Manageability Standards and Requirements

From HUIT Architecture Advisory Group

Contents

[hide]

Manageability Standards and Requirements

The information on this page is designed to help software engineers, program managers, and other HUIT operations and administrative staff as they develop, acquire from third parties, and operate systems and their constitutive elements. It includes the following information:

- Types of information that should be available from all the systems, related to fault, configuration, performance and accounting and security information.
- Protocols/access methods and data formats that should be used.
- Logging and log levels based on different operational scenarios.
- Data collection, retention and other policies and analysis related to information collected from the systems.

Types of Information To Collect

Note that these items are to be collected even in steady state operations. Increasing the frequency of data collection or the addition of other objects may be appropriate in those cases where a root cause analysis is ongoing.

Data Collection Policies

The information in the following sections should be thought of as a check list of data elements that should be available in the majority of situations, incuding normal operations, for all systems in our HUIT environment. Systems in third party clouds are, for the purposes of this requirement, in the HUIT environment.

Applicability

In general terms, the information described in this page should be collected if the hardware or software system in question provides the service (e.g., HTTP) or has the resource (e.g, Memory or Disk) identified by the object. The frequency of data collection or reduction is a matter to be refined by the operational team responsible for the technology stack supporting a specific service (e.g., iSites, PIN, PeopleSoft, etc.)

NOTE WELL: It is not the purpose of this page to enumerate in exact detail the objects for each of the services HUIT supports. That function is the responsibility of each of the service-specific teams. The objective here is to list those areas that are of interest and point teams to examples of some of the information types that are useful for each service. Over time, more specific details will be published and folded into the Enterprise Architecture standards requirements relevant to instrumentaiton and monitoring.

Format of the Management Objects

This section describes the requirements for information that must be made available for HUIT Enterprise Architecture compliant systems, not the specifics of how each system will make available the information that is required.

For the moment, some of the information is expressed in SNMP MIB Object Format since it allows for concise and precise expression of the desired data elements. This is primarily for illustrative purposes. Future work will standardize the information formats for specific types of data. Other alternatives are acceptable absent these objects or if there is a compelling alternative.

Not part of this standard is how these data elements must be integrated into the the single management infrastructure to be identified for the service. In some cases other approaches may be preferable, for example using some Puppet functions for some system details and installed software.

Data Elements

Each of the sections below contains information about management objects for collection at a particular layer of the technology stack. For the most part, these are server centric. There is a special section for Network Devices.

Harwdware

See the Host Resources MIB for object descriptions used below.

Note that the hrDeviceTable is a way to get a quick inventory of al the devices in the system such as interfaces, disks, processor(s), errors and current status.

- Disk/storage - information here from the hrStorage table: hrStorageType, hrStorageDescr, hrStorageAllocationUnits, hrStorageSize, hrStorageUsed, and hrStorageAllocationFailures.

Total extents, contiguous extents, block count (health metrics to be furhter specified). Disk information should also include data of the kind found in iostat.

- Memory - hrMemorySize
- CPU - percent utilization per core.
- Network Interfaces - type, capacity etc. The standard SNMP MIB modules. See the ifTable in RFC 2863.

Basic Operating System Data

- OS and process level information from RFC-2790, the Host Resources MIB Module:
  - hrSystemProcesses
  - memory/disk types from the hrStorageTable should be collected
  - hrProcessorLoad
- High-level application/process information can be found in RFC-2287, the Systems Application MIB Module:
- sysApplInstallPkgTable and sysApplInstallElmtTable - the data in this table need only be collected occasionally to verify what software has been installed on a system (this is an example of data that might be collected via other methods, in this case, Puppet might collect some useful information.

    - sysApplElmtRunState
    - sysApplElmtRunName
    - sysApplElmtRunCPU
    - sysApplElmtRunMemory
    - sysApplElmtRunNumFiles - Note this object definition specifically excludes transport connections which means we will have to correlate this information with information from the TCP level described below or collect FD information via other methods.
- File system and I/O data:
    - inodes, percent utilized.
    - FSTAB data
    - iostat
- SAN Connectivity Information

The data in this section also include application layer information like the number of threads used by a particular application which may be comprised of many processes (some in different VMs). It also includes dependencies like connections to Databases, LDAP servers, the number of HTTP connections, etc. It should also include key performance metrics where possible such as latency of connections to dependent resource.

Information in the Communication Stack

- From RFC-4293, the IP MIB Module - note only aggregate vs. interface specific objects are suggested. If data collected suggests issue with a particular interface, data collection for those specifics can be turned on. If the systems we are dealing with do not support the newer table, we can use the per-interface layer stats/ifTable.
    - ipSystemStatsInReceives - whenever a 64 bit alternatives such as ipSystemStatsHCInReceives is available, it is assumed we will collect that instead - that is assumed for all objects.
    - ipSystemStatsInHdrErrors
    - ipSystemsStatsInNoRoutes
    - ipSystemStatsInAddrErrors
    - ipSystemStatsInDiscards
    - ipSystemStatsInDelivers
    - ipSystemStatsOutRequests
    - ipSystemStatsOutTransmits

- From RFC-4022, the MIB Module for TCP. Under normal conditions it is not appropriate to collecte these data. In certain conditions when attempting to diagnose a problem they may be helpful. Please see section 2.1.3 that discusses the correlation of data from this Module with the HOST-RESOURCES and SYSAPPL MIB Modules:
    - tcpMaxConn
    - tcpActiveOpen
    - tcpPassiveOpens
    - tcpAttemptFails
    - tcpEstabResets
    - tcpCurrEstab
    - tcpInErrs
    - tcpOutRsts

- From RFC-4311, the UDP MIB, the elements from the udpBaseGroup and udpEdpointGroup (along with HC elements where appropriate) should be collected.

Monitoring JVMs

The Sun JVM included SNMP instrumentation from 1.5 forward. Oracle has incorporated documentation for that environment. This extensive set of instrumentation contains notifications for low memory and objects for heap and memory and other indicators that could be helpful. Please see this blog entry for suggested objects for collection and graphing.

LDAP

Depending on the supplier of the LDAP server, there are a number of insrumentation alternatives. There are some standard RFCs that

describe common attributes. The LDAP 389 server has a complete MIB Module posted on GitHub that comes with the redhat distribution. It includes key operational statistics aswell as notificaitons on server failure and restart.

Relational Technology

Databases are at the center of many of our applications and information about their status is critical to all areas of management. Since there are a number of database technologies used, there may be more than one information format. In this section as in others SNMP is used as a common form. As is the case with many different technologies, different vendors will put their own 'twist' on insturmentation even when it has been standardized. Where we can we should encourage vendors to support the common standards and add where necessary. In other cases HUIT will have no choice but to integrate proprietary objects and protocols.

In the case of Oracle, they have a fairly complete documentation. For example, this page points to support for 11g. There are good online resources that can be used - in addition to those at the oracle site, to learn what instrumentation is available.

In the case of MySql, there is also a complete set of information. The MIB Documents are on GitHub. The example here if for the main server. There are additional modules available for other aspects of MySql technolgoy including Clusters.

MIddleware

As with other elements in our technology stack, middleware/J2EE are represented by multiple implementations. Oracle has extensive documentaiton on the SNMP agent they support for WebLogic.

J2EE (e..g., WebLogic/JBOSS) Tomcat

Web Server

Time/NTP

Time if fundamental to many of the systems HUIT operates. Instrumentation of NTP and monitoring specific aspects of its behavior can help detect problems before systems fail. It is recommended that all systems/servers support RFC 5907. Which specific objects are appropriate depend on the function of the server in question.

Environmental Monitoring

- Temperature
- Humidity
- Power
- HVAC

Network Infrastructure Specific Data Elements

The items in this section are for data elements specific to our communictions infrastructure such as routers, firewalls, load balancers etc. Most of the requirements for hardware and basic performance data are the same as identified in the server-centric section above. Specific variations and additional requirements for objects comprise the lists that follow unless otherwise noted. The following list is from Ooi and is included for completeness, we have to reformat this:

```
-Firewall Monitoring
Hardware/Software Type
Hardware cpu/memory usage
Hardware power and environmental
Port bandwidth/capacity usage
Fail Over/High Availability status
Management Access Frequency and Total Sessions
Routing table changes
Port bandwidth usage (b/s or /pps)
Syslog rate
Connection rate
App inspection rate
Total number of connections
Total number of translations
Top applications/ports
```

```
Total hosts
Embryonic connections
Bad traffic stats (illegitimate packets)
Capacity Breach (e.g. Max connection per client)

Routing/Switching
Hardware/Software Type
Hardware cpu/memory usage
Hardware power and environmental
Failover/High Availability status
Port bandwidth/capacity/broadcast/link error
Total flows
Local Routing protocol/spanning tree instances
Spanning tree root
Number of per routing process/spanning tree neighbors
Total prefixes of each routing instance
Per neighbor routing prefixes sent/received
Total number of mac addresses for each vlan
Internal vs external route type counts
Change of routing protocol's neighbors status
Routing/Spanning Tree convergence or topology change

Router/switch monitoring miscellaneous
Breach of monitoring thresholds (e.g.dhcp snooping, total mac address per port, broadcast suppression…and etc)

Router/switch monitoring through snmp trap

rivergw1#
snmp-server enable traps snmp authentication linkdown linkup coldstart warm start
snmp-server enable traps c6kxbar intbus-crcexcd intbus-crcrcvrd swbus
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps memory buffer peak
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vlan-mac-limit
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bgp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
….

-Firewall monitoring through SSH

scox60wrlsfw1# sh resource usage
Resource               Current        Peak      Limit        Denied Context
SSH                          2           4          5             0 System
Syslogs [rate]             122       28668        N/A             0 System
Conns                   387405      686011    4000000             0 System
Xlates                  398038      689936        N/A             0 System
Hosts                   111031      218245        N/A             0 System
Conns [rate]              3009       38896        N/A             0 System
Inspects [rate]           1008        6410        N/A             0 System


Wireless Network Monitoring
802.11a/g/n radio usage
breakdown of end device type and count
total AP on the per building/subregion/region/wireless controller
total wireless clients on the per AP/SSID/building/subregion/region/wireless controller and the combinations
unique client count on the per SSID/AP/building/sub-region/region/wireless controller
bandwidth usage per SSID/AP/switch/sub-region/region/controller/fw
auth/deauth, association/dis-association, probes rates threshold breach
Rogue AP summary
Coverage hole alerts

Load Balancer Monitoring
Stats and threshold breach on the below parameters on the per user/lb context/VIP/serverfarm/application/server that have relevance:

Failover/HA status
concurrent connections
mgmt connections
proxy-connections
xlates
bandwidth
throughput
mgmt-traffic rate
```

```
connections rate
ssl-connections rate
inspect-conn rate
acl-memory
sticky
regexp
syslog buffer
syslog rate
Application end-to-end probes
Bad traffic (e.g. buffer overflow)
SSL expiration
```

Protocols/Access Methods and Data Formats

Logging and Log Levels

Data Collection, Retention and Analyses

Events and Alarms

This section applies to the events and alarms that a managed device might send to one or more management systems.