SNMP Support for Cisco Unified Communications Domain Manager 8.1.4

First Published: October 29, 2014
Last Modified: October 29, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

SNMP Support for Cisco Unified Communications Domain Manager 8.1.4

Contents

Overview

This document is aimed at internal system engineers and advanced system engineers and administrators who will be required to manage and configure a CUCDM server.

This system supports various deployments/solutions including HCS and Large Enterprise (LE). This document describes the product in general and is not specific to a particular deployment/solution. Information may vary slightly depending on the installation environment.

Typographic Conventions

The following typographic conventions are used in this document:

Item	Character format	Example
Buttons	**Bold**	Click the **Enter** button.
Checkboxes	*italic*	Select the *Country* checkbox.
Dialog boxes menu items, tab names, radio buttons	*italic*	Select the *Configuration* option, or select the *Parameters* tab.

CHAPTER 1

Introduction to SNMP

What is SNMP?

Simple Network Management Protocol(SNMP) is a UDP[1]-based network protocol used mostly in network management systems[2] to monitor[3] network-attached devices. SNMP is a component of the Internet Protocol Suite[4] as defined by the Internet Engineering Task Force[5] (IETF) and consists of a set of standards[6] for network management, including an application layer[7] protocol[8], a database schema[9] and a set of data objects[10].

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 information or to trend data i.e. CUCDM server load graph via HOST-SYSTEMS-MIB
- Receive notifications in the form of traps or informs in response to events, threshold violations, and other trap definitions that are in the MIBs. Process monitoring and disk space checks are enabled. When triggered, these send out a trap.

What are MIBS?

A management information base (MIB) is a form of virtual database used for managing the entities in a communications network. Working closely with SNMP[11], 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[12] 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

[1] http://en.wikipedia.org/wiki/User_Datagram_Protocol
[2] http://en.wikipedia.org/wiki/Network_management_systems
[3] http://en.wikipedia.org/wiki/Network_monitoring
[4] http://en.wikipedia.org/wiki/Internet_Protocol_Suite
[5] http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force
[6] http://en.wikipedia.org/wiki/Standards
[7] http://en.wikipedia.org/wiki/Application_layer
[8] http://en.wikipedia.org/wiki/Protocol_(computing)
[9] http://en.wikipedia.org/wiki/Logical_schema
[10] http://en.wikipedia.org/wiki/Data_object
[11] http://www.networkworld.com/details/748.html
[12] http://www.ietf.org/rfc/rfc1155.txt

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:**A Network Management System is a combination of hardware[13] and software[14] used to monitor and administer a network[15] and the devices associated with that network.

Configuration

SNMP on Platform 4 is configured via the wizard during 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). This defaults to `nodename.domainname'.

- SNMP system location

  The SNMP system location describes the location of the system. This defaults to `Unknown'.

- SNMP system contact

  The SNMP system contact defines the email address of administrator responsible for the system.

- 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. This defaults to all hosts.

- SNMP load triggers

  The 1, 5 and 15 minute load averages that will trigger warnings via SNMP. This 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

[13] http://en.wikipedia.org/wiki/Computer_hardware
[14] http://en.wikipedia.org/wiki/Software
[15] http://en.wikipedia.org/wiki/Computer_network

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.

An example of the configuration file is provided in the appendix.

CHAPTER 2

Management Information Bases

SNMP information is grouped together in Management Information Bases (MIBs). The MIBs loaded on CUCDM 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 CUCDM is provided below.

In order to manage CUCDM, 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 CUCDM. 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 CUCDM returns the CUCDM name that was assigned during setup (e.g. sysName.0 "CUCDM 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).

Note

SNMP version 3 and SNMP writes are not supported at present.

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.

MIBs

CUCDM uses standard MIBs that are usually deployed as part of a Network Management System (NMS). Specific MIBs can be downloaded from http://www.mibsearch.com[1]

Contact support for a download of the complete archive of MIBs used.

The default net-SNMP packages that ship with CUCDM include:

- AGENTX-MIB.txt
- DISMAN-EVENT-MIB.txt

[1] http://www.mibsearch.com/

- DISMAN-SCHEDULE-MIB.txt
- DISMAN-SCRIPT-MIB.txt
- EtherLike-MIB.txt
- HCNUM-TC.txt
- HOST-RESOURCES-MIB.txt
- HOST-RESOURCES-TYPES.txt
- IANA-ADDRESS-FAMILY-NUMBERS-MIB.txt
- IANAifType-MIB.txt
- IANA-LANGUAGE-MIB.txt
- IANA-RTPROTO-MIB.txt
- IF-INVERTED-STACK-MIB.txt
- IF-MIB.txt
- INET-ADDRESS-MIB.txt
- IP-FORWARD-MIB.txt
- IP-MIB.txt
- IPV6-ICMP-MIB.txt
- IPV6-MIB.txt
- IPV6-TCP-MIB.txt
- IPV6-TC.txt
- IPV6-UDP-MIB.txt
- NET-SNMP-AGENT-MIB.txt
- NET-SNMP-EXAMPLES-MIB.txt
- NET-SNMP-EXTEND-MIB.txt
- NET-SNMP-MIB.txt
- NET-SNMP-TC.txt
- NET-SNMP-VACM-MIB.txt
- NOTIFICATION-LOG-MIB.txt
- PCMK-MIB.txt
- RFC1155-SMI.txt
- RFC1213-MIB.txt
- RFC-1215.txt
- RMON-MIB.txt
- SCTP-MIB.txt
- SMUX-MIB.txt
- SNMP-COMMUNITY-MIB.txt

- SNMP-FRAMEWORK-MIB.txt
- SNMP-MPD-MIB.txt
- SNMP-NOTIFICATION-MIB.txt
- SNMP-PROXY-MIB.txt
- SNMP-TARGET-MIB.txt
- SNMP-USER-BASED-SM-MIB.txt
- SNMP-USM-AES-MIB.txt
- SNMP-USM-DH-OBJECTS-MIB.txt
- SNMPv2-CONF.txt
- SNMPv2-MIB.txt
- SNMPv2-SMI.txt
- SNMPv2-TC.txt
- SNMPv2-TM.txt
- SNMP-VIEW-BASED-ACM-MIB.txt
- TCP-MIB.txt
- TRANSPORT-ADDRESS-MIB.txt
- UCD-DEMO-MIB.txt
- UCD-DISKIO-MIB.txt
- UCD-DLMOD-MIB.txt
- UCD-IPFWACC-MIB.txt
- UCD-SNMP-MIB.txt
- UDP-MIB.txt
- LM-SENSORS-MIB.txt

For further info on how to add a MIB, see: http://www.net-snmp.org/wiki/index.php/TUT:Using_and_loading_MIBS

CHAPTER 3

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.

Note

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.
- **Log generation**warnings are issued if the system is unable to deliver scheduled health and performance logs
- **Backup failure**warnings are issued if the system is unable to complete scheduled backups successfully
- **Synchronization failure**warnings are issued if the system is unable to synchronize the Primary database and filesystem to the DR Standby host

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 CUCDM (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 CUCDM-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 CUCDM-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 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 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 also normal during HA or DR 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 when the system 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 or DR failover.

The state of the system can be monitored either on the NMS for subsequent cold-start traps, or via the command line interface (documented in the Command Line Interface guide) 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.

Log generation [Low Priority]

- Priority: Low
- Action: Monitor

If health and performance logs are scheduled to be delivered (via email, or file transfer), SNMP traps will be generated if the logs cannot be generated or delivered.

The non-delivery of health reports does not necessarily represent a critical problem on the server, but possible causes should be examined. In particular, run the 'health' report from the CLI to check the system status, including whether the disk is full

Backup failure [High Priority]

- Priority: HIGH
- Action: Attempt to diagnose fault and escalate to Support if necessary

Backups are vital to assure the ability to roll-back the database in all eventualities. Backups can be scheduled by the system automatically, including delivery off-site of the backups.

Should these backups fail to be generated or delivered, a SNMP trap is delivered to the NMS. These SNMP traps should be treated as a high priority and corrective action taken to diagnose and fix the problem.

In many cases, the problem may simply be that the backup volume is full (i.e. too many previous copies are kept). Either reduce the number of backup copies, or add a larger backup volume. The current disk status can be checked via the 'health' function in the CLI.

Alternatively, the problem may be that the backup cannot be copied to the remote destination. Check the configured destination with the `test` function in the Destinations menu on the CLI.

If the problem cannot be diagnosed, please escalate to Support.

Synchronization failure [High Priority]

- Priority: HIGH

- Action: Attempt to diagnose fault and resynchronize

In a Disaster Recovery deployment, the Primary system performs continual synchronization to the Standby system. Should the Primary system fail, the Standby system is expected to be in sync such that it can take over services with minimal impact.

Synchronization takes the form of filesystem and database updates being transfered to the Standby system. There are seperate SNMP traps for each: `SyncSharedFS` and `SyncDRfailed` respectively.

The current state of synchronization can be checked using the `state` in the DR menu on the CLI. Usually the system should be synchronized, however during bulkloads and heavy transaction usage, it is normal if the Standby system lags behind the Primary system. However if the system reports that it is unable to communicate with the remote host, check network connectivity and IP configuration. Synchronization may also fail if the communication keys are not valid - the `exchange_keys` can be used to recover this situation.

It is possible that the systems may lose synchronization if either system disk is full, or the Primary system outperforms the Standby system with new transactions for a long period of time. The two databases can be resynchronized by running the `sync` command from the DR menu.

If the problem cannot be diagnosed, please escalate to Support.

CHAPTER 4

Reconfigure SNMP

SNMP configuration settings can be managed from the USMCLI. For details on how to access and use the USMCLI see the CUCDM Command Line Interface guide.

The following options can be configured in the USMCLI.

- Enabled -Enable or disable SNMP Queries
- Community- SNMP v2c Community String used to query this server
- Username - SNMP v3 Username to query this server
- Password - SNMP v3 Password to query this server
- Query_source - IP address that is allowed to query this server

  For example: set query_source <IP_Address_of_PC4HCS_IM> (where IP_Address_of_PC4HCS_IM is the IP address of the PC4HCS Infrastructure Monitoring 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 USMCLI:

- Hostname - Server name to send SNMP traps to.
- Version - Version of SNMP to use for sending trap, version 2c or 3.
- Community - SNMP V2c community string.
- Mode - Send Trap or Inform message.
- Username - SNMP V3 Username.
- Password - SNMP V3 Password.
- Encryption - SNMP V3 Password Encryption. SHA or MD5.
- Engineid - To send traps as.

CHAPTER 5

Appendix

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.

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).

- **sysUpTime:** The time since the network management portion of the system was last re-initialised.
- 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

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 initialised (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
- The trap OID can be used to identify the cause of the SNMP trap

  .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

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

SNMP object 1.3.6.1.4.1.32723.1

```
iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationResource:  <resource>:
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationNode: node00:
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationOperation: start:
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationDescription: ok:
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationReturnCode: INTEGER:  0:
```

```
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationTargetReturnCode:  INTEGER: 0:
.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationStatus:  INTEGER: 0:
```

where<resource> is one of the following:

- shared-fs
- pgsql-fs
- shared-fs
- pgsql-fs
- dhcp-fs
- memcached
- dhcp-fs
- memcached
- dhcpd3
- hyperestraier-fs
- r-hyperestraier
- pgsql-dbms
- database-up
- pgsql-dbms
- vossbkr-fs
- vossbkr-imq
- mq-up
- vossbkr-imq
- usm-batch
- usm-selfcare
- apache2
- haproxy
- apache2
- ldfd
- ldfc
- iptdevmn
- iptqueue
- iptparent
- usm-loader-scheduler
- usm-phone-login-timeout
- usm-loader-scheduler
- usm-reverse-proxy

- usm-local-autoregister
- usm-net-autoregister

SNMP Traps: Service Monitoring

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:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:  TimeTicks:
150 days, 18 hours, 50 minutes, 4 seconds.:

.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.
snmpTrap.snmpTrapOID.0:  Object ID:  .1.3.6.1.4.1.32723.1:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationResource:  <resource>:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationNode:  node00:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationOperation:  stop:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationDescription:  ok:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationTargetReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationStatus:  INTEGER:  0:
```

Service restart is indicated by the following:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:  TimeTicks:
150 days, 18 hours, 50 minutes, 4 seconds.:

.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.
snmpTrap.snmpTrapOID.0:  Object ID: .1.3.6.1.4.1.32723.1:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationResource:  <resource>:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationNode:  node00:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationOperation:  start:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationDescription:  ok:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationTargetReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationStatus:  INTEGER:  0:


.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:  TimeTicks:
```

```
150 days, 18 hours, 50 minutes, 4 seconds.:

.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.
snmpTrap.snmpTrapOID.0:  Object ID: .1.3.6.1.4.1.32723.1:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationResource:  <resource>:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationNode:  node00:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationOperation:  monitor:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationDescription:  ok:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationTargetReturnCode:  INTEGER:  0:

.iso.org.dod.internet.private.enterprises.pacemaker.pacemakerNotification.
pacemakerNotificationStatus:  INTEGER:  0:
```

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.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.2.1.88.2.0.1iso.3.6.1.2.1.88.2.1.1.0
  = STRING: "shutdown requested"
  ```

Trap OID

- `iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.2.1.88.2.0.1iso.3.6.1.2.1.88.2.1.1.0 = STRING: "shutdown requested"`

Variable Bindings

- `iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.2.1.88.2.0.1iso.3.6.1.2.1.88.2.1.1.0 = STRING: "shutdown requested"iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1`

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 CUCDM
- 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.
dismanEventMIBNotificationObjects.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.
dismanEventMIBNotifications.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.
dismanEventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Disk full.
```
-
```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.mteHotTargetName.0 =
```
-
```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.mteHotContextName.0 =
```
-
```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.mteHotOID.0 = dskErrorFlag.1
```
-
```
.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.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: Disk Wait Time

A trap is generated if disk wait value is too high.

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 CUCDM
- 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

- `.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 = "diskwaitfail"`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.?dismanEventMIBNotificationObjects.mteHotValue.0 = <the average disk IO wait time>`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: Disk Service Time

A trap is generated if disk wait value is too high.

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 CUCDM
- 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

- `.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 = "diskservicefail"`
- `iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.?dismanEventMIBNotificationObjects.mteHotValue.0 = <the average disk IO service time>`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

SNMP Trap: Disk Load Fail

A trap is generated if disk wait value is too high.

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 CUCDM
- 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

- `.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 = "diskloadfail"`
- `iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.?dismanEventMIBNotificationObjects.mteHotValue.0 = <the disk load percentage>`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

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 CUCDM
- 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.
dismanEventMIBNotificationObjects.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.
dismanEventMIBNotifications.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.
  dismanEventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Excessive load.
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.mteHotTargetName.0 =
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.mteHotContextName.0 =
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.mteHotOID.0 = laErrorFlag.1
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.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 CUCDM
- 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 - 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.dismanEventMIBNotificationObjects.mteHotTrigger.0 = "backupCompleted"
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotValue.0 = 0
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Variable Bindings - failed backup

- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEve
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEve

SNMP Trap: DR Initial Synchronization

An initial synchronization takes place when the Primary database is synchronized to the Standby system using the `sync` command.

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 CUCDM
- 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

- .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 = "pginitsync"
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.

```
dismanEventMIBNotificationObjects.mteHotValue.0 = 5
```

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

SNMP Trap: DR Database Synchronization Failure

A trap is generated if the DR system is unable to synchronize database updates from primary to secondary.

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 CUCDM
- 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

- ```
  .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 = "SyncDRfailed"
  ```
- ```
  .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.mteHotValue.0 = 5
  ```
- ```
  .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
  ```

SNMP Trap: DR Filesystem Synchronization Failure

A trap is generated if the DR system is unable to synchronize the filesystem from primary to secondary.

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 CUCDM
- 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

- .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 = "SyncSharedFS"
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
  dismanEventMIBNotificationObjects.mteHotValue.0 = 5
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Performance Logs

A trap is generated if the generation of performance logs fails.

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

- .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 = "perflogfail"
-

```
   .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.
dismanEventMIBNotificationObjects.mteHotValue.0 = 5
```

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

SNMP Trap: Additional Performance Monitoring

Traps are generated during monitoring.

Actual Trap

- 2014-05-23T09:00:04.300397+00:00 'SYSNAME' snmp: Args:
- SNMPv2-MIB::snmpTrapOID.0 DISMAN-EVENT-MIB::mteTriggerFired
- DISMAN-EVENT-MIB::mteHotTrigger.0 s The combination of Apache and Postgress
- total ram is running below the threshold DISMAN-EVENT-MIB::mteHotContextName.0
- s Postgres Ram, 2014/05/23 09:00:02, 351538.5, KB, 5767168, 7340032, Green
- Check http access. Raise TAC Case DISMAN-EVENT-MIB::mteHotValue.0 i 1
- SNMPv2-MIB::sysName.0 s 'SYSNAME'

Description

There are three possible thresholds; Green (OK), Amber (Warning) and Red (ERROR).

The SNMP trap is described as follows:

- Description: The combination of Apache and Postgres total ram is running below the threshold - This means that the Apache and Postgres combined memory usage is actually less than the thresholds, which is good.
- Service name: Postgres Ram
- Date timestamp: 2014/05/23 09:00:02
- Unit: KB - This means that the all memory usage reading is in KiloBytes
- Current memory usage: 351538.5
- Amber Threshold: 5767168
- Red Threshold: 7340032
- Status Flag: Green - everything is ok
- Action Status: If the Status Flag is Red or Amber, the following messages are displayed: Check http access. Raise TAC Case.

SNMP Trap: Health Logs

A trap is generated if health logs 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 CUCDM
- 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`

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.dismanEve`
- `.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEve`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`