Alarms

This chapter lists the Cisco VDS Service Broker Release 1.1 alarms. Each alarm is followed by an explanation and recommended action. The chapter also defines the six generic SNMP alarm traps.

Severity Level

An alarm can have one of the following three severity levels: critical, major or minor:

- Critical alarm indicates that a critical problem exists somewhere in the network. Critical alarms cause failover and should be cleared immediately.
- Major alarm indicates that a serious problem exists that is disrupting service. Major alarms differ from critical alarms in that they do not cause failovers. Major alarms should also be cleared immediately.
- Minor alarms should be noted and cleared as soon as possible.

Critical Alarms

Alarm 330001 (svcdisabled)—service name—service has been disabled.

Explanation The Node Manager tried restarting the specified service but the service kept restarting. The number of restarts has exceeded an internal limit and the service has been disabled.

Recommended Action The device may have to be reloaded for the service to be re-enabled.

Alarm 330002 (servicedead)—service name—service died.

Explanation A critical service has died. Attempts are made to restart this service, but the device may run in a degraded state.

Recommended Action The device could reboot itself to avoid instability. Examine the syslog for messages relating to the cause of service death.

Alarm 335000 (alarm_overload) Alarm Overload State has been entered.

Explanation The Node Health Manager issues this alarm to indicate that the device is raising alarms at a rate that exceeds the overload threshold.

Recommended Action Access the device and determine what services are raising the alarms. Take corrective action to resolve the individual services' issues.

Alarm 335001 (keepalive) Keepalive failure for—application name—Timeout = *n* seconds.

Explanation An application is not being responsive, indicating it may not be properly operating.

Recommended Action Access the device and determine the state of the specific application.

Alarm 335003 (test1) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335006 (test4) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335008 (test1) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 445002 (disk_smartfailcrit) An SE disk has severe early-prediction failure which requires immediate action.

Explanation The SYSMON issues this alarm to indicate that one of the disks attached to the SE has severe early-prediction failure (for example, the disk has failed SMART self-check).

Recommended Action Back up data immediately on the disk to prevent data loss, and replace the disk after it is marked bad by the SE.

Alarm 445005 (disk_softraidcrit) A SoftRAID device has malfunctioned and requires immediate action.

Explanation The System Monitor issues this alarm to indicate that a SoftRAID device has malfunctioned (for example, both component disks of a RAID-1 array have become inaccessible or faulty).

Recommended Action Replace the disks and restore the data from backup storage, or remanufacturing and reload the disks.

Alarm 445012 (crit_hw_validation) Critical hardware validation failure.

Explanation The System Monitor issues this whenever it fails to validate critical hardware components. Critical hardware components are vital to the system's overall functionality, and should be addressed immediately.

Recommended Action Access the device, retrieve hardware information from the **show inventory** command, and contact Cisco TAC as soon as possible.

Alarm 700004 (device_offline_alarm) Device is offline. Re-register device to cdsm is strongly recommended.

Explanation The device is offline.

Recommended Action Check the device or network status. It may be necessary to re-register the device to the CDSM.

Major Alarms

Alarm 330003 (servicedead)—service name—service died.

Explanation The node manager found the specified service to be dead. Attempts are made to restart this service.

Recommended Action Examine the syslog for messages relating to the cause of service death. The alarm is cleared if the service stays alive and does not restart soon.

Alarm 335002 (test) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335004 (test2) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335009 (test2) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335010 (test3) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 445001 (core_dump) A *User Core* file or *Kernel Crash* dump has been generated.

Explanation The SYSMON issues this alarm to indicate that one or more of the software modules or the kernel has generated core files.

Recommended Action Access the device and check the directory */local1/core_dir*, or */local1/crash*, retrieve the core file through FTP, and contact Cisco TAC.

Alarm 445003 (disk_smartfailmajor) An SE disk has early-prediction failure.

Explanation The SYSMON issues this alarm to indicate that one of the disks attached to the SE has early-prediction failure. This alarm indicates the disk could fail in the near future.

Recommended Action Make proper preparations for the incoming disk drive failure, such as making data backups and preparing a replacement disk.

Alarm 445008 (rootfs_lowmem) Rootfs is low on memory.

Explanation The root filesystem is low on memory. If the rootfs runs out of memory completely, applications start to fail.

Recommended Action Contact Cisco TAC immediately for a diagnosis.

Alarm 445009 (system_hittempmajor) System temperature is too high.

Explanation The System Monitor issues this alarm to indicate that the motherboard sensor reports high temperatures.

Recommended Action Check the temperature of the lab and the airflow inside the CDE.

Alarm 445010 (local_lowspace) Directory /local1 usage exceeds the threshold.

Explanation This directory runs out of space at 80%. If this directory runs out of space, some applications will not work properly. Clean up the files under /local1 now, otherwise the system will automatically delete log files to save space.

Recommended Action Clean up the files under /local1 to save space.

Alarm 445013 (major_hw_validation) Major hardware validation failure.

Explanation The System Monitor issues this whenever it fails to validate critical hardware components. Critical hardware components are vital to the system's overall functionality, and should be addressed immediately.

Recommended Action Access the device, retrieve hardware information from the show inventory command, and contact Cisco TAC as soon as possible.

Alarm 445018 (MegaRAID_battery) MegaRAID SAS Controller Battery Backup Unit has failed.

Explanation The MegaRAID SAS Controller Battery Backup Unit (BBU) may fail at any time; failure is imminent. If a UPS is not installed, in the event of a power-outage, there is a risk that the contents of the MegaRAID Controller Cache may be compromised, thereby causing potential filesystem corruption to the SYSTEM disk(s).

Recommended Action Contact Cisco TAC for further assistance.

Alarm 540002 (linkdown) Network interface is inactive or down.

Explanation The network interface is inactive or down.

Recommended Action Check the cables connected to the network device.

Alarm 540003 (speed_mismatch) An alarm is raised for a portchannel if an interface within a portchannel has a different negotiated data rate than the rest of the interfaces in the portchannel.

Explanation Speed mismatch among interfaces assigned to portchannel.

Recommended Action Check the switch settings and verify cables are connected.

Alarm 540004 (lacp_link_down) Network LACP interface is inactive or down.

Explanation Network LACP interface is inactive or down.

Recommended Action Check the cables connected to the network device.

Alarm 540005 (lacp_no_neighbor) Network LACP interface has no neighbor.

Explanation Network LACP interface can not receive any LACPDU packet.

Recommended Action Check if switch side has LACP turned on.

Alarm 560001 (threshold) Service monitor CPU threshold exceeded.

Explanation The Service Monitor CPU threshold has been exceeded.

Recommended Action Check the file */tmp/threshold_exceeded.txt*.

Alarm 560002 (threshold) Service monitor memory threshold exceeded.

Explanation The Service Monitor memory threshold has been exceeded.

Recommended Action Check the file */tmp/threshold_exceeded.txt.*

Alarm 560003 (threshold) Service monitor kernel memory threshold exceeded.

Explanation The Service Monitor kernel memory threshold has been exceeded.

Recommended Action Check the file */tmp/threshold_exceeded.txt*.

Alarm 560005 (threshold) Service monitor Disk threshold exceeded.

Explanation The Service Monitor disk threshold has been exceeded.

Recommended Action Check the file */tmp/threshold_exceeded.txt.*

Alarm 560006 (threshold) Service monitor Disk Failure count threshold exceeded.

Explanation The Service Monitor disk failure count threshold has been exceeded.

Recommended Action Check the file */tmp/threshold_exceeded.txt*.

Alarm 560015 (AllGeoSvrFail) Geo Server Failure Alarm.

Explanation Connectivity to all Geo Servers Fails.

Recommended Action Check connectivity to the IP address and port number for all configured geo servers.

Alarm 661001 (svclowdisk) Alarm database is running low in disk space in the STATEFS partition.

Explanation The database monitor service issues this alarm to indicate that it is running low in disk space in the STATEFS partition, and therefore content replication service (acquisition and distribution) has been temporarily stopped.

Recommended Action Execute the **cms database maintenance** command or schedule database maintenance more frequently to reclaim the disk space.

Alarm 700002 (cms_clock_alarm) Device clock is not synchronised with the primary VDSM. Enabling NTP on all devices is recommended.

Explanation SB clock needs to be synchronized with the primary VDSM to make statistics monitoring, program file etc to work. For Standy VDMS devices the clock needs to be synchorized with the primary VDSM for VDSM failover to work.

Recommended Action The clock on device or the primary VDSM needs to be fixed.

Alarm 710001 (ftp_export_failed) FTP export failed.

Explanation The alarm is raised when the system fails to export transaction logs to an FTP server. Check the network connectivity to the FTP server. Check the user name and password to access the server.

Minor Alarms

Alarm 330004 (servicedead)—service name—service died.

Explanation The node manager found the specified service to be dead. Attempts are made to restart this service.

Recommended Action Examine the syslog for messages relating to the cause of service death. The alarm is cleared if the service stays alive and does not restart in a short while.

Alarm 335005 (test3) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 335007 (test5) NHM Alarm Testing [string].

Explanation This alarm is used for testing the Node Health Manager.

Recommended Action No action is required. This alarm should never occur during normal operation.

Alarm 445000 (disk_failure) An SE disk has failed.

Explanation The SYSMON issues this alarm to indicate that one of the disks attached to the SE is not responding.

Recommended Action Access the device and execute the **show disk details** command. If the problem persists, replace the disk.

Alarm 445004 (disk_smartfailminor) A SE disk has minor early-prediction failure.

Explanation The SYSMON issues this alarm to indicate that one of the disks attached to the SE has a minor early-prediction failure. It warns that the disk may fail soon.

Recommended Action Monitor the disk for early indications of errors occurring. If more severe SMART errors occur, or if disk errors occur, take the appropriate action.

Alarm 445006 (disk_softraidminor) A SoftRAID device has become degraded and requires immediate action.

Explanation The SYSMON issues this alarm to indicate that a SoftRAID device has become degraded (for example, one disk of a RAID-1 array has become inaccessible or faulty).

Recommended Action If the system suspects an inconsistency in the RAID volume, it will initiate a resync to restore the volume's integrity. Check the RAID status using the **show disk raid** command to verify whether a disk failure or resync is occurring. For a resync, wait for the sync(s) to complete. For a degraded array, replace the disk.

Alarm 445007 (system_psufailminor) A power supply power cable is unplugged or the power supply has failed.

Explanation The System Monitor issues this alarm to indicate that at least one power supply failed or is unplugged.

Recommended Action Check the back of the CDE and locate the power supplies. Verify the power cables are plugged in and replace any failed power supplies.

Alarm 445011 (disk_badsector_minor) Bad sector(s) on disk.

Explanation The system came across a corrupted disk sector(s) that it may (or may not) have been able to identify in the description above.

Recommended Action Contact tech support. The sector(s) might be recoverable by executing the 'disk repair' command. When running 'disk repair', all data on the drive will be lost; however, any repaired sector(s) will be available for data storage again.

Alarm 445014 (minor_hw_validation) Minor hardware validation failure.

Explanation The System Monitor issues this whenever it fails to validate minor hardware components. Minor hardware components are vital to the system's overall functionality, and should be addressed immediately.

Recommended Action Inspect the alarm’s instance information. If the alarm is raised for a removable component, such as disk00, replace the component according to documentation. For additional assistance, contact Cisco TAC and provide the output of **show alarms detail support** and **show inventory**.

Alarm 445015 (filesystem_failure) A filesystem error has occurred.

Explanation The System Monitor raises this alarm to indicate that an unexpected filesystem error has occurred.

Recommended Action If the problem is isolated to a single CDNFS disk, it may be possible to reformat the disk to recover. Contact Cisco TAC for further assistance.

Alarm 445017(nas_offline) NAS attached to SE seems to be offline.

Explanation NAS attached to SE seems to be offline.

Recommended Action Check whether the NAS server is online and has sufficient mount permissions.

Alarm 445019 (MegaRAID_battery) MegaRAID SAS Controller Battery Backup Unit imminent failure detected.

Explanation The MegaRAID SAS Controller Battery Backup Unit (BBU) may fail at any time; failure is imminent. If a UPS is not installed, in the event of a power-outage, there is a risk that the contents of the MegaRAID Controller Cache may be compromised, thereby causing potential filesystem corruption to the SYSTEM disk(s).

Recommended Action Contact Cisco TAC for further assistance.

Alarm 511011 (fmsthresholdexceeded) FMS has reached service threshold limits.

Explanation FMS service has reached concurrent connection limits.

Recommended Action Avoid further service requests to this device, or contact Cisco TAC for more connection licenses.

Alarm 511017 (rtspgaugmentexceeded) RTSP Gateway TPS has reached augmentation threshold limits.

Explanation RTSP Gateway TPS has reached augmentation limits on maximum concurrent connections/allowed bandwidth.

Recommended Action No service disruption. Monitor device to see if it exceeds service threshold limits and add more devices if necessary.

Alarm 520001 (LinkDown) -group-ifc-slot-port- Specified interface in the standby group is down.

Explanation The specified interface in the standby group is down. There could have been a link failure on the interface or it may have been shut down on purpose.

Recommended Action Check the configuration and cabling of the specified interface.

Alarm 520002 (RouteDown) -group-ifc-slot-port- Unable to reach the configured default gateway on the specified interface.

Explanation Unable to reach the configured default gateway on the specified interface in the standby group.

Recommended Action Check the network configuration on the specified interface.

Alarm 520003 (MaxError) -group-ifc-slot-port- The specified interface has seen errors exceeding maximum allowable error count.

Explanation The specified interface has seen errors exceeding the maximum allowable error count.

Recommended Action Check the cabling or configuration of the specified interface.

Alarm 540001 (shutdown) Network interface is shutdown.

Explanation The network interface is shut down.

Recommended Action Check the interface configuration.

Alarm 560007 (augmentation) Service Monitor CPU augmentation alarm.

Explanation Service monitor CPU augmentation alarm.

Recommended Action Check augmentation threshold, threshold and average load for the above alarm Instance. Add more devices if necessary.

Alarm 560008 (augmentation) Service Monitor Memory augmentation alarm.

Explanation Service Monitor Memory augmentation alarm.

Recommended Action Check augmentation threshold, threshold and average load for the above alarm Instance. Add more devices if necessary.

Alarm 560009 (augmentation) Service Monitor Kernel Memory augmentation alarm.

Explanation Service Monitor Kernel Memory augmentation alarm.

Recommended Action Check augmentation threshold, threshold and average load for the above alarm Instance. Add more devices if necessary.

Alarm 560011 (augmentation) Service Monitor Disk augmentation alarm.

Explanation Service Monitor Disk augmentation alarm.

Recommended Action Check augmentation threshold, threshold and average load for the above alarm Instance. Add more devices if necessary.

Alarm 560012 (augmentation) Service Monitor disk failure count augmentation alarm.

Explanation Service Monitor disk failure count augmentation alarm.

Recommended Action Check augmentation threshold, threshold for the above alarm Instance. Add more devices if necessary.

Alarm 560013 (PrimGeoSvrFail) Primary Geo Server Failure Alarm.

Explanation Connection to the Primary Geo Server fails.

Recommended Action Check the connetivity to the IP address and Port number for the primary geo server.

Alarm 560014 (SecGeoSvrFail) Seconday Geo Server Failure Alarm.

Explanation Connection to Secondary Geo Server fails.

Recommended Action Check the connetivity to the IP address and Port number for the secondary geo server.

Alarm 640001 (admin-shutdown) Network interface is admin shutdown.

Explanation Network interface is admin shutdown.

Recommended Action Check the interface configuration.

Alarm 700001 (cms_test_alarm) CMS test alarm with instance value - instance was raised. The title is used in the CDSM GUI.

Explanation This is a test alarm defined and used in CMS code. This alarm is identified by a tuple (340001, instance). This means the system may have several raised alarms with the 340001 ID having different instance values. Instance is usually used to link an alarm to a particular data item (such as a particular failed disk, or a delivery service that is having A&D troubles).

Recommended Action Advise the user how to handle this raised alarm. This is shown in the CDSM GUI or command-line interface (CLI).

SNMP Alarm Traps

Cisco VDS Service Broker Release 1.1 software supports six generic alarm traps. Table 2-1 presents the trap number and trap type of the six generic alarm traps. Alarm traps sent from a VDS device contain a numeric alarm identifier, a trap number, a module identifier, and a category identifier. To enable the VDS device to send SNMP alarm traps for a specific alarm condition, use the **snmp-server enable traps** command. You can configure the generation of alarm traps based on the severity of the alarm and on whether the alarm is raised or cleared.

Table 2-1 Generic Alarm Traps

Trap Number	Trap Type
7	Critical alarm raised
8	Critical alarm cleared
9	Major alarm raised
10	Major alarm cleared

Table 2-1 Generic Alarm Traps (continued)

Trap Number	Trap Type
11	Minor alarm raised
12	Minor alarm cleared

Table 2-2 below presents the mapping of module names to module identifiers.

Table 2-2 Mapping of Module Names to Module Identifiers

Module Name	Module Identifier
Active Directory Database	8000
Content Management Service	3000
Node Health Manager	1
Node Health Manager 2	500
Network Interface Card	5500
Node Manager	2000
Remote Execution Agent	3500
Service Broker	5600
Standby	4000
Service Monitor	5700
System Monitor	1000

Table 2-3 below presents the mapping of category names to category identifiers.

Table 2-3 Mapping of Category Names to Category IDs

Category Name	Category Identifier
Communications	1
Service Quality	2
Processing Error	3
Equipment	4
Environment	5
Content	6