentation for invasive monitoring of applications which were not designed for manageability.

• In the meantime, some progress can be made in a non-intrusive manner for the monitoring and control of mission critical applications.

• Watch mission-critical applications from the “outside” including distributed client-server applications.

• Monitor processes, CPU time, memory size, etc.
Non-Invasive management

• Make inferences about their health by watching the resources they consume using the instrumentation provided by the run-time environment (operating system)

• Start applications as children so you can catch them along with their exit codes [if and] when they die
Fully Integrated approach

• Watch applications from the “inside”
• Design for manageability
• Install the instrumentation inside the application to meter the appropriate data
• Implement MIB in the application using a user-friendly toolkit (e.g. a Subagent Development Kit) to provide direct access to the instrumentation
Enabling Technologies

• Two important enabling technologies for making systems and applications SNMP aware:
  – MIB standards (Host Resources, System Application, etc)
  – extensible agents (including tools to extend)
System Management

SNMPv3 agent

CPU
Memory
File system
Disks
System Management

• React to problems
  – File systems filling up
  – CPU overutilized
  – Low memory availability

• Anticipate problems
  – Watch trend of shrinking file system free space

• Troubleshoot
  – Where is activity when problem is occurring?
Application and Service Management

SNMP agent

Processes

Process memory use

Log files

Installed applications

Services
Application Management

Process management is key component of application management

Example: HP OpenView

- Are all processes running?
- Is trapd.log growing?
- Any processes using lots of CPU?
- Any processes using lots of memory?
# System & Application Management

## Using SNMPv1

<table>
<thead>
<tr>
<th><strong>Pros</strong></th>
<th><strong>Cons</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Resources MIB (RFC 1514) provides much system information</td>
<td>Security not rigorous</td>
</tr>
<tr>
<td>Applications MIB (RFC 2287) provides much application information</td>
<td>Access control generally non-existent</td>
</tr>
</tbody>
</table>
System & Application Management

Using SNMPv1: Risks

- If someone knows the read-write community string then they could...
  - Set your system date
  - Set the boot device
  - Halt processes, like inetd

*like can be done via the host resources MIB*
System and Application Management with SNMPv1

- Security could be better
- Need better administrative functions
- Poor performance retrieving lots of data (no get-bulk)
Features of SNMPv2

• Expanded data types
  – 64-bit counters
• Improved efficiency and performance
  – Get-bulk operator
• Confirmed event notifications

<table>
<thead>
<tr>
<th>SNMPv1</th>
<th>Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2</td>
<td>Inform</td>
</tr>
<tr>
<td></td>
<td>(acknowledged trap)</td>
</tr>
</tbody>
</table>
Features of SNMPv2 (cont’d)

• Better error handling
  – Request 10 MIB objects
  – One object not available in agent

<table>
<thead>
<tr>
<th>Feature</th>
<th>SNMPv1</th>
<th>SNMPv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result</td>
<td>Error. noSuchName. (Even though 9 of 10 are OK.)</td>
<td>9 values returned. One noSuchValue returned for non-existent object.</td>
</tr>
</tbody>
</table>
SNMPv3 is key enabling technology

SNMPv2 +

Security

Administration
SNMPv3 Security

• User-based security model
  – Fine-grained access control
• Authentication
  – MD5
  – SHA
• Privacy (encryption)
  – DES
  – 3DES
  – AES
User-based Security Model

Defends against the following four threats

- Masquerade/data origin authentication
  - Interloper assumes the identity of a sender to gain its privileges

- Modification of information/data integrity
  - Alteration of in-transit messages

- Message stream modification
  - Messages are re-ordered, delayed, or replayed

- Disclosure/data confidentiality
  - Privileged information is obtained via eavesdropping on messages
SNMPv3 Administration

• Fine-grained authorization and access control
• Remotely configurable via SNMP set operations
• Logical contexts
View-based Access Control Model

• access is a function of . . .
  – who: securityModel, securityName
  – how: securityModel, securityLevel
  – why: read, write, notification
  – where: contextEngineID (constant), contextName
  – what: objectName
  – which: objectInstance
MIB Views

• Allow: (instance level granularity is optional)
  – some groups of users to have read-only access all MIB data
  – other groups to have read-only access to subsets of the MIB data
  – others get read-write access to some of the data
  – some could have read-write access to all of the data
  – all others get no access
MIB Views

• Source-side notification
  – Trap and inform
  – Filtering configurable via a standard MIB module
  – Source-side suppression of unwanted notifications
SNMPv3 Configuration

• Configure both agents and managers using SNMP sets
• Manually, one target at a time, or
• Semi-automated using configuration applications
• Easy-to-use tool for one target at a time (example = SNMPv3 Configuration Wizard)
• Policy-based configuration pushed to multiple targets (example = Simple PolicyPro)
SNMPv3 Configuration Wizard

Select type of configuration:

- Configure Community String
- Configure SNMPv3 USM User
SNMPv3 Configuration Wizard
SNMPv3 and HP OpenView

- SNMPv3 support available today using the SNMP Security Pack for HP OpenView NNM, OVPI, OVO, etc.
- EMANATE agent release 15.1 and above
Management of Networks, Systems, Applications, and Services (revisited)

- SNMPv3 allows you to manage what you want…
  - Securely
  - Easily
  - More efficiently
  - More reliably
- And elegantly integrates with existing management ecosystems
Standards-based, Secure, Smart Agents

• Standards-based
  – SNMPv3 with security and administration
  – Standard MIBs
    • Host Resources (RFC1514)
    • Application (RFC 2287)
    • Distributed Management (DISMAN)
    • etc

• Secure
  – SNMPv3 USM
  – Authentication and privacy

• Smart
  – Configure agent for distributed monitoring tasks
    • Distributed Management (Disman)
  – Intelligent notifications to management stations
    • Source-side suppression
  – Private MIB extensions
    • Critical application monitoring
    • Log file monitoring
    • Service monitoring
Extensible SNMPv3 Agent

- Run-time extensible SNMP agent
  - Add/remove modules dynamically
- Master agent/subagent architecture
- Development kit to add agent extensions (subagents)
- SNMPv1
- SNMPv3 with security and administration
- Consistent tools
- Can be integrated with existing management products
Host Resources MIB

• RFC 2970
• Information about systems and applications running on those systems
• Approximately 85 MIB objects
• Software information
  – Software installed
  – Software running
Host Resources MIB

• System Information
  – Number and type of CPU(s)
  – Processor speeds
  – System uptime
  – Processor load

• Storage and file system information
  – Number and type of disks
  – Disk utilization
  – System swap configuration
  – System memory and utilization
System Application MIB

- RFC 2287
- Applications installed on the system
- Elements and processes that are included in an application
- Currently running applications
- Past run applications
Application Monitoring via NNM and sysAppl MIB

![System Application MIB - Package Information: solaris26](image)

<table>
<thead>
<tr>
<th>Name or IP Address</th>
<th>Manufacturer</th>
<th>Product Name</th>
<th>Version</th>
<th>Serial Number</th>
<th>Package Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>solaris26</td>
<td>Sun Microsystems, Inc.</td>
<td>UTF-8 X Locale Environment</td>
<td>1.2,REV=1.0</td>
<td>unknown</td>
<td>/usr/openwin/lib/locale/c</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>UTF-8 Locale Environment</td>
<td>1.2,REV=1.0</td>
<td>unknown</td>
<td>/usr</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Iconv Man Pages for UTF-8</td>
<td>1.3,REV=1.0</td>
<td>unknown</td>
<td>/usr/share/man/man5/iconv</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Iconv modules for UTF-8 L</td>
<td>1.2,REV=1.0</td>
<td>unknown</td>
<td>/usr/lib/iconv</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>On-Line Open Issues ReadM</td>
<td>45</td>
<td>arthurn101438</td>
<td>/usr/share/release_info/S</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Power Management OM Utility</td>
<td>2.2,REV=97.0</td>
<td>it97062517004</td>
<td>/etc/default/sys-suspend</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Partial Locales</td>
<td>2.0,REV=97.0</td>
<td>ocelot9205081</td>
<td>/usr/lib/locale</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Core Architecture, (Kvm)</td>
<td>11.6.0,REV=1</td>
<td>on297w1521472</td>
<td>/usr/platform/sun4m</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>Korean UTF-8 iconv module</td>
<td>6.0,REV=1.0</td>
<td>aquaman970425</td>
<td>/usr/lib/iconv</td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems, Inc.</td>
<td>X11 ISO-8859-9 required f</td>
<td>3.6,REV=138</td>
<td>unknown</td>
<td>/usr/openwin/lib</td>
</tr>
</tbody>
</table>

Messages

[Buttons: Close, Stop, Restart]
Application Monitoring via EnterPol and sysAppl MIB
DISMAN Event MIB

• Defined by the IETF distributed management working group
• Monitor MIB objects and perform actions based on given conditions
• Reduces network traffic
• Designed to test SNMP MIB objects
  – Thresholds
  – Boolean tests
  – Existence tests
DISMAN Script MIB

• Defined by the IETF distributed management working group
• Monitor MIB objects and perform actions based on given conditions
• Reduces network traffic
• Uses scripts to aggregate, summarize, and transform data into useful information
DISMAN Schedule MIB

• Defined by the IETF distributed management working group
• Periodically perform SNMP operations at scheduled intervals
Remote Operations MIB

• Defined by the IETF distributed management working group
• Designed to perform ping, traceroute, and nslookup operations from a remote host
• Perform operations periodically and report problems
Critical Application Monitor

• Monitor an application
• Send a trap when the application terminates
• Automatically restart the application
NNM Application Monitoring

• Monitor processes via private MIB
NNM Application Monitoring

• Monitor processes via private MIB
Log File Monitor

• Examine log files
• Perform an action when user defined patterns are encountered
• Perform and action when the log file exceeds a certain size
• Actions
  – Send a trap
  – Run a command and/or script
NNM Log File Monitoring

- Monitor application log files via private MIB
NNM Log File Monitoring

• Monitor application log files via private MIB
File System Monitor

• Shows current file system information (df –k command)
• Sends notifications when a file system reaches near capacity
• Perform actions based on file system problems
• Actions include sending a trap and running a command or script
NNM File System Monitoring

- Monitor file systems via host resources or private MIBs
Service Monitor

• Determine if a service is working properly
• Measure the response time of a service
• Services include http, ftp, dns, smtp, pop3, and snmp
• User defined services are also supported
Native Agent/Subagent adapters

• Allows for smooth coexistence superagents and the native SNMP agent provided by the underlying operating system or other SNMP agents
• Other SNMP agents will work seamlessly
Summary

• The combination of
  – HP OpenView NNM and
  – Standards-based, Secure, Smart Agents

• provides functionality, security, administration, and performance needed to perform integrated management of networks, systems, applications, and services,

• while integrating with your existing management infrastructure.