Ultra M Component Event Severity and Fault Code Mappings

Events are assigned to one of the following severities (refer to CFaultSeverity in Ultra M MIB):

- emergency(1), -- System level FAULT impacting multiple VNFs/Services

- critical(2), -- Critical Fault specific to VNF/Service

- major(3), -- component level failure within VNF/service.

- alert(4), -- warning condition for a service/VNF, may eventually impact service.

- informational(5) -- informational only, does not impact service

Events are also mapped to one of the following fault codes (refer to cFaultCode in the Ultra M MIB):

- other(1), -- Other events

- networkConnectivity(2), -- Network Connectivity -- Failure Events.

- resourceUsage(3), -- Resource Usage Exhausted -- Event.

- resourceThreshold(4), -- Resource Threshold -- crossing alarms

- hardwareFailure(5), -- Hardware Failure Events

- securityViolation(6), -- Security Alerts

- configuration(7), -- Config Error Events serviceFailure(8) -- Process/Service failures

The Ultra M Manager Node serves as an aggregator for events received from the different Ultra M components. These severities and fault codes are mapped to those defined for the specific components. The information in this section provides severity mapping information for the following:

OpenStack Events

Component: Ceph

Table 1: Component: Ceph

Failure Type	Ultra M Severity	Fault Code
CEPH Status is not healthy	Emergency	serviceFailure
One or more CEPH monitors are down	Emergency	serviceFailure
Disk usage exceeds threshold	Critical	resourceThreshold
One or more OSD nodes are down	Critical	serviceFailure
One or more OSD disks are failed	Critical	resourceThreshold
One of the CEPH monitor is not healthy.	Major	serviceFailure
One or more CEPH monitor restarted.	Major	serviceFailure
OSD disk weights not even across the board.		resourceThreshold

Component: Cinder

Table 2: Component: Cinder

Failure Type	Ultra M Severity	Fault Code
Cinder Service is down	Emergency	serviceFailure

Component: Neutron

Table 3: Component: Neutron

Failure Type	Ultra M Severity	Fault Code
One of Neutron Agent Down	Critical	serviceFailure

Component: Nova

Table 4: Component: Nova

Failure Type	Ultra M Severity	Fault Code
Compute service down	Critical	serviceFailure

Component: NTP

Table 5: Component: NTP

Failure Type	Ultra M Severity	Fault Code
NTP skew limit exceeds configured threshold.	Critical	serviceFailure

Component: PCS

Table 6: Component: PCS

Failure Type	Ultra M Severity	Fault Code
One or more controller nodes are down	Critical	serviceFailure
Ha-proxy is down on one of the node	Major	serviceFailure
Galera service is down on one of the node.	Critical	serviceFailure
Rabbitmq is down.	Critical	serviceFailure
Radis Master is down.	Emergency	serviceFailure
One or more Radis Slaves are down.	Critical	serviceFailure
corosync/pacemaker/pcsd - not all daemons active	Critical	serviceFailure
Cluster status changed.	Major	serviceFailure
Current DC not found.	Emergency	serviceFailure
Not all PCDs are online.	Critical	serviceFailure

Component: Rabbitmqctl

Table 7: Component: Rabbitmqctl

Failure Type	Ultra M Severity	Fault Code
Cluster Status is not healthy	Emergency	serviceFailure

Component: Services

Table 8: Component: Services

Failure Type	Ultra M Severity	Fault Code
Service is disabled.	Critical	serviceFailure
Service is down.	Emergency	serviceFailure
Service Restarted.	Major	serviceFailure

The following OpenStack services are monitored:

- Controller Nodes:
    - httpd.service
    - memcached
    - mongod.service
    - neutron-dhcp-agent.service
    - neutron-l3-agent.service
    - neutron-metadata-agent.service
    - neutron-openvswitch-agent.service
    - neutron-server.service
    - ntpd.service
    - openstack-cinder-api.service
    - openstack-cinder-scheduler.service
    - openstack-glance-api.service
    - openstack-glance-registry.service
    - openstack-heat-api-cfn.service
    - openstack-heat-api-cloudwatch.service
    - openstack-heat-api.service
    - openstack-heat-engine.service

- openstack-nova-api.service

- openstack-nova-conductor.service

- openstack-nova-consoleauth.service

- openstack-nova-novncproxy.service

- openstack-nova-scheduler.service

- openstack-swift-account-auditor.service

- openstack-swift-account-reaper.service

- openstack-swift-account-replicator.service

- openstack-swift-account.service

- openstack-swift-container-auditor.service

- openstack-swift-container-replicator.service

- openstack-swift-container-updater.service

- openstack-swift-container.service

- openstack-swift-object-auditor.service

- openstack-swift-object-replicator.service

- openstack-swift-object-updater.service

- openstack-swift-object.service

- openstack-swift-proxy.service

- Compute Nodes:

  - ceph-mon.target

  - ceph-radosgw.target

  - ceph.target

  - libvirtd.service

  - neutron-sriov-nic-agent.service

  - neutron-openvswitch-agent.service

  - ntpd.service

  - openstack-nova-compute.service

  - openvswitch.service

- OSD Compute Nodes:

  - ceph-mon.target

  - ceph-radosgw.target

- ceph.target

- libvirtd.service

- neutron-sriov-nic-agent.service

- neutron-openvswitch-agent.service

- ntpd.service

- openstack-nova-compute.service

- openvswitch.service

UCS Server Events

UCS Server events are described here:https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/faults/reference/ErrMess/FaultsIntroduction.html

The following table maps the UCS severities to those within the Ultra M MIB.

Table 9: UCS Server Severities

UCS Server Severity	Ultra M Severity	Fault Code
Critical	Critical	hardwareFailure
Info	Informational	hardwareFailure
Major	Major	hardwareFailure
Warning	Alert	hardwareFailure
Alert	Alert	hardwareFailure
Cleared	Informational	Not applicable

UAS Events

Table 10: UAS Events

Failure Type	Ultra M Severity	Fault Code
UAS Service Failure	Critical	serviceFailure*
UAS Service Recovered	Informational	serviceFailure*
* *serviceFailure* is used except where the Ultra M Health Monitor is unable to connect to any of the modules. In this case, the fault code is set to *networkConnectivity*.		

ESC VM Events

By default, the Ultra M Manager continuously monitors and processes VNF VM event notifications from ESC as reported through NETCONF.

☞

Important   In release 6.0, the feature that enables monitoring of UGP VNFCs using ESC was not fully qualified and made available only for testing purposes. In 6.2 and later releases, this feature has been fully qualified for use in the appropriate deployment scenarios. For more information, contact your Cisco Accounts representative.

Table 11: ESC VM Event Severities

ESC Event	Ultra M Severity	Fault Code	VNFR State
VM_DEPLOYED	Major	Service Failure	deployed
VM_ALIVE	Info	Other	alive
VM_UNDEPLOYED	Critical	Service Failure	offline
VM_REBOOTED	Major	Service Failure	rebooting
VM_RECOVERY_REBOOT	Major	Service Failure	If the event completion status is successful, then it is rebooting. If the event completion status is failure, then it is an error.
VM_RECOVERY_UNDEPLOYED	Critical	Service Failure	If the event completion status is successful, then it is offline. If the event completion status is failure, then it is an error.
VM_RECOVERY_DEPLOYED	Major	Service Failure	If the event completion status is successful, then it is rebooting. If the event completion status is failure, then it is an error.

ESC Event	Ultra M Severity	Fault Code	VNFR State
VM_RECOVERY_COMPLETE	Info	Other	If the event completion status is successful, then it is alive. If the event completion status is failure, then it is an error.
VM_STOPPED	Alert	Service Failure	stop_requested