SNMP

Introduction to SNMP and MIB

Simple Network Management Protocol (SNMP) is a UDP-based network protocol used mostly in network management systems to monitor network-attached devices. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force(IETF) and consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems that describe the system configuration. These variables can be queried using SNMP management applications.

SNMP allows a Network Management Station to do the following:

- Poll a device for info or to trend data i.e. Cisco Unified Communications Domain Manager 10.6(1) server load graph via HOST-SYSTEMS-MIB
- Receive notifications in the form of traps or informs in response to events, threshold violations, whatever the trap definitions in the loaded MIBs are. We enable process monitoring and disk space checks - when triggered, these send out a trap.

A management information base (MIB) is a form of virtual database used for managing the entities in a communications network. Working closely with SNMP, the hierarchical data structure describes all of the objects that a device can report the status of.

The MIB is structured based on the RFC 1155 standard. This standard defines how the MIB information is organized, what data types are allowed and how resources within the MIB are named. Each MIB contains the name, object identifier (a numeral), data type and the permissions relating to whether the value can be read or written to. The top hierarchies of the MIB are fixed; however, certain sub trees can be defined by product vendors and other organizations.

The variables within MIB are named using the Abstract Syntax Notation 1 (ASN.1). This is an international standard for representing data.

SNMP Terminology:

- MIB: The term MIB is used to refer to the complete collection of management information available on an entity, while MIB subsets are referred to as MIB-modules.
- NMS: ANetwork Management System is a combination of hardware and software used to monitor and administer a network and the devices associated with that network.

Configuration

SNMP on Cisco Unified Communications Domain Manager 10.6(1) is configured after initial system setup. The following SNMP parameters can be configured.

- SNMP integration

  Enable SNMP functionality. If this setting is disabled, the other SNMP parameters will not be displayed for configuration.

- SNMP system name

  The SNMP system name identifies the system being monitored on the NMS (Network Management System). Defaults to nodename.domainname.

- SNMP system location

  The SNMP system location describes the location of the system. Defaults to Unknown.

- SNMP system contact

  The SNMP system contact defines the email address of administrator responsible for the system. Defaults to None.

- SNMP query source

  CIDR-style IP (e.g. 196.0.0.0/8) network allowed to query SNMP from this host. This is used to limit the hosts allowed to manage the system via SNMP. Defaults to all hosts.

- SNMP load triggers

  The 1, 5 and 15 minute load averages that will trigger warnings via SNMP. Defaults to values dynamically calculated from the number of CPUs in the system. This should be formatted as 8n/4n/2n (where n represents the number of processors available) when entered into the configuration wizard during setup.

- SNMP trap destination

  This is the destination to which SNMP traps will be sent. Formatted as *destination[/community[/port]]* where both community and port are optional, but port may not be specified unless community is specified too.

- SNMP inform destination

  Inform events are similar to traps, except that they are acknowledged at the network layer to ensure delivery of the event notification. Formatted as destination[/community[/port]] where both community and port are optional, but port may not be specified unless community is specified too. It is generally preferable that SNMPv2 trap destinations are used instead, while leaving this field blank.

SNMP Traps

When the managed system generates certain events, it will forward a SNMP trap. The reason for the event trap is contained in the SNMP MIB string. Note that if the corresponding SNMP MIB is not loaded on the NMS, a numerical representation of the SNMP entry is provided. The list of monitored events is described in the SNMP Trap section below. A detailed breakdown of each SNMP trap type is provided in the appendix.

The SNMP will send traps to the trap destination configured. If the trap destination is incorrect or not configured, the NMS will not receive the traps.

The following system parameters are monitored by default:

- Disk Space: warnings are issued if the file system becomes full
- System Load Monitoring: warnings are issued if the system load is excessive (the system load parameters can be defined during configuration)
- SNMP: standard SNMP System Events, for example, Cold Start
- Process state changes: Informative messages are sent to the NMS indicating that processes have been restarted.

In general, the originator of the SNMP traps is determined by originating hostname / IP address. Many Network Management Systems provide trap management and escalation per system being managed, including identification based on system name, location and contact details. Those events monitored directly by Cisco Unified Communications Domain Manager 10.6(1) (e.g. disk space, system load and process warnings) include the system name as part of the variable bindings to assist identification of the originating system.

Disk Space Low [High Priority]

- Priority: HIGH
- Action: Call support

SNMP monitors the percentage of free space available, and will raise a trap if the filesystem becomes full. By default, the threshold is 10% free space available. The filesystem is used to store log files, etc. and under normal conditions will recycle these to ensure that disk space is managed. If a disk space low warning is received, it should be treated as a high priority, customer support should be contacted to determine the reason for the filesystem becoming full.

Excessive Load [Medium Priority]

- Priority: Medium
- Action: Monitor for short-term spikes (e.g. 1 and 5 minute intervals)
- Action: Escalate to support if excessive load average reported over 15 minute intervals.

During configuration, the maximum load can be specified as an average over 1minute, 5minute and 15minute intervals. The system load may spike during certain activities such as bulk loading and will recover. The warning should only be treated as serious if the system load is high for an extended period (e.g. over a 10 minute average).

The load can be monitored either on the NMS for further excessive load traps, or via the command line interface (documented in the Command line interface guide) using the status and healthlog commands.

If the 15-minute threshold is exceeded, diagnosis is required to determine the cause of the high load. Ensure that sufficient CPU and Memory resources are available to the Cisco Unified Communications Domain Manager 10.6(1) system as per the initial hardware scaling requirements. The problem may also be caused by incidents such as network outages, delayed backups, manual intervention by a system administration, etc. Please contact support for further diagnosis of the problem.

Process State Changes [Medium Priority]

- Priority: Medium
- Action: Monitor

Process state changes (e.g., restart of services) are normal behavior when the Cisco Unified Communications Domain Manager 10.6(1) system is started or shutdown. Manual intervention by a system administrator is also likely to cause services to start or stop. The system manages processes automatically and will restart services as required. Process state changes are normal during HA (cluster failover).

The state of processes can be monitored either on the NMS for subsequent process state change traps, or via the command line interface (documented in the Command line interface guide) using the monitor command.

Check if there is a known outage, change control window, or scheduled work in progress for this platform. If there is none, then these traps represent a high priority issue and need to be logged with support.

Standard SNMP Events [Low Priority]

- Priority: Low
- Action: Monitor

Standard SNMP traps for cold-start and shutdown are generated by the Cisco Unified Communications Domain Manager 10.6(1) system when it is started or shutdown. Manual intervention by a system administrator may also generate these traps if the system is restarted. Cold-start notices may also indicate HA (cluster failover).

The state of the Cisco Unified Communications Domain Manager 10.6(1) system can be monitored either on the NMS for subsequent cold-start traps, or via the command line interface (CLI) using the monitor and healthlog commands.

Check if there is a known outage, change control window, or scheduled work in progress for this platform. If there is none, then these traps represent a high priority issue and need to be logged with support.

Reconfigure SNMP

SNMP configuration settings can be managed from the CLI. Refer to the CLI **notify** command:

```
platform@development:~$ notify
USAGE:
------
notify add [info|warn|error]       - Add the email or snmp URI to a
   <email/snmp-uri> ...                specified notification level.
```

SNMP must be configured under the SNMP menu and the SNMP URI needs to be configured for all the notify severity levels(info|warn|error]).

SNMP URI usage:

- snmpv2: snmp://community@host[:port]
- snmpv3: snmp://user:auth:password]@host[:port] ... minimum auth/password length is 8 characters.

For example:

- snmpv2: notify add info snmp://public@1.2.3.4

- snmpv3: notify add error snmp://public:publicauth:password@1.2.3.4

The following options can be configured under the SNMP menu in the CLI.

- Enabled -Enable or disable SNMP Queries
- Community- SNMP v2c Community String used to query this server
- Authorized Username - SNMP v3 Username to query this server
- Password - SNMP v3 Password to query this server
- Query - IP address that is allowed to query this server
- Sysname - Name of this server, as it will appear when queried via SNMP
- Syslocation - Location of this server
- Syscontact - Contact person(s) for this server (email address)
- Load1 - 1 Minute load average alarm value
- Load5 - 5 Minute load average alarm value
- Load15 - 15 Minute load average alarm value

Two SNMP Trap destinations can be configured:

The following options can be configured in the CLI:

- Hostname - Server name to send SNMP traps to.
- Version - Version of SNMP to use for sending trap, version 2c or 3.
- Community - refer to the SNMP-URI command usage.
- Mode - Send Trap or Inform message.
- Username - refer to the SNMP-URI command usage.
- Password - refer to the SNMP-URI command usage.
- Encryption - refer to the SNMP-URI command usage.
- Engineid - To send traps as. - Currently not implemented

Management Information Bases

SNMP information is grouped together in Management Information Bases (MIBs). The MIBs loaded on the Cisco Unified Communications Domain Manager 10.6(1) system represent all the configuration/data items that can be queried or be used to generate traps (notifications) when certain events occur. A list of all MIBs loaded on the system is provided below.

In order to manage the system, a Network Management System (NMS) should be installed at the customer site (e.g. HP OpenView, iReasoningMib Browser). The NMS should be loaded with the same set of MIBs as those installed on the system. The NMS should be configured to send SNMP queries to the managed host (i.e. correct IP address, port number (default 161), community string (default public), and version (default version 2c). Further, the NMS should be configured to receive traps from the managed host - the correct IP, port number (default 162), version (default version 2), and community strings (default public) should be provided).

SNMP items can be selected in the MIBs and the item queried on the remote managed system. The remote system will return a response to the MIB entry being queried. For example, if the following entry is queried (.1.3.6.1.2.1.1.5.0 alias '.iso.org.dod.internet.mgmt.mib-2.system.sysName.0'), the system will return the system name that was assigned during setup (e.g. sysName.0 'Voss Node00'). Note that if any of the configured details on the NMS are incorrect, it is likely that the query will never reach the managed host and no response will be received. Please ensure that version 2 is selected with the correct community string (default public).

When the managed system generates certain events, it will forward a SNMP trap. The reason for the event trap is contained in the SNMP MIB string. Note that if the corresponding SNMP MIB is not loaded on the NMS, a numerical representation of the SNMP entry is provided. The list of monitored events is described in the SNMP Trap section below.

Refer to the MIB List at the end of this document for the list of net-SNMP packages that ship with Cisco Unified Communications Domain Manager 10.6(1).

MIB and Trap Details

SNMPv2-MIB - RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

Basic information about SNMP on the entity. Includes:

- sysDescr: A text description of the entity
- sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity.
- sysUpTime: The time since the network management portion of the system was last re-initialised.

Note sysUpTime indicates how long the SNMP software has been running on the box, and not how long the box itself has been up (this is a common misconception).

- Counters for SNMP requests and responses.

IF-MIB - RFC 2863 - The Interfaces Group MIB

Describes the network interfaces on the entity. For each interface the following information is given:

- ifType: The type of interface
- ifMtu: Size of the largest packet which can be sent/received on the interface
- ifSpeed: An estimate of the interface's current bandwidth
- ifPhysAddress: The interface's address at its protocol sub-layer. For 802.x interfaces, this is the MAC address
- The administrative and operational state of the interface

- The number of octets and packets sent and received on the interface

MIB-II - RFC 1213 - Management Information Base for Network Management of TCP/IP- based internets

TCP/IP network information not covered by the other MIBs, split into a number of groups:

- Address translation group:
  - atPhysAddress: The media-dependent physical address
  - atNetAddress: The network address (IP address) corresponding to the physical address
- IP group:
  - ipRouteTable: IP routing table, contains an entry for each route presently known to this entity

IP-MIB - RFC 4293 - Management Information Base for the Internet Protocol (IP)

Internet Protocol information:

- Counters for IP packets sent and received
- For each IP address:
  - The IP address
  - Index of the physical interface (in the IF-MIB)
  - Netmask
  - ICMP counters

TCP-MIB - RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP)

TCP information:

- Retransmission timeout information
- Overall counters for number of inbound and outbound connections
- For each current connection:
  - Connection state
  - Local and remote IP addresses and TCP port numbers

UDP-MIB - RFC 4113 - Management Information Base for the User Datagram Protocol (UDP)

UDP information:

- Counters for datagrams sent and received
- Local IP addresses and UDP port numbers

HOST-RESOURCES-MIB - RFC 2790 - Management Information Base for Host Resources

Objects useful for the management of host computers. These are split into a number of groups:

- System Group
  - hrSystemUptime: Amount of time since the host was last initialized (note this is different from sysUpTime).
  - hrSystemDate: The host's notion of the local date and time of day
  - hrSystemProcesses: The number of process contexts currently loaded or running on this system
- Storage Group
  - hrMemorySize: The amount of physical read-write main memory, typically RAM, contained by the host
  - For each storage device:
    - hrStorageType: The type of storage (RAM, fixed disk etc.)
    - hrStorageDescr: A description of the storage (Swap Space, mount point etc.)
    - Size of storage units, number available and number used
- Device Group
  - For each device:
    - Type (processor, network, disk, printer etc.)
    - Description
  - For each disk storage device:
    - Access (read-write, read-only)
    - Fixed/removable
    - Capacity
  - For each disk partition:

        - Label
    - For each file system:
        - Mount point
        - Type
        - Access (read-write, read-only)
        - Bootable
- Running Software Group
    - For each running process:
        - Name
        - Path
        - Parameters
        - Status
    - Running Software Performance Group for each running process:
        - CPU resources consumed by this process
        - Amount of real system memory allocated to this process

SNMP Traps: System Startup

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- alarms and escalation to the relevant system operator
- .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.coldStart

Trap OID

.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.coldStart

Variable Bindings

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 190 milliseconds (19)
- snmpTrapOID = coldStart
- .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapEnterprise.0= linux

SNMP Traps: Service Startup Changes Made

The following events are generated at startup indicative of the various services changing state:

```
SNMP 1.3.6.1.2.1.88.2.0.1
2014-07-04   15:40:30       <server_IP>   [UDP:  [<server_IP>]:56005->[<snmp_server_IP>]]:
iso.3.6.1.2.1.1.3.0 = Timeticks:   (8785393) 1 day, 0:24:13.93 iso.3.6.1.6.3.1.1.4.1.0 =
OID:
iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: “ProcessRestart”
iso.3.6.1.2.1.88.2.1.3.0
= STRING: <resource> iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1 iso.3.6.1.2.1.1.5.0 = STRING:
“<hostname>
“
```

where<resource> is one of the following:

- voss-deviceapi: voss-wsgi
- voss-deviceapi: voss-notifications
- voss-deviceapi: voss-queue
- mongodb:router
- mongodb:config
- mongodb:arbiter
- mongodb:database
- snmp:daemon
- snmp:traps
- nginx:proxy
- services:wsgi
- services:logs
- services:firewall
- services:mount
- services:time
- services:syslog

SNMP Traps: Service Monitoring - Changes Made

For each of the services listed above, the system will monitor the process and restart as necessary.

When the service shuts down, it sends a trap indicating a resource stopped in the following format:

```
.       2014-07-04   15:40:30  <server_IP> [UDP: [<server_IP>]:56005->[<snmp_server_IP>]]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (8785393) 1 day, 0:24:13.93 iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: “ProcessStop”
iso.3.6.1.2.1.88.2.1.3.0 =
STRING: <resource> iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1 iso.3.6.1.2.1.1.5.0 = STRING:
“<hostname>
“
```

Service restart is indicated by the following:

```
2014-07-04       15:40:30   <server_IP>  [UDP:   [<server_IP>]:56005->[<snmp_server_IP>]]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (8785393) 1 day, 0:24:13.93 iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: “ProcessRestart”
iso.3.6.1.2.1.88.2.1.3.0
= STRING: <resource> iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1 iso.3.6.1.2.1.1.5.0 = STRING:
“<hostname>
“
```

SNMP Traps: System Shutdown

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID can be used to identify the cause of the SNMP trap
- .iso.org.dod.internet.private.enterprises.netSnmp.netSnmpNotificationPrefix.netSnmpNotifications.nsNotifyShutdown

Trap OID

.iso.org.dod.internet.private.enterprises.netSnmp.netSnmpNotificationPrefix.netSnmpNotifications.nsNotifyShutdown

Variable Bindings

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 44 seconds (4414) snmpTrapOID =
nsNotifyShutdown
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapEnterprise.0
= netSnmpNotificationPrefix
```

SNMP Trap: Disk Full

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`
- The following variable binding can be used to determine that a disk partition is full.
  - `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Disk full`

- The following variable binding can be used to further diagnose the extent of the filesystem that has become full
    - `.iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskErrorMsg.1 = /: less than 75% free (= 26%)`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Disk full.`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotTargetName.0 =`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotContextName.0 =`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotOID.0 = dskErrorFlag.1`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotValue.0 =1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`
- `.iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPath.1 = /`
- `.iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskErrorMsg.1 = /: less than 75% free (= 26%)`

SNMP Trap: Excessive Load

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

- The following variable binding can be used to determine that the load average threshold has been exceeded.
  - .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Excessive load.
- The following variable binding can be used to further diagnose which time interval threshold has been exceeded
  - .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laNames.<LoadIdx> = <LoadError>
  - .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laErrMessage.<LoadIdx> = <LoadMessage>

Load average interval	<LoadIdx>	<LoadError>	<LoadMessage>
1 minute	1	Load-1	1 min Load Average too high (= 2.52)
5 minute	2	Load-5	5 min Load Average too high (= 1.27)
15 minute	3	Load-15	15 min Load Average too high (= 1.27)

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Excessive load.
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotTargetName.0 =
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotContextName.0 =
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotOID.0 = laErrorFlag.1
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

- .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laNames.1 = Load-1
- .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laErrMessage.1 = 1 min Load Average too high (= 1.36)

SNMP Trap: Backup

A trap is generated on every backup.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - successful backup

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = “backup completed”
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 0
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Variable Bindings - failed backup

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = “backup failed”
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 5
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Health Emails

A trap is generated if health email send fail to be generated.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Trouble sending health email'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: Disk Latency

A trap is generated when the disk appears to be slow.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - Disk slow

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Disk slow'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Mailbox Status

A trap is generated when the local mailbox reaches 200 plus emails.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
disman-EventMIBNotifications.mteTriggerFired

Variable Bindings - Mailbox email messages reach 200

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: The total messages in
  the local mailbox for %s has reached in excess of 200'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1

- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Variable Bindings - Mailbox email messages reach 500

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- SnmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'INFO: Messages for <server info> auto archived as it reached more than 500'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Cluster Status

A trap is generated when one or more nodes are down in a cluster.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - One or more nodes are down in the cluster

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: One or more nodes are down in the cluster'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Database Failover Status

A trap is generated when one or more nodes are down in a cluster.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the Cisco Unified Communications Domain Manager 10.6(1) system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.`
`dismanEvent-MIBNotifications.mteTriggerFired Variable Bindings - db constantly fails over`

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: The db is failing over constantly within 5 min'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: Large Log Files

A trap is generated when large log files are detected in /var/log/.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings - large log files detected

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Log files larger than 1Gig found in /var/log'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: Network Status

A trap is generated when a network failures occur.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings - Network failures

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Network Failures'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`

- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Security Updates

A trap is generated when security updates are available.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - Security updates availabe.

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: Security Updates available'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Memory Usage

A trap is generated for high memory usage.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:

- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - High memory usage

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: High memory usage'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Variable Bindings - Extremely high CPU usage

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Extremely high CPU usage'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: NTP Status

A trap is generated if NTP is not configured.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings - NTP not configured

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: No ntp configured for <server info>'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: DNS status

A trap is generated if DNS is not configured.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
    - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

Trap OID

`.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEvent-MIBNotifications.mteTriggerFired`

Variable Bindings - DNS not configured

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: No dns configured for <server info>'`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1`

- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Domain Status

A trap is generated if the domain is not configured.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - Domain not configured

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: No domain configured for
  <server info>'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: NTP Offset

A trap is generated when the NTP offset exceeds 1 second.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system

- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotifications.
mteTriggerFired Variable Bindings - NTP exceeds 1 second. *
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065) * snmpTrapOID =
mteTriggerFired
* .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.
mteHotTrigger.0 = 'WARNING: The ntp offset exceeds 1 second on
<server info>' *
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.mteHotValue.0 = 1 * .iso.org.dod.internet.mgmt.mib-
2.system.sysName.0 = standalone
```

SNMP Trap: Process Memory Threshold Status

A trap is generated when the a process memory exceeds its current threshold.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. dismanEvent-
MIBNotifications.mteTriggerFired
```

Variable Bindings - Process exceeds memory threshold

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-
  EventMIBNotificationObjects.mteHotTrigger.0 = '<process name: mem_<name> exceeded maxi-
  mum value of current_threshold with current_reading>'
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix. disman-
  EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone