System Monitoring

The COS Service can be monitored through the following:

COS Cluster Status Monitoring

The COS service is implemented through an instance of the application instance controller (AIC). Each application instance represents a service instance. Some earlier COS releases supported a single service instance with one endpoint, one cluster, and one redundancy policy. COS Release 3.18.1 deployments can support multiple COS clusters, and each cluster has its own asset redundancy policy.

The **Cisco Cloud Object Store (COS) > COS Service Status** page of the V2PC GUI reports the status of each cluster. The values for Storage Status, Disk Status, Interface Status, Service Status, and Fault Status can be reported as one of the following:

- **Normal** – all member nodes report Normal for that status.
- **Warning** – at least one member node reports a Warning level for that status.
- **Critical** – at least one member node reports a Critical level for that status.

On this page, you can drill down through a COS cluster to view the status of its individual COS nodes. Drilling down to each node reveals the status of individual node disks, interfaces, and services, and displays any active alarms for the node.

Note COS Release 3.18.1 supports resiliency status monitoring for two resiliency parameters per COS node, Local Erasure Coding (LEC, if enabled) and GOIDS.

COS Node Status Monitoring

A COS node is in service if both the associated COS application instance and the cluster to which it belongs are in Enabled state. The V2PC GUI displays the status of each node that is in service and part of a COS cluster. This status is updated once per minute, or when a fault is detected.

A reported fault raises an alarm or an event (or both), which is displayed in the V2PC GUI. If the fault is serious, the service interfaces for that COS node are removed from the DNS.

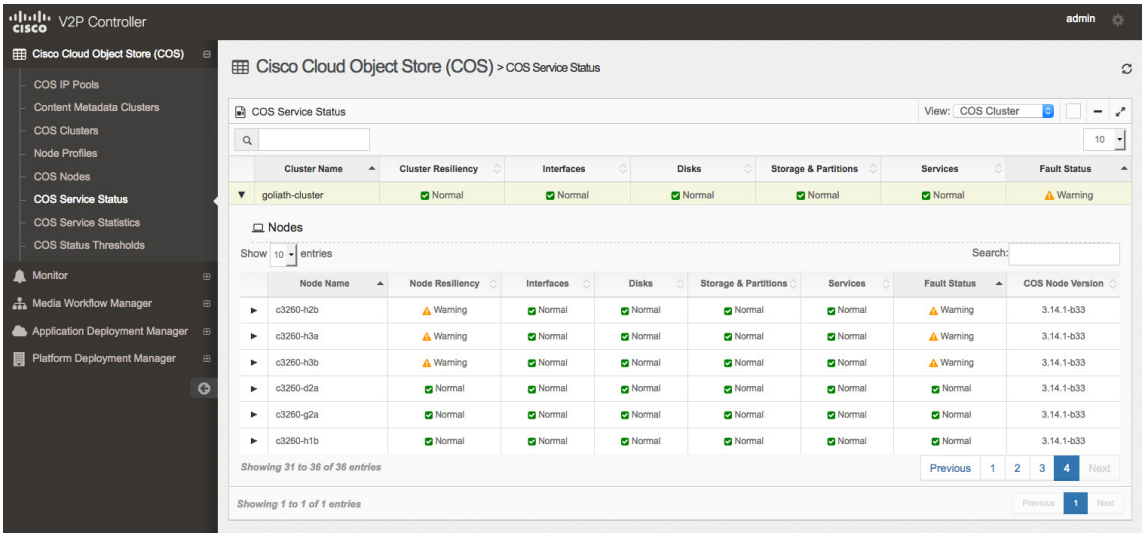
When the fault is no longer present, the service interfaces are replaced in the DNS and the node returns to normal service.

Viewing COS Node Status

To view a summary of node usage and alarms (if any) using the V2PC GUI, open the GUI as described in Accessing the V2PC GUI, page A-2 and navigate to **Cisco Cloud Object Store (COS) > COS Service Status**.

COS Release 3.18.1 supports filtering the COS service status view by COS Cluster (default) or by Resiliency Group, which shows the COS nodes grouped by resiliency group. You can also choose to view Metadata Cluster status.

Figure 3-1 V2PC GUI, COS Service Status Page



The COS Service Status page lists the service instances and displays the associated node usage along with any alarms. This page displays the following information:

- Any components that are down, disabled, inactive, or otherwise unavailable are marked with a red (as opposed to green) icon for identification.
- The Disks table lists the status of drives as down if the drive is defective or missing. If all disks are down, the associated node is reported as down.
- If a critical service is down, the associated node is reported as down.

Viewing Deployment Status

To view the status of the overall deployment from the V2PC GUI, open the GUI as described in Accessing the V2PC GUI, page A-2 and navigate to **Dashboard > System Overview**. The System Overview page offers information about Bandwidth (Tx/Rx) and Session (Tx/Rx) Storage usage.

Viewing COS Alarms and Events

The COS Alarms & Events page lists significant COS-related system events and provides details for user evaluation. To view this page in the V2PC GUI, open the GUI as described in Accessing the V2PC GUI, page A-2 and navigate to **Dashboard > Alarms & Events**.

All the events for the node are listed with the oldest event first. Events belong to one of the following levels of severity:

- **Info** – The event represents information only and does not require operator intervention.
- **Warning** – The event represents an issue that is possibly transitory and the operator should investigate the cause.
- **Critical** – The event represents an issue from which the node may not recover without operator intervention, and the operator must act immediately because the issue may cause service outage.

COS-AIC Alarms and Events

The COS AIC reports alarms and events to the V2PC GUI. The AIC generates alarms and events based on both GUI REST transactions (user input) and AIC client-generated status notifications.

GUI/REST Transactions

Events

Table 3-1 GUI/REST Transactions - Events

Event Name	Description	Severity	Details
CosActiveIpPoolEdited	The active IP Pool: "poolName" was edited.	critical	Event is triggered when a user edits an IP Pool that is in use by COS-AIC.
CosActiveIpPoolEdited	The active IP Pool: "poolName" was edited.	critical	Event is triggered when a user edits an IP Pool that is in use by COS-AIC.
CosActiveIpPoolDeleted	The active IP Pool: "poolName" was deleted.	critical	Event is triggered when a user deletes an IP Pool that is in use by COS-AIC.
CosNodeConfigError	The COS Node: "hostName" physical interface count has been changed.	critical	Event triggered if the number of interfaces changes for a node.
CosNodeConfigError	The COS Node: "hostName" IP Pool: "poolName" does not have sufficient IPs available.	major	Event triggered by IP Pool running out of IPs.
CosAddNode	New COS Node: "hostName" processed and added to cluster: "clustName"."	info	Event triggered by addition of new COS Node.
CosDeleteNode	COS Node: "hostName" has been deleted.	warning	Event triggered when a COS Node is deleted.
CosNodeDnsAddError	COS dnsOperation -> addDNSRecord: "Domain Details" returned error: "errorString".	major	Event triggered when a DNS Add/Remove returns other than 200.

Alarms

Table 3-2 GUI/REST Transactions - Alarms

Alarm Name	Description	Severity	Details
CosClusterDeactivated	COS Cluster: "clusterName" has been Deactivated.	critical	Alarm is triggered when a COS Cluster is set to "disabled".

AIC Client Status Notifications

Events

Table 3-3 AIC-Client Status Notifications - Events

Event Name	Description	Severity	Details
CosNodeHeartBeat	COS Node: "hostName" has missed a heartbeat.	critical	Event triggered when a COS Node misses a scheduled heartbeat (aic_cosnodeheartbeat).
CosNodeServiceDown	COS Node: "hostName" non-critical service "Sensu Client" is down.	warning	Event triggered when Sensu Client is reported down, because COS Node can't send events (aic_cosnodestatus).

Alarms

Table 3-4 AIC-Client Status Notifications - Alarms

Alarm Name	Description	Severity	Details
CosNodeDiskDown	COS Node: "hostName" > "disksDown" of the total "disksTotal" disks ("percentageDisksDown"%) are last reported as down.	varies by % down	Alarm is triggered when disks are reported down (aic_cosnodestatus).
CosNodeInterfaceDown	COS Node: "hostName" interfaces(s) "list" reported as down.	varies by % down	Alarm triggered when interfaces are reported as down (aic_cosnodestatus).
CosNodeDown	COS Node: "hostName" is down and removed from DNS.	critical	Alarm triggered by either missed heartbeat, all disks down, or critical service down.
CMCNodeStorageCapacity	CMC Node: 'hostname' Storage capacity reported as usage XX.nm%.	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.

Table 3-4 AIC-Client Status Notifications - Alarms

Alarm Name	Description	Severity	Details
MetadataStoragePartition	CMC Node: 'hostname' Storage capacity reported as usage XX.nm%.	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.
MetadataCommitLog-Partition	CMC Node: 'hostname' Storage capacity reported as usage XX.nm%.	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.
CmcApplicationLogPartition	CMC Node: 'hostname' Storage capacity reported as usage XX.nm%.	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.
CosServiceLogPartition	CMC Node: 'hostname' Storage capacity reported as usage XX.nm%.	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.
CosNodeStorageCapacity	COS Node: 'hostname' Storage capacity reported as usage XX.nm%	warning | critical	Alarm is raised when capacity exceeds the warning or critical thresholds values set in the thresholds settings page.
CmcNodeServiceDown	CMC Node: 'hostname' service 'ServiceName' is down.	warning | critical	Alarm is raised when a CMC service goes down. If the service is critical, a critical alarm is raised; otherwise, a warning level alarm is raised. **Note:** If the Consul service goes down, communication between the CMC node and COS AIC is lost, and a NodeDown alarm is raised in the event of failure of the Consul service.

COS AIC Client Events

The COS AIC client generates events pertaining to storage (disk), network (interface), and service (process) for each node. These events are generated only if the AIC client monitoring is enabled. For more information on this monitoring activity, see Viewing Deployment Status, page 3-3.

The events generated by a COS AIC client are listed in Table 3-5.

Table 3-5 COS AIC Client Events

Event Name	Description	Severity	Event Type	Event Subtype
CosNodeInterfaceDown	Interface *if_name* down.	Warning	COS-Node	Health
CosNodeInterfaceUp	Interface *if_name* up.	Info	COS-Node	Health

Table 3-5 COS AIC Client Events

Event Name	Description	Severity	Event Type	Event Subtype
CosNodeServiceDown	Service *if_name* down.	Warning	COS-Node	Health
CosNodeServiceUp	Service *if_name* up.	Info	COS-Node	Health

- An event is generated for every change in the state of operation of a disk, interface, or process.
- Events can also be appear in response to activity monitoring, which occurs at 10-second intervals.

COS AIC Server Events

The COS AIC server generates the events listed in Table 3-6.

Table 3-6 COS AIC Server Events

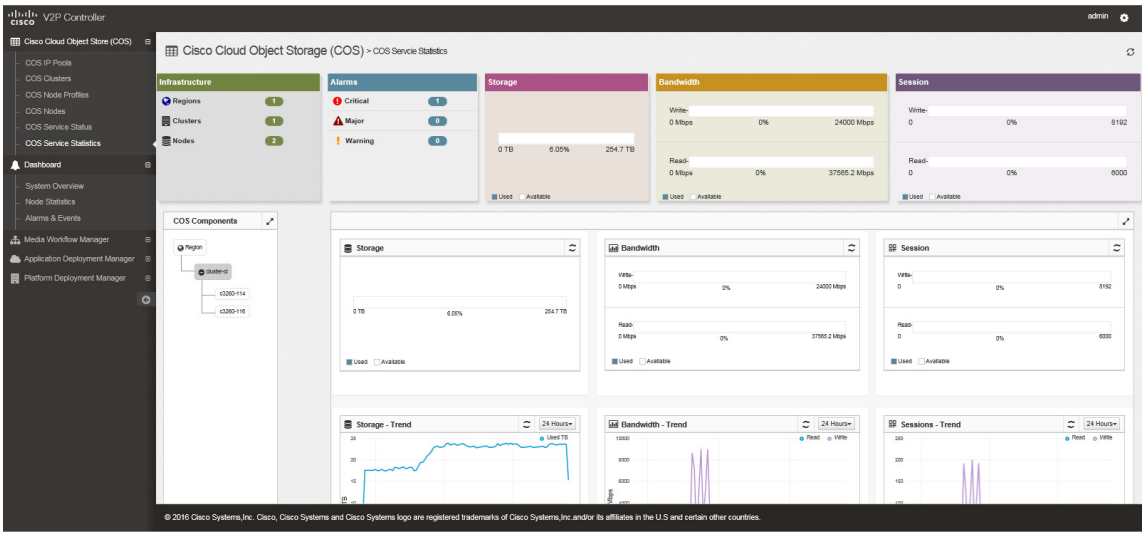
Event Name	Description	Severity	Event Type	Event Subtype
AddCosNode	A new COS node was added.	Info	COS-Node	Accessibility
CosNodeInterfaceError	No IP addresses are available in the IP pool.	Major	COS-Node	Accessibility
CosUpdatedActiveIpPool	An active IP pool was edited.	Critical	COS-Node	Accessibility
CosDeletedActiveIpPool	An active IP Pool was deleted.	Critical	COS-Node	Accessibility

Viewing COS Statistics

The COS Services Statistics page provides a graphical summary of the status and performance of the node infrastructure. The displays update every 15 minutes to track changes in key system states over time.

To view the COS Statistics page in the V2PC GUI, open the GUI as described in Accessing the V2PC GUI, page A-2 and navigate to **Cisco Cloud Object Store (COS) > COS Services Statistics.**

Figure 3-2 V2PC GUI, COS Service Statistics Page



This page displays the following information:

- Windows across the top report the regions, clusters, and nodes in the infrastructure, display any current alarms by severity, and show current storage, bandwidth, and session utilization.
- Graphical displays in the mid-section show current and trending storage, bandwidth, and session utilization for the selected COS component.
- The time zone shown at upper right in the page is that of the server, and can be changed by an Admin user. Individual nodes may be spread across multiple time zones.
- Scrolling to the bottom of the page reveals tables that list the current status of all of the disks, services, and interfaces associated with the selected COS component, along with any alarms.

COS AIC Client Monitoring

The COS AIC client running on a COS node periodically monitors the disks, interfaces, and services (processes) of that node and posts the data to the DocServer as a COS-specific document.

The AIC client begins the monitoring activity when a node is configured and added to a COS cluster. As long as the node is running and is part of a COS cluster, monitoring occurs once every 10 seconds.

Storage Monitoring

The AIC client can monitor and report storage (disk) state and statistics only if the CServer is running on the node. The following information is reported for each disk:

- Disk name
- Bytes read
- Bytes written
- Requests
- State
- S.M.A.R.T. Status

The client also reports the total storage space on all disks and the total storage space currently in use.

Interface Monitoring

For each interface, the AIC client reports the interface state and the transmit and receive statistics. The client can monitor and report the state and statistics of CServer interfaces only when the CServer is running on the node.

Services Monitoring

The AIC client monitors the following services:

- Cisco Cache Server (CServer)
- Cisco Cloud Object Storage Daemon (cosd)
- Cassandra Server
- NTP Daemon
- SNMP Daemon
- Monit
- Consul Agent
- Sensu Client

CMC AIC Client Monitoring

The CMC AIC client running on a CMC node periodically monitors the metadata, log storage, interfaces, and services (processes) of that node and posts the data to the DocServer as a node-specific document.

The CMC AIC client begins monitoring activity when a node is configured and added to a CMC cluster. As long as the node is running and is part of a CMC cluster, monitoring occurs once every 2 seconds. Status is reported once every hour unless there is a significant change in state; for example, if an interface or service changes state (down or up) or if storage changes by more than 1%.

Storage Monitoring

The CMC AIC Client monitors and reports the usage information (path, total MB and used MB) for Metadata Storage, Metadata Commit Log and CMC Application Log partitions on the CMC node.

Interface Monitoring

The CMC AIC client reports the interface speed and state for each CMC interface.

Services Monitoring

The CMC AIC Client monitors the following services: Cassandra, NTP Daemon, and Consul Agent.

Troubleshooting Alarms, Events, and Statistics

If one or more COS nodes in a cluster are not generating any alarms, events, or statistics, perform the following steps to ensure that monitoring is configured and working correctly.

Checking COS Nodes

Perform these steps for each COS node attached to the cluster in V2PC master.

Step 1 To confirm that the Sensu client is running on the COS node, connect to the node using SSH, type the command **service sensu-client status**, and check the response to see if the client is running. If not, type **sensu-client start** to start the service.

Step 2 To confirm that the Sensu configurations are present on the COS node, SSH into the node, type **cd /etc/sensu/conf.d**, and check that the following files are present and configured correctly:

- client.json
- rabbimq.json
- transport.json
- metrics-cos-nodes.json – confirm that the interval attribute is set to 900 (15 minutes)

Note If helpful, compare the contents of each file with those on another known working COS node.

Additionally, check the plugins directory (**cd /etc/sensu/plugins**) and confirm that metrics-cos-nodes.js is present.

Step 3 To confirm that the sensu-service log is present on the COS node, SSH into the node and type **tail –f /var/log/sensu/sensu-client.log**. Sensu checks for this information every 15 minutes.

Step 4 To confirm that the COS node statistics document is present, SSH into the node, type **cd /tmp**, then type **ls -al** and check the timestamp on the aic_cosnodestats.json file. This file should update every 15 minutes. If the file is present, type **cat /tmp/aic_cosnodestats.json** and confirm that it is not empty.

Step 5 To confirm that the rabbitmq messaging file on the COS node can be accessed, SSH into the node and type **cat /etc/sensu/conf.d/rabbitmq.json**.

Step 6 Try to ping the host from the COS node to confirm that it can be reached.

Note It is normal in an HA environment for the host ping to return different IP addresses.

Checking the Sensu Master

An HA environment can have multiple Sensu masters. Perform the following steps to check each master:

Step 1 Connect via SSH to the Sensu master that you are accessing using the V2PC GUI.

Step 2 Type **consul members** to list all of the active masters in the HA environment.

Step 3 Check the conf.d directory (**cd /etc/sensu/conf.d**) to see if **handler-metrics-cos-nodes-influxdb.json** is present. If not, copy this file from another working master and place it in the conf.d directory.

Step 4 Open **influxdb.json** and confirm that it has the configuration information needed to access influxdb.

Step 5 Try to ping the influxdb host to confirm that it can be reached.

Note It is normal in an HA environment for the host ping to return different IP addresses.

Step 6 Check the handlers directory (**cd /etc/sensu/handlers**) to see if **metrics-cos-nodes-influxdb.js** is present. If not, copy this file from another working master and place it in the handlers directory.

Step 7 Also check to see if the **node_modules** directory is present and contains influx. If not, copy this directory from another working master.

Step 8 Type **systemctl status sensu-server** to confirm that the Sensu server is running.

Step 9 Type **tail –f /var/log/sensu/sensu-server.log** to check the Sensu server logs.