Monitor the Cisco Prime Collaboration Assurance Server

This section explains the following:

Monitor the Cisco Prime Collaboration Assurance Server

For Cisco Prime Collaboration Release 11.5 and later

You can monitor the Cisco Prime Collaboration Assurance Server health using the Cisco Prime Collaboration Assurance application. You can get information on CPU, memory, disk utilization, logical storage areas, and process details.

Prerequisites:

- Enable SNMP v1, v2c, or v3 in Cisco Prime Collaboration Assurance. For more information on enabling SNMP v1, v2c, and v3, See the *Configuring Cisco Prime Collaboration Assurance Server* section in Configure Devices for Prime Collaboration Assurance.
- Enable SNMP v1/v2c using admin access. Root access is not needed to enable SNMP v1/v2c.
- Enable SNMP v3 using root access. You need to raise a TAC case to get the root access.
- Connect to Cisco Prime Collaboration Assurance Server from a SNMP Manger using SNMP v1, v2c, or v3 RO community string in settings.

Monitor Cisco Prime Collaboration Server Health

The MIB details required to monitor the health of Cisco Prime Collaboration Assurance Server are listed in the following table:

Component	Table	OID	MIB
CPU	systemStats	1.3.6.1.4.1.2021.11	UCD-SNMP-MIB
Memory	memory	1.3.6.1.4.1.2021.4	UCD-SNMP-MIB
Disk Storage	hrDeviceTable	.1.3.6.1.2.1.25.3.2	HOST-RESOURCES-MIB
	hrDiskStorageTable	.1.3.6.1.2.1.25.3.6	

Component	Table	OID	MIB
Logical Storage areas	hrStorageTable	.1.3.6.1.2.1.25.2.3	HOST-RESOURCES-MIB
Process	hrSWRunTable	.1.3.6.1.2.1.25.4.2	HOST-RESOURCEs-MIB

Example:

- To monitor the CPU utilization

  If you have enabled SNMP v1 or v2c, enter the following commands:

  Syntax

  `# snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::systemStats`

  Example

  `snmptable -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::systemStats`

  If you have enabled SNMP v3, enter the following commands:

  Syntax

  `snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1 -a MD5 <PCA IP> UCD-SNMP-MIB::systemStats`

  Example

  `snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane -a MD5 <PCA IP> UCD-SNMP-MIB::systemStats`

  Sample Output

```
UCD-SNMP-MIB::ssIndex.0 = INTEGER: 1
UCD-SNMP-MIB::ssErrorName.0 = STRING: systemStats
UCD-SNMP-MIB::ssSwapIn.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssSwapOut.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssIOSent.0 = INTEGER: 609 blocks/s
UCD-SNMP-MIB::ssIOReceive.0 = INTEGER: 0 blocks/s
UCD-SNMP-MIB::ssSysInterrupts.0 = INTEGER: 994 interrupts/s
UCD-SNMP-MIB::ssSysContext.0 = INTEGER: 5508 switches/s
UCD-SNMP-MIB::ssCpuUser.0 = INTEGER: 6
UCD-SNMP-MIB::ssCpuSystem.0 = INTEGER: 0
UCD-SNMP-MIB::ssCpuIdle.0 = INTEGER: 87
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 15940286
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 14270
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 1046654
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 193992466
UCD-SNMP-MIB::ssCpuRawWait.0 = Counter32: 6614683
```

```
UCD-SNMP-MIB::ssCpuRawKernel.0 = Counter32: 0
```

- To monitor the memory utilization

  If you have enabled SNMP v1 or v2c, enter the following commands :

  Syntax

  # snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::memory

  Example

  snmptable -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::memory

  If you have enabled SNMP v3, enter the following commands :

  Syntax

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1 -a MD5 <PCA IP> UCD-SNMP-MIB::memory

  Example

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane -a MD5 <PCA IP> UCD-SNMP-MIB::memory

  Sample Output

```
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 25165816 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 25165724 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 14236500 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 848220 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 26013944 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 516240 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 3495964 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: noError(0)
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

- To monitor the disk storage details

  If you have enabled SNMP v1 or v2c, enter the following commands:

  Syntax

  snmptable -v 2c -c public <PCA IP> [OID]

  Example

  snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.2

  If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.3.2
```

Sample Output

Table 1: SNMP table: HOST-RESOURCES-MIB::hrDeviceTable

hrDeviceIndex	hrDeviceDescr	hrDeviceType	hrDeviceID	hrDeviceStatus	hrDeviceErrors
1552	HOST-RESOURCES-TYPES::hrDevice DiskStorage	SCSI disk (/dev/sda)	SNMPv2-SMI::zeroDotZero	running	?
1538	HOST-RESOURCES-TYPES::hrDevice DiskStorage	VMware Virtual IDE CDROM Drive	SNMPv2-SMI::zeroDotZero	running	?

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmptable -v 2c -c public <PCA IP> [OID]
```

Example

```
snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.6
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.3.6
```

Sample Output

Table 2: SNMP table: HOST-RESOURCES-MIB::hrDiskStorageTable

hrDiskStorageAccess	hrDiskStorageMedia	hrDiskStorageRemoveble	hrDiskStorageCapacity
readWrite	unknown	true	0KBytes
readWrite	unknown	false	262144000 KBytes

- To monitor the logical storage areas

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmptable -v 2c -c public <PCA IP> [OID]
```

Example

```
snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.2.3
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.2.3
```

Sample Output

Table 3: SNMP table: HOST-RESOURCES-MIB::hrStorageTable

hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageAllocationFailures
1	HOST-RESOURCES-TYPES::hrStorageRam	Physical memory	1024 Bytes	14236500	13338404	?
3	HOST-RESOURCES-TYPES::hrStorageVirtualMemory	Virtual memory	1024 Bytes	39402316	13338496	?

- To monitor the process details

If you have enabled SNMP v1 or v2c, enter the following commands:

Syntax

```
snmptable -v 2c -c public <PCA IP> [OID]
```

Example

```
snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.4.2
```

If you have enabled SNMP v3, enter the following commands:

Syntax

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> [OID]
```

Example

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u
user1 <PCA IP> .1.3.6.1.2.1.25.4.2
```

Sample Output

Monitor the Cisco Prime Collaboration Assurance Server

Table 4: SNMP table: HOST-RESOURCES-MIB::hrSWRunTable

hrSW RunIndex	hrSW RunName	hrSW RunID	hrSW RunParameters	hrSW RunType	hrSW RunStatus	hrSW Runpath
2367	postgres	SNMPv2-SMI : : zeroDotzero	""	application	runnable	postgres: cmuser cpcm 127.0.0.1 (51478) idle
2643	postmaster	SNMPv2-SMI : : zeroDotzero	""	application	runnable	postgres: primea cqdb 127.0.0.1 (50175) FETCH