APPENDIX E

System Alert Descriptions and Default Configurations

The following list comprises the system alerts, their definitions, and default settings.

AuthenticationFailed

Authentication validates the user ID and password that are submitted during log in. An alarm gets raised when an invalid user ID and/or the password gets used.

Default Configuration

Table E-1 Default Configuration for the AuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Number of AuthenticationFailed events exceeds: 1 time in the last 1 minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoDRFFailure

This alert occurs when the DRF backup or restore process encounters errors.

Default Configuration

Table E-2 Default Configuration for the CiscoDRFFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoDRFFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-2 Default Configuration for the CiscoDRFFailure RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

CoreDumpFileFound

This alert occurs when the CoreDumpFileFound event gets generated. This indicates that a core dump file exists in the system.

Default Configuration

Table E-3 Default Configuration for the CoreDumpFileFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CoreDumpFileFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Not Selected
Enable Email	Selected
Trigger Alert Action	Default

CpuPegging

CPU usage gets monitored based on configured thresholds. If the usage goes above the configured threshold, this alert gets generated.

Default Configuration

Table E-4 Default Configuration for the CpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: 99%
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CriticalServiceDown

The CriticalServiceDown alert gets generated when the service status equals down (not for other states).

Default Configuration

Table E-5 Default Configuration for the CriticalServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Service status is DOWN
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

HardwareFailure

This alert occurs when a hardware failure event (disk drive failure, power supply failure, and others) has occurred.

Default Configuration

Table E-6 Default Configuration for the HardwareFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: HardwareFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogFileSearchStringFound

This alert occurs when the LogFileSearchStringFound event gets generated. This indicates that the search string was found in the log file.

Default Configuration

Table E-7 Default Configuration for the LogFileSearchStringFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: LogFileSearchStringFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-7 Default Configuration for the LogFileSearchStringFound RTMT Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionHighWaterMarkExceeded

This alert occurs when the percentage of used disk space in the log partition exceeds the configured high water mark. When this alert gets generated, LPM deletes files in the log partition (down to low water mark) to avoid running out of disk space.

Note LPM may delete files that you want to keep. You should act immediately when you receive the LogPartitionLowWaterMarkExceeded alert.

Default Configuration

Table E-8 Default Configuration for the LogPartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionLowWaterMarkExceeded

This alert occurs when the LogPartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark.

Note Be aware that this alert is an early warning. The administrator should start freeing up disk space. Using RTMT/TLC, you can collect trace/log files and delete them from the server. The administrator should adjust the number of trace files that are kept to avoid hitting the low water mark again.

Default Configuration

Table E-9 Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowActivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space on the active partition is lower than the configured value.

Default Configuration

Table E-10 Default Configuration for the LowActivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Active Partition available diskspace below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowAvailableVirtualMemory

RTMT monitors virtual memory usage. When memory runs low, a LowAvailableVirtualMemory alert gets generated.

Default Configuration

Table E-11 Default Configuration for the LowAvailableVirtualMemory RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Available virtual memory below (30%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowInactivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space of the inactive partition equals less than the configured value.

Default Configuration

Table E-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive Partition available disk space below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily

Table E-12 Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

LowSwapPartitionAvailableDiskSpace

This alert indicates that the available disk space on the swap partition is low.

Note The swap partition is part of virtual memory, so low available swap partition disk space means low virtual memory as well.

Default Configuration

Table E-13 Default Configuration for the LowSwapPartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Swap Partition available disk space below (10%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ServerDown

This alert occurs when a remote node cannot be reached.

Note *Unified CM clusters only:* The ServerDown alert gets generated when the currently "active" AMC (primary AMC or the backup AMC, if the primary is not available) cannot reach another server in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

Default Configuration

Table E-14 Default Configuration for the ServerDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ServerDown occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionHighWaterMarkExceeded

This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table E-15 Default Configuration for the SparePartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionLowWaterMarkExceeded

This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition has exceeded the low water mark threshold.

Default Configuration

Table E-16 Default Configuration for the SparePartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SyslogSeverityMatchFound

This alert occurs when the SyslogSeverityMatchFound event gets generated. This indicates that a syslog message with the matching severity level exists.

Default Configuration

Table E-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogSeverityMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table E-17 Default Configuration for the SyslogSeverityMatchFound RTMT Alert (continued)

Value	Default Configuration
Syslog Severity Parameters	Critical
Enable Email	Selected
Trigger Alert Action	Default

SyslogStringMatchFound

This alert occurs when the SyslogStringMatchFound event gets generated. The alert indicates that a syslog message with the matching search string exists.

Default Configuration

Table E-18 Default Configuration for the SyslogStringMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogStringMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Syslog Alert Parameters	(Text box for search string)
Enable Email	Selected
Trigger Alert Action	Default

SystemVersionMismatched

This alert occurs when a mismatch in system version exists.

Default Configuration

Table E-19 Default Configuration for the SystemVersionMismatched RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SystemVersionMismatched occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TotalProcessesAndThreadsExceededThreshold

This alert occurs when the TotalProcessesAndThreadsExceededThreshold event gets generated. The alert indicates that the current total number of processes and threads exceeds the maximum number of tasks that are configured for the Cisco RIS Data Collector Service Parameter. This situation could indicate that a process is leaking or that a process has thread leaking.

Default Configuration

Table E-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TotalProcessesAndThreadsExceededThreshold event generated
Duration	Trigger alert immediately

Table E-20 Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default