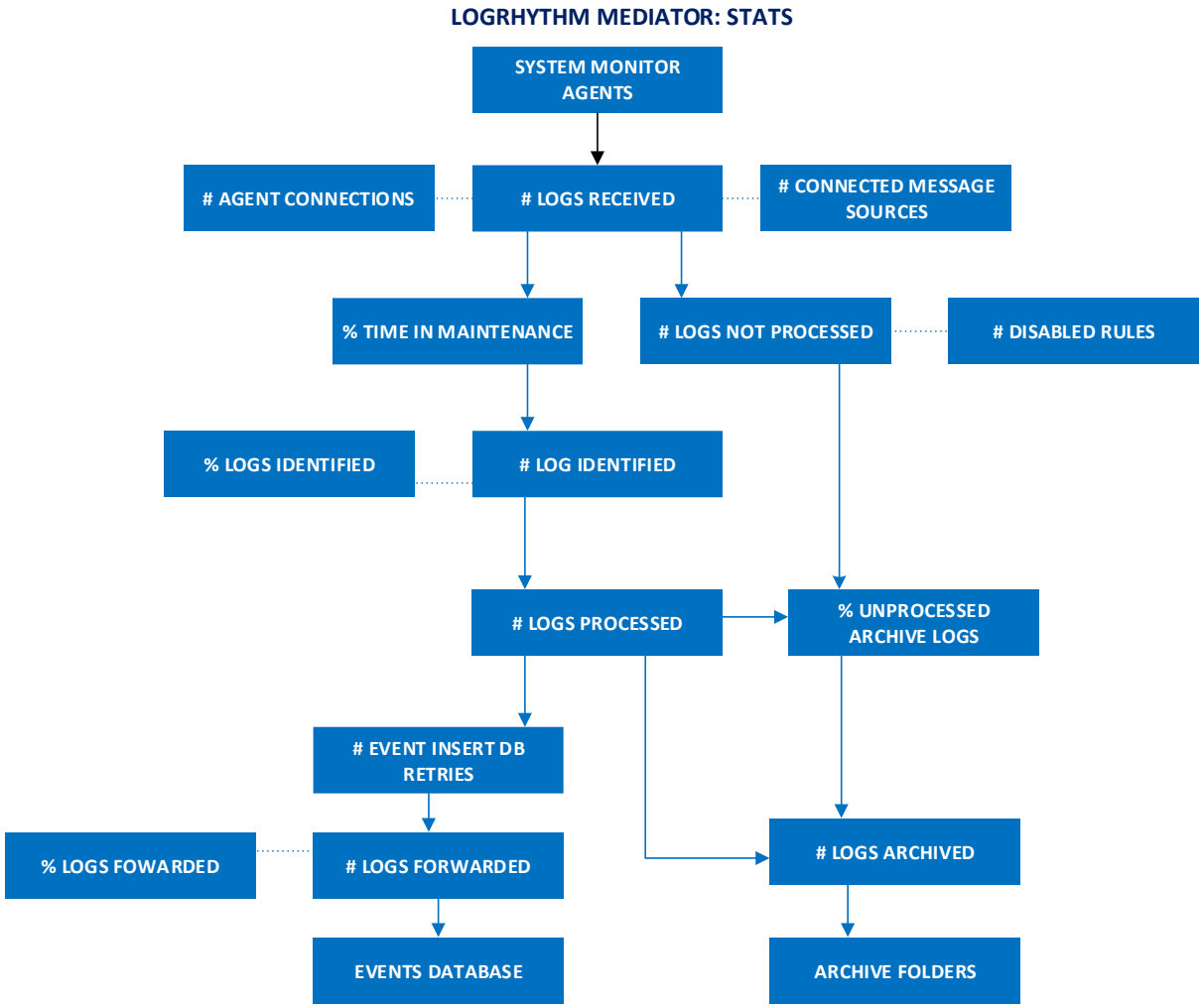
LogRhythm Performance Counter Reference Guide

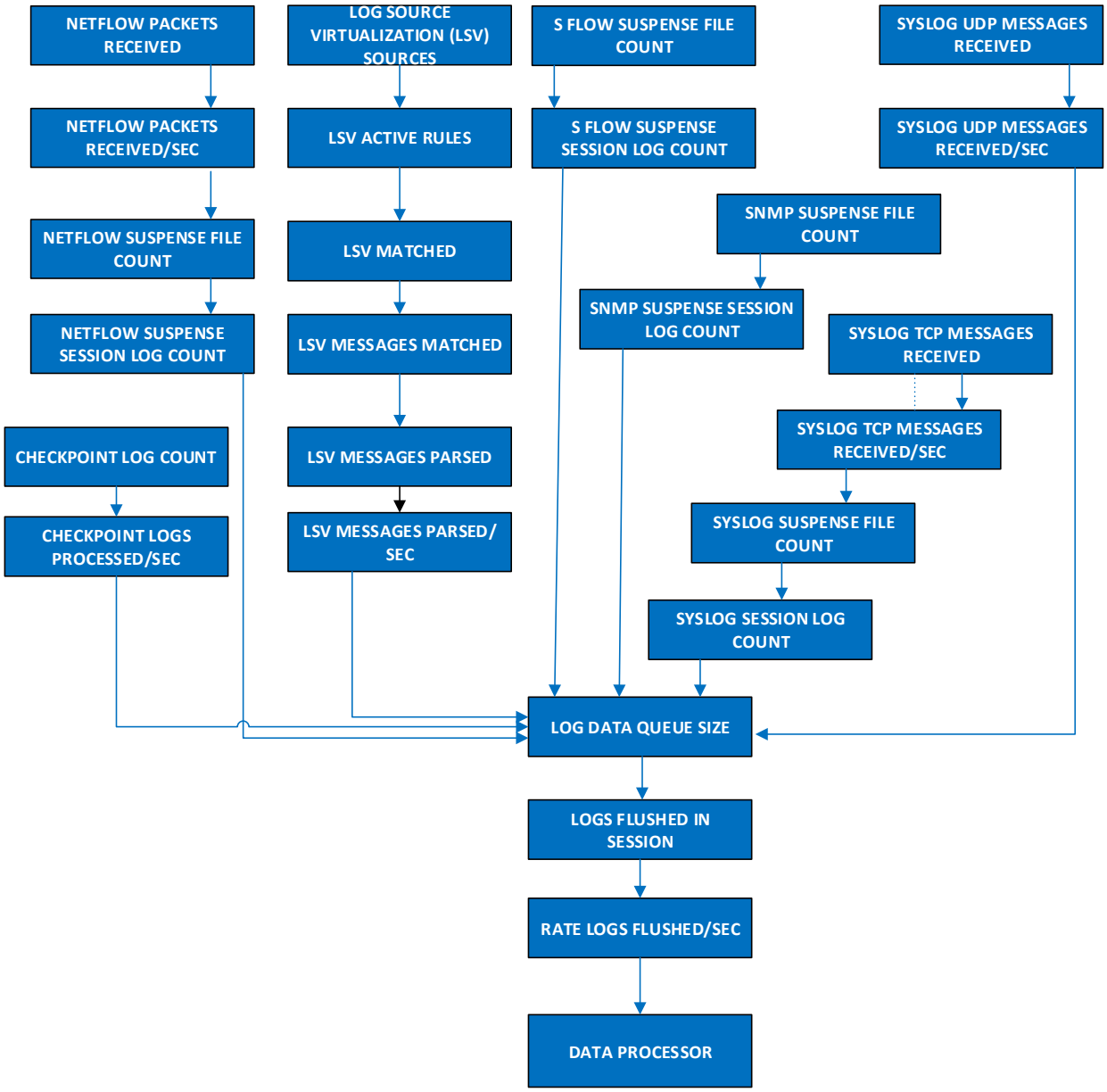
The following diagram illustrates the flow order a log takes through the LogRhythm performance counters within Windows.



LOGRHYTHM MEDIATOR - STATS

Performance Counter	Description
# Agent Connections	Number of current System Monitor Agent connections to the Data Processor.
# Connected Message Sources	Total number of Log Sources currently connected to the Data Processor.
# Disabled Rules	Total number of MPE rules that have been disabled due to poor performance.
# Event Insert DB Retries	Number of retries inserting into Events DB.
# Logs Archived	Total number of logs that have been written to the Archives.
# Logs Forwarded	Total number of logs forwarded as Events by the MPE.
# Logs Identified	Total number of logs that have matched to a MPE rule.
# Logs Not Processed	Total number of logs not yet processed by the MPE.
# Logs Processed	Total number of logs that the MPE has processed.
# Logs Received	Total number of logs received from agents.
# Unprocessed Archive Logs	Total number of unprocessed logs to be archived.
% Logs Forwarded	Percentage of processed logs that have been forwarded to the Platform Manager as events.
% Logs Identified	Percent of logs that have matched a MPE rule.
% Time in Maintenance	Percentage of time the MPE has spent performing maintenance in relation to processing cycle.

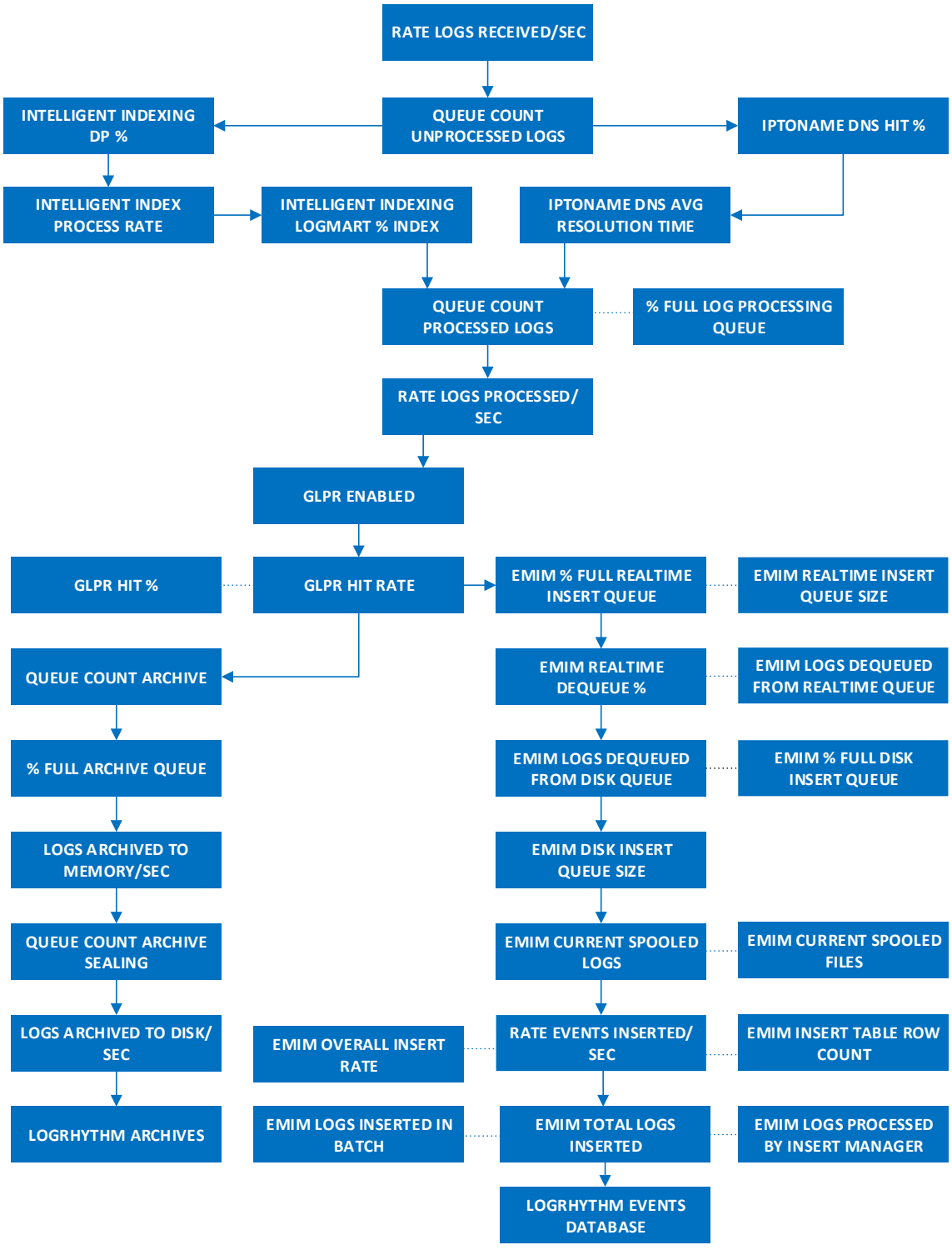
LOGRHYTHM SYSTEM MONITOR



LOGRHYTHM SYSTEM MONITOR

Performance Counter	Description
# Agent Connections	Number of current System Monitor Agent connections to the Data Processor.
# Connected Message Sources	Total number of Log Sources currently connected to the Data Processor.
# Disabled Rules	Total number of MPE rules that have been disabled due to poor performance.
# Event Insert DB Retries	Number of retries inserting into Events DB.
# Logs Archived	Total number of logs that have been written to the Archives.
# Logs Forwarded	Total number of logs forwarded as Events by the MPE.
# Logs Identified	Total number of logs that have matched to a MPE rule.
# Logs Not Processed	Total number of logs not yet processed by the MPE.
# Logs Processed	Total number of logs that the MPE has processed.
# Logs Received	Total number of logs received from agents.
# Unprocessed Archive Logs	Total number of unprocessed logs to be archived.
% Logs Forwarded	Percentage of processed logs that have been forwarded to the Platform Manager as events.
% Logs Identified	Percent of logs that have matched a MPE rule.
% Time in Maintenance	Percentage of time the MPE has spent performing maintenance in relation to processing cycle.

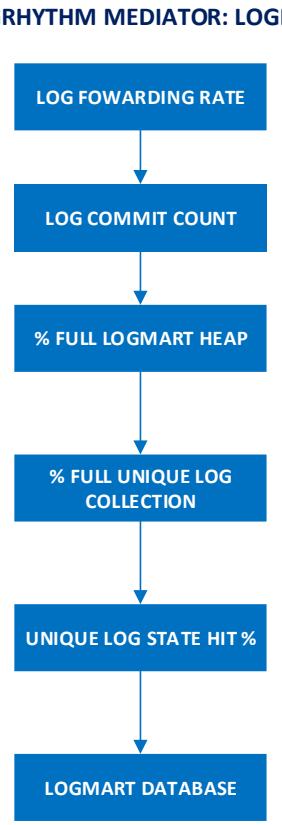
LOGRHYTHM MEDIATOR: PROCESSING



LOGRHYTHM MEDIATOR - PROCESSING

Performance Counter	Description
% Full Archive Queue	The percentage full of the Archiving queue (logs awaiting archiving). Queue Size / Queue Capacity.
% Full Log Processing Queue	The percentage full of the Log Processing queue (logs not yet processed). Queue Size / Queue Capacity
	The mediator queue size (the maximum size of the archive queue and the unprocessed log queue) can be modified in the Data Processor Advanced Properties.
EMIM % Full Disk Insert Queue	The percentage of the disk insert queue that is full of events waiting to be inserted into the Event database.
EMIM % Full Realtime Insert Queue	The percentage of the realtime insert queue that is full of events waiting to be inserted into the Event database. This counter indicates how current the insert manager is in processing the event inserts (100% means the events are being inserted in real time).
EMIM Current Spooled Files	The current number of spooled data files containing events waiting to be inserted into the Events database.
EMIM Current Spooled Logs	The current number of spooled events waiting to be inserted into the Events database.
EMIM Disk Insert Queue Size	The number of events in the disk insert queue waiting to be inserted into the Events database.
EMIM Insert Table Row Count	The number of events inserted into the Events database during the last insert operation.
EMIM Logs Dequeued From Disk Queue	The total number of events inserted into the Events database from the disk insert queue (versus the realtime insert queue) since startup.
EMIM Logs Dequeued From Realtime Queue	The total number of events inserted into the Events database from the realtime insert queue (versus the disk insert queue) since startup.
EMIM Logs Inserted In Batch	The number of events inserted into the Events database during the last insert operation.
EMIM Logs Processed By Insert Manager	The total number of events inserted by the insert manager into the Events database since startup.
EMIM Overall Insert Rate	The running insert rate for events into the Events database since startup.
EMIM Realtime Dequeue %	The percentage of events inserted into the Events database from the realtime insert queue (versus the disk insert queue) since startup.
EMIM Realtime Insert Queue Size	The number of events in the realtime insert queue waiting to be inserted into the Events database.
EMIM Total Logs Inserted	The total number of events inserted into the Events database since startup.
EMIM Total Spooled Files	The total number of spooled data files containing events waiting to be inserted into the Events database since startup.

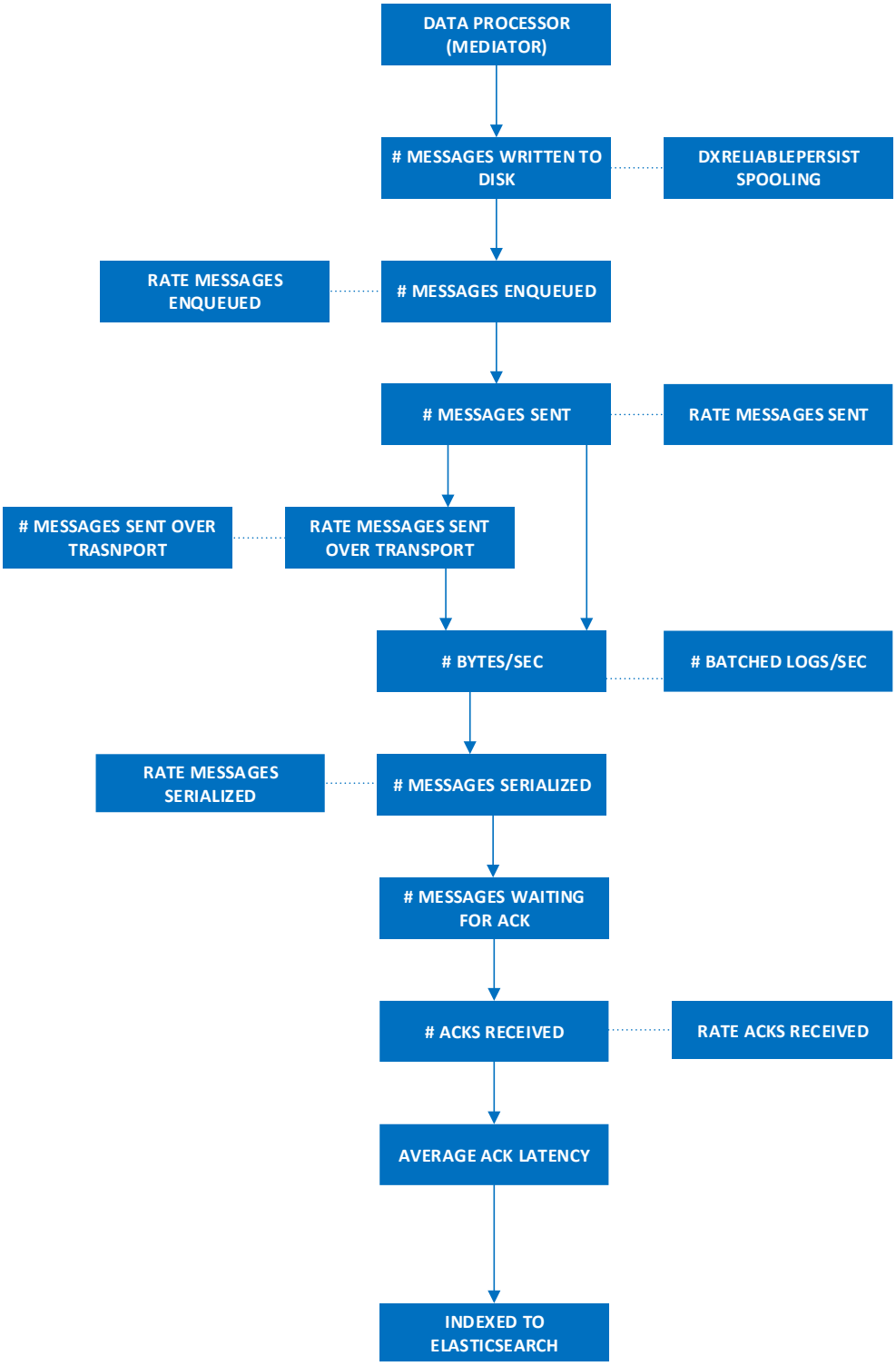
EMIM Total Spooled Logs	The total number of spooled events waiting to be inserted into the Events database.
GLPRs Enabled	The number of enabled Global Log Processing Rules.
GLPRs Hit %	The percent of logs that matched a Global Log Processing Rule
GLPRs Processing Rate	The rate at which logs are being processed by all enabled GLPRs.
Intelligent Indexing Data Processor % Indexed	The percentage of logs processed against Data Processor Intelligent Indexing rules which matched a rule.
Intelligent Indexing LogMart % Indexed	The percentage of logs processed against LogMart Intelligent Indexing rules that matched a rule.
Intelligent Indexing Processing Rate	Processing Rate for Intelligent Indexing
IPtoName DNS Avg. Resolution Time	The average time taken to perform IPToName resolution (in milliseconds.)
IPToName DNS Hit %	The percentage of IPToName DNS resolutions that resulted in a hit.
Logs Archived to Disk / Sec	The rate logs are written from memory to disk during archiving.
Logs Archived to Memory / Sec	The rate logs are queued into memory during archiving.
Queue Count Archive	The total number of logs in memory in the Archive queue. Logs in this queue are awaiting being written to disk for archiving.
Queue Count Archive Sealing	The total number of active archives awaiting sealing.
Queue Count Processed Logs	The total number of processed logs awaiting insertion into the Data Processor and Events databases.
Queue Count Unprocessed Logs	The number of logs currently in the MPE Log Processing queue.
Rate Events Inserted / Sec	The number of events inserted per second into the Events database.
Rate Logs Processed / Sec	The number of logs processed by the MPE per second.
Rate Logs Received / Sec	The number of Log Data messages received from all connected Agents per second by the scmedsvr service.



LOGRHYTHM MEDIATOR - LOGMART

Performance Counter	Description
% Full LogMart Heap	The percentage full for the LogMart heap (LoadTable).
%Full UniqueLog Collection	The percentage full for the current UniqueLog Collection. UniqueLog Count / Batch Size.
Log Commit Count	The number of UniqueLogs last committed to the LogMart insert queue (LoadTable).
Log Forwarding Rate	The rate at which logs are being forwarded for LogMart processing.
UniqueLog Hit %	The percentage of incoming logs that match an existing UniqueLog in the collection.
UniqueLogStat Hit %	The percentage of incoming logs that match an existing UniqueLogStat in the collection.

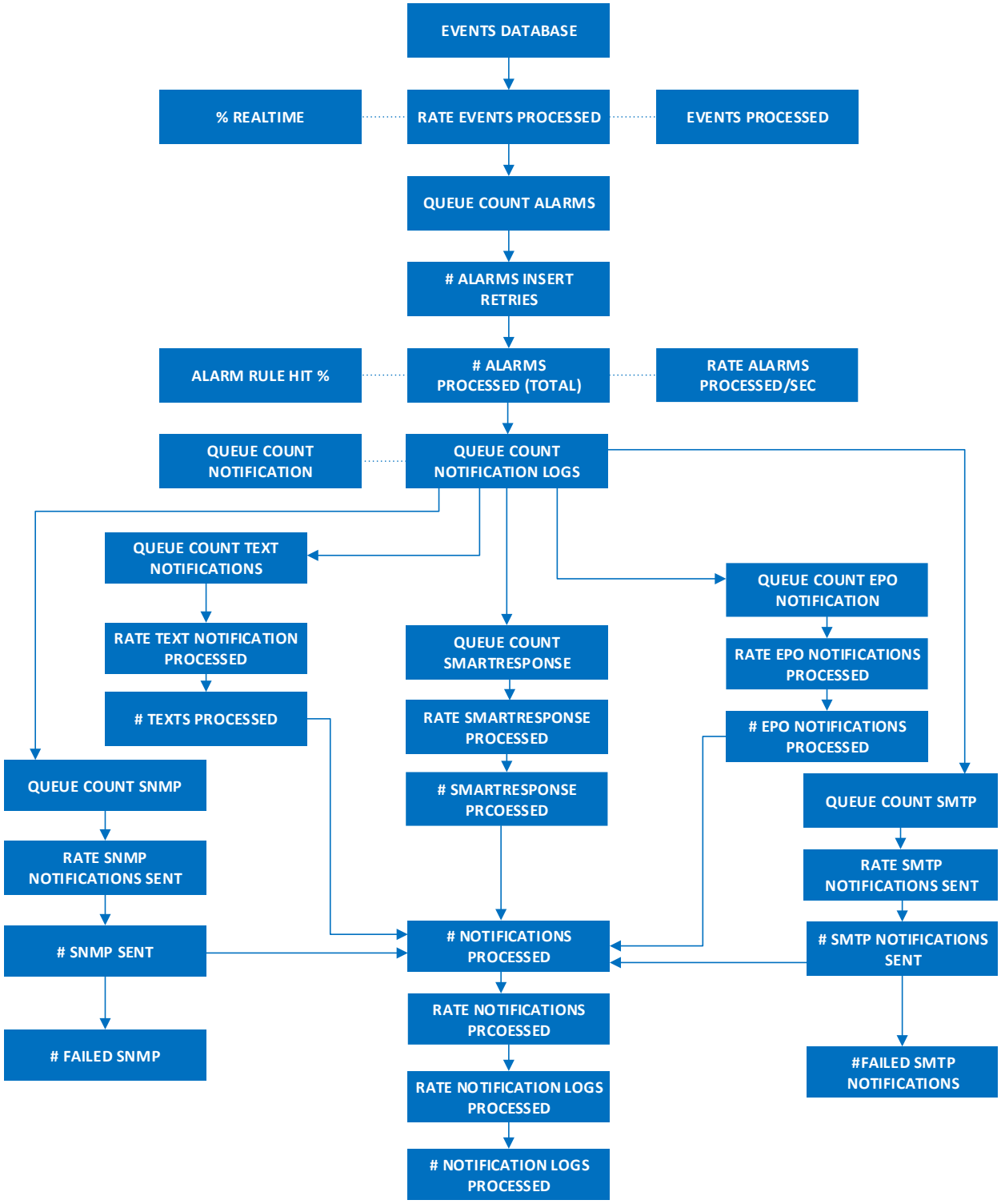
LOGRHYTHM MESSAGING (DPTODX)



LOGRHYTHM RELAIABLE MESSAGING (DPTODX)

Performance Counter	Description
# Acks Received	The total number of message acknowledgments received from the Data Indexer.
# batched logs/sec	The number of logs sent over the transport per second.
#bytes/sec	The number of bytes sent over the transport per second.
# Messages Awaiting Serialization	The total number of messages waiting to be parsed.
# Messages Enqueued	The total number of messages in the queue to be sent from the Mediator to the Data Indexer.
# Messages Sent	The total number of messages sent from the Mediator to the Data Indexer.
# Messages Sent over Transport	The number of API Gateway messages sent.
# Messages Serialized	The total number of messages parsed.
# Messages Waiting for Ack	The total number of messages sent to but not yet acknowledged by the Data Indexer.
# Messages Written to Disk	The total number of messages written to disk for reliable messaging. If # Messages Enqueued is greater then 500,000, raw messages will be written to disk so that no messages are lost.
Average Ack Latency	The average amount of time it takes for an ack to come back.
Rate Acks Received	The number of acknowledgments received from the Data Indexer per second.
Rate Messages Enqueued	The number of messages (per second) that are ready to be sent from the Mediator to the Data Indexer (messages that are parsed but have not been sent to the Data Indexer).
Rate Messages Sent	The number of messages that are being sent per second from the Mediator to the Data Indexer.
Rate Messages Sent over Transport	The number of messages sent per second for API Gateway.
Rate Messages Serialized	The number of messaged parsed per second.
Transport Errors Since Subsystem Start	The number of errors in the transport since service start.

LOGRHYTHM ALARM AND RESPONSE MANAGER



LOGRHYTHM ALARM AND RESPONSE MANAGER

Performance Counter	Description
# Alarms Insert DB Retries	The total number of alarm bulk insert DB retries.
# Alarms Processed	The total number of unique alarms generated and processed by the ARM service since it was last started.
#ePO Notifications Processed	The total number of ePO notifications processed.
# Events Processed	The total number of events processed by the ARM service since last started.
# Failed SMTP Notifications	The total number of failed SMTP notifications (errors when sending an alarm to a LogRhythm user) processed by the ARM service since it was last started.
# Failed SNMP Notifications	The total number of failed SNMP (trap) notifications (errors when sending a trap notification to an SNMP receiver) processed by the ARM service since it was last started.
# Notifications Logs Processed	The total number of notification logs processed.
# Notifications Processed	The total number of notifications processed.
# SmartResponse™ Processed	The total number of SmartResponse™ actions processed.
# SMTP Notifications Sent	The total number of SMTP (email) notifications sent by the ARM service since it was last started.
# SNMP Notifications Sent	The total number of SNMP (trap) notifications sent by the ARM service since it was last started.
# Text Notifications Processed	The total number of text notifications processed.
% Realtime	How current the ARM is in processing the event stream. 100% means the events are being processed in real time.
Alarm Rule Hit %	The percentage of events matching one or more Alarm Rules.
Queue Count Alarms	The number of alarms, new and existing, queued for processing and awaiting insertion into the EMDB.
Queue Count ePO Notifications	The number of ePO notifications, new and existing, queued for processing.
Queue Count Notification Logs	The number of notification logs, new and existing, queued for processing.
Queue Count Notifications	The number of notifications, new and existing, queued for processing.
Queue Count SmartResponse™	The number of SmartResponse™ actions, new and existing, queued for processing.
Queue Count SMTP	The number of SMTP (email) notifications, individual and batch, queued for notification.
Queue Count SNMP	The number of SNMP trap notifications queued for notification.
Queue Count Text Notifications	The number of text notifications, new and existing, queued for processing.
Rate Alarms Processed	The number of alarms, new and existing, processed per second.
Rate ePO Notifications Processed	The number of ePO notifications processed per second.
Rate Events Processed	The number of events processed per second.
Rate Notification Logs Processed	The number of notification logs processed per second.

Rate Notifications Processed	The number of notifications processed per second.
Rate SmartResponse™ Processed	The number of SmartResponse™ actions processed per second.
Rate SMTP Notifications Sent	The number of SMTP (email) notifications, individual and batch, sent per second.
Rate SNMP Notifications Sent	The number of SNMP trap notifications sent per second.
Rate Text Notifications Processed	The number of text notifications processed per second.