Management Information Base for Virtual Machines Controlled by a Hypervisor

draft-ietf-opsawg-vmm-mib-01

H. Asai, M. MacFaden,

J. Schoenwaelder, K. Shima, T. Tsou

OPSA WG, IETF 90 @Toronto, ON, Canada

July 23, 2014

VM-MIB: MIB objects related to virtual machines controlled by a hypervisor

- Objects
  - Hypervisor software information
  - Virtual machine list (info, config and stats)
  - Virtual resources (info, config, and stats) allocated to each virtual machine
    - Virtual CPU, Virtual memory, Virtual storage, Virtual network interface
- VMM-MIB objects are managed at a hypervisor
  - e.g., An SNMP agent implementing VMM-MIB is to be installed in a hypervisor, not in each virtual machine.

Update from -00

- Read-write to read-only access to fit the IESG statement
  - Changed from read-write to read-only
    - vmAdminState
    - vmCurCpuNumber
    - vmMinCpuNumber
    - vmMaxCpuNumber
    - vmCurMem
    - vmMinMem
    - vmMaxMem
    - vmCpuAffinity
  - Remain read-write
    - vmPerVMNotificationsEnabled
    - vmBulkNotificationsEnabled
  - *(js's comment: From an SMIv2 perspective, it is odd that the MAX-ACCESS of some of the objects has been changed from read-write to read-only but it seems the "political climate" overrules what MAX-ACCESS used to mean in STD 58.)*
- Description on two read-write objects (but need to be modified)
  - "Changes to this object MUST NOT persist across re-initialization of the management system, e.g., SNMP agent."

Active discussions (will be updated in -02)

- Read-write objects
    - vmPerVMNotificationsEnabled
    - vmBulkNotificationsEnabled
  - Changes suggested in M
    - OLD
      - Changes to this object MUST NOT persist across re-initialization of the management system, e.g., SNMP agent.
    - NEW
      - Changes to this object may be lost when the management system, e.g., SNMP agent, is re-initialized.
    - Add text more?
      - Mike's comment: We could add text to explain that any design that is 100% reliant on notifications as the sole means of maintaining distributed state is a failed design to begin with. notification only designs must be bounded either by poll or reverse poll/periodic event to detect a failure to receive notifications regardless of what caused the failure.
- Security considerations
  - OLD
    - When SNMPv3 strong security is not used, these objects should have access of read-only, not read-write.
  - NEW
    - When SNMPv3 strong security is not used, the access control model (e.g., the View-based Access Control Model [RFC3415]) should be configured to disallow write access.
    - It is recommended that default access control configurations shipped with an implementation exclude write access to these objects.