

See IMS Log Data More Clearly

TABLE OF CONTENTS

NEEDLE IN A HAYSTACK 1
BMC LOG ANALYZER FOR IMS 3
USE CASES. 6
CONCLUSION 7

NEEDLE IN A HAYSTACK

IMS today is not your father's IMS. Over the years, it has evolved from a few databases running on one IMS image to data sharing across multiple IMS images, to access from DB2 and CICS/DBCTL, and even to access from the Internet. Applications that were written in the 1970s-1980s were simpler than today's applications; the databases and systems were more finite and more clearly defined. But as IMS has expanded, the applications have become far more complex – even simple applications span multiple IMS images and spawn business processes that run on several IMS systems. Other applications enter requests from the web and switch between WebSphere Application Server, IMS Connect, WebSphere MQ, CICS, IMS, and DB2.

The ability to open IMS to the web has breathed new life into the legacy databases, but it has also added a great deal of complexity. When business processes and applications fail in these mixed environments, it can be difficult and time-consuming to determine what caused the problem. Making matters worse, the problems are more visible because many different systems and users are involved; an outage in a web application may generate headlines as well as cause expense and possibly lost business.

When you have a problem in IMS, how do you find what caused it? The new world of IMS has lots of potential failure points. Finding the root cause of a problem can be like trying to find a needle in a haystack.

NOT ALL PROBLEMS ARE RELATED TO PERFORMANCE

You may think that your problem is related to performance, but performance issues cause only about 25 percent of application problems. The other 75 percent of problems arise from communication failures, application errors, and data integrity issues.

Monitoring tools use real-time information to alert you when performance thresholds are not met or when abends occur. They provide a real-time view of the system and can tell you how long it took for a transaction to complete, but they don't have the benefit of providing an historical, detailed view of business application flows. To diagnose incorrect results or integrity problems, it is essential to understand detailed historical information, which is stored in the IMS logs.

Other examples of problems that are not related to performance include:

- » A problem occurs every Wednesday at 2:00 p.m. What is causing that problem? Why is the database getting out of sync?
- » A user calls the help desk the day after they experienced slow response times. How can you analyze the transaction workload for this user and determine why they experienced slow response times several days earlier?

You could analyze the IMS log records associated with the time frame when these problems occurred – a task that could take hours, or even days. But will solving these problems be at the top of your priority list, or will you be working on today's hot problem?

By using the information in the IMS logs, you can determine what caused an IMS problem; however, manually gathering information from the IMS logs is difficult.

IMS LOGS

The IMS logs, more commonly known as online log data sets (OLDS) and system log data sets (SLDS), record and store a wealth of information, including:

- » Receipt of an input message in the input queue and successful receipt of an output message by a terminal
- » Online transaction information, including receipt of a message and insert of a message into a queue
- » Start and termination of programs
- » Users signing on, signing off, and performing actions
- » Before and after images of database updates by programs

IMS logs contain the answer to almost any question that you could ask about your IMS environment and the activities and events in that environment. But the primary purpose of IMS logs is simply to record the information, not to organize and present it in a way that you can easily use. Records have cryptic contents, and the quantity of records in logs can be daunting – a log can contain millions of records, and many log data sets can be written in a relatively short span of time.

READING AND ANALYZING LOG DATA IS DIFFICULT

The quantity and complexity of IMS log records can make your head spin. It takes an IMS expert to determine which log data sets and log records are needed for problem diagnosis and what those records mean. Even if you are an expert, it can be difficult, time-consuming, and error-prone to find and access the information you need. If an unplanned outage or a critical problem occurs, diagnosis time can be costly.

The real challenge is finding the cause of a problem in the volumes of information in the IMS logs. For example, a user may have reported unexpected (and unexplained) updates to a database. It could be something as simple as faulty application logic updating a field incorrectly. It could be as complex as a transaction that updates the account number in the customer database, then incorrectly spawns a remote transaction to run on another IMS and the second transaction is doing the undesired updates from the wrong IMS system. If you knew why the problem was occurring, you could fix the problem easily. How do you find out why the problem happened?

The information you need to diagnose the problem is often somewhere in the IMS logs, but the log records you need are mixed in with millions of records that are not relevant to the problem. You need a complete view of the application flow in context with the other activity that was occurring when the transaction was executing. In addition, clues about the problem might be contained in many different types of log records, and you need an understanding of the contents of the relevant records and how they correlate to each other.

IMS provides tools that allow you to dump the IMS log records and to select and view the records individually. You may have written your own tools to correlate some of the IMS records and better understand application flow, or you may have written ad-hoc reports when a failure occurred. You may have developed a process to get this information with REXX EXECs or SAS reports. But who maintains this process when a new version of IMS is released and the format of the log records is changed or new types of log records are added?

If you are responsible for diagnosing IMS problems, you need a tool that can determine which log records to analyze and then analyze them. You need a tool that can:

- » Summarize millions of log records into concise, logical units of work and provide a view of the IMS transactions and the application flow that is represented on the IMS logs
- » Provide a big-picture view of application processing, regardless of how many transaction message switches occurred or how many IMS systems were involved
- » Explain “who did what?” during a specific time frame, and what exactly they did

AUDITING

At times, you may be asked to investigate the actions of a particular user. With compliance regulations, you may be receiving more of these requests. You may be asked to track unethical activity by employees. For example, a service representative at a phone company may apply a payment to the account of a friend – even though the payment was never received. The log records can provide supporting documentation to the legal department.

The IMS logs contain the information you need, but how can you find that information easily?

BMC LOG ANALYZER FOR IMS

When you have an IMS problem, check your monitoring tool to see whether the problem is related to performance. For performance problems, follow your standard procedures. For problems that are not caused by performance (for example, application errors or data integrity issues), you must turn to the IMS logs. Because the IMS logs are too overwhelming to analyze manually, you need a tool to simplify the process.

BMC Log Analyzer for IMS gathers the log records that are relevant to the problem and presents the log data in an understandable form. It correlates the raw data in the logs into an application flow for a business view. It organizes log records by finding the specific records you need, grouping related records into logical units of work (LUOWs), sorting them, and identifying them with understandable labels.

BMC Log Analyzer for IMS makes it easy to diagnose problems, such as transaction failures and delays, in an IMS environment. You can trace all events that are related to an activity. Traditional DFSERA10, 30, and 70 records provide the ability to see a transactional flow – if you are an IMS expert and have the time to choose the correct records. With BMC Log Analyzer for IMS, that relationship is easily viewable, especially with the ISPF interface. You can zoom to choose the level of detail you want.

BMC Log Analyzer for IMS

- » Synthesizes millions of log records into a few pertinent work flows and correlates all related log records into a concise view that reflects all events for an IMS transaction or application flow
- » Provides a big-picture view of application processing, regardless of how many transaction message switches occurred or how many IMS systems were involved, and helps less experienced technicians to understand application flows
- » Enables you to drill down from a logical view of the application flow into detailed views of the individual records that comprise the transaction
- » Enables you to search for pertinent log records by a specified criteria, perform complex searches with combinations of criteria, and search for specific log records
- » Shows a transaction in context with all other activity that was occurring in the system
- » Audits user, terminal, database, and other activities to explain “who did what?” during a specific time frame, and exactly what they did

For example, BMC Log Analyzer for IMS can show you that an application program is updating an address field incorrectly. You could then use a database recovery tool to restore the database and make the updates to the application program so that it no longer updates a database unexpectedly.

The overall infrastructure of BMC Log Analyzer for IMS is simple. You do not need a z/OS, network, or even detailed IMS background to understand how it works.

LOGICAL UNITS OF WORK

To determine the root cause of a problem, you must know which log records are relevant: log records that represent important actions related to a particular IMS object (transaction, database, user, and so on).

BMC Log Analyzer for IMS organizes log information into logical units of work (LUOWs), which provide a more comprehensive, useful view of activities in your IMS systems than a simple unit of work (UOW) can provide. A UOW is a familiar concept in the IMS environment:

- » In an IMS DB environment, a UOW comprises all input and output messages that are associated with a transaction.
- » In an IMS TM environment, a UOW comprises a single IMS message.
- » In an IMS Shared Queues (CQS) environment, a UOW comprises a client-defined grouping of data objects.

Figure 1 shows a typical transaction UOW. A message arrives in IMS and is placed on a message queue. The message is scheduled for execution. Application processing occurs, including DL/I database calls. All processing is completed, a sync point is taken, and an output message is sent.

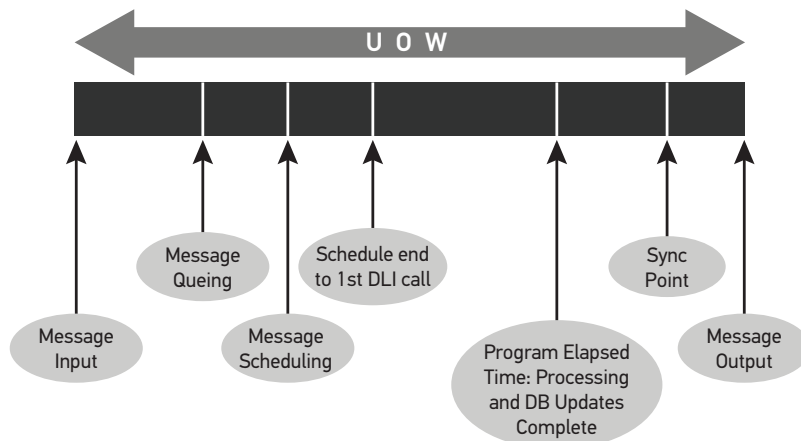


Figure 1 Unit of work example

BMC Log Analyzer for IMS identifies logical UOWs to provide more meaningful insights into complex activities than a view of isolated UOWs can provide. An LUOW captures the entire application flow across boundaries of UOWs, message switches, IMS systems, sysplexes, and LPARs. Processing on non-IMS platforms is also represented in an LUOW to give you a complete view of the application flow.

The logical unit of work contains just the information you need – when you need it. To create LUOWs, BMC Log Analyzer for IMS uses a patent-pending process to associate log records with each other by matching the values of certain fields (such as the UOW-1 field and the recovery token field) in those records.

Figure 2 shows typical activities in an LUOW.

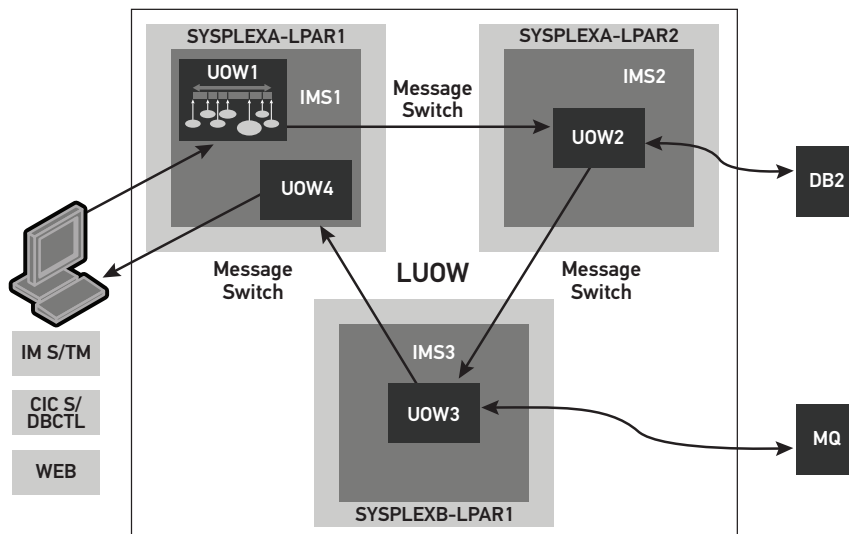


Figure 2 Logical unit of work example

For each log record that is identified as a candidate for the record selection process, BMC Log Analyzer for IMS determines whether the record belongs to an LUOW that has already been created and, if so, associates the record with that LUOW. If not, BMC Log Analyzer for IMS creates a new LUOW and associates the record with it.

By focusing on an LUOW (which contains just the information you need) instead of the voluminous log records, you are automatically set on a path of success. For example, if a failure occurred in an application around 10:00 a.m., you can simply choose by time frame, transaction ID, or database. You can extract the information that is relevant to the situation and filter out the rest.

TYPES OF LUOWS

BMC Log Analyzer for IMS creates the following types of LUOWs:

- » Transaction LUOWs. A transaction typically has an origin (a source, such as an LTERM), a destination (such as another LTERM), and an originating user.
- » Miscellaneous LUOWs. A miscellaneous LUOW has no identifiable origin, destination, or user ID. This type of LUOW is often the result of work that IMS systems must perform to move data between systems in a shared-queue environment. A miscellaneous LUOW might also result from a traditional transaction that did not contain a type-01 record or a type-03 record, possibly because the record was written to a log that was not included in the input to the analysis job or because the record had a time stamp that was not within the specified range for analysis.
- » Non-transaction LUOWs. Non-transaction LUOWs represent events that are not directly related to transactions, including users signing on to/off from the system, databases being opened and closed, databases taking extents, system checkpoints being taken, and so on. BMC Log Analyzer for IMS assigns each event to a separate LUOW.

OUTPUT PROCESSING

BMC Log Analyzer for IMS produces the following output:

- » Batch reports that show which LUOWs were created (log records that were processed can be written to SYSOUT-type data sets).
- » Index files that contain information about LUOWs and associated log records.
- » Extract files that contain copies of all log records that have been associated with LUOWs of interest. You can use the extract file as input to a subsequent analysis job.
- » BMC Log Analyzer for IMS retains the LUOWs so that if you need them for subsequent processing, you have them. Other tools use serial processing to analyze log records, but they do not retain that information. If you need the information later, you must rerun the log analysis job and incur the CPU and elapsed time associated with it.

DATABASE UPDATE ACTIVITIES

Sometimes you need to identify which updates have been made to an IMS database. For example, you might need to diagnose the cause of a database integrity problem because “someone” incorrectly updated the database or an application program was in error. BMC Log Analyzer for IMS can provide correlated information on all updates to a database from all IMS systems at a given time with the exact IOPCB of those application calls.

MESSAGE SWITCHING AND MSC TRAFFIC

BMC Log Analyzer for IMS can help to diagnose problems with transactions in message-switching environments and with MSC traffic. The ideal way to trace message-switching transactions is to collect data from each remote site by creating an extract file and forwarding that file to the local site. At the local site, you can execute a job that uses the remote extract file as input and processes local log data sets. This produces comprehensive reports showing all records that were produced for the transactions.

You can analyze MSC traffic even if the data from one or more of the participating remote IMS systems is not available. If you are analyzing data from a single IMS that is in an MSC environment, you see log records for the transactions from the local system.

Some log records show the outbound messages or transactions being enqueued to the MSLink names for delivery to another IMS. Other log records show the replies or messages from the MSLink as the transaction came back to the originating IMS system.

AUDITING

In our compliance-conscious environment, it is increasingly important to see who does what and when they do it. You know that all activities are recorded in the IMS logs, and you need to be able to find specific information quickly and present it to someone who may not be familiar with IMS at all. They just want answers. BMC Log Analyzer for IMS makes it easy to find the information you need and provides the data in simple, concise reports. The Audit reports can be used to establish base lines and monitor trends, as well as provide data in legal matters.

FLEXIBILITY AND INTELLIGENCE

BMC Log Analyzer for IMS is easy enough for novices to use, but flexible enough to accommodate the needs of expert IMS technicians. IMS logs can contain extremely large amounts of data and a human can work with only a few hundred records at a time. Flexible and powerful search capabilities are essential. BMC Log Analyzer for IMS provides filters and a zoom capability that is invaluable when narrowing or expanding a search and weeding out irrelevant records.

By using filters, you can search for specific log records. You can

- » Search for various types of targets (such as user IDs, transaction origins and destinations, and database names)
- » Include and exclude specific types of log records (such as including sign-on and sign-off records and excluding padding records)
- » Use a combination of filters with Boolean logic
- » Search for content in IMS transaction input and output messages
- » Zoom in and zoom out to narrow or expand a search and weed out irrelevant records – for example, start with a general time stamp and a target, then zoom in or out as needed to find specific information

APPLICATION DEVELOPMENT AND TESTING SUPPORT

As you make application changes, you can use BMC Log Analyzer for IMS to verify that the application works as planned. You can see exactly what occurred by looking at the LUOW. You can verify that updates were made to the correct database. You can see specific information, including the DBD name, data set ID, PSB name, database organization (HDAM, HALDB, and so on), data set organization (VSAM/OSAM), DL/I call type, and physical I/O function (such as insert, replace, delete).

USE CASES

Customers have used BMC Log Analyzer for IMS to find application errors quickly, to improve performance, and to determine who made changes.

FIND APPLICATION ERRORS

A funds transfer application at a financial institution erroneously posted a \$2M funds transfer as a \$4M transaction. The end user had an incorrect balance, but was unable to determine why. The IMS system programmer used BMC Log Analyzer for IMS to view the LUOW flow, which allowed the application team to identify and resolve the problem. They found that the error was caused by the application not checking the status code.

A financial institution needed to diagnose an application problem. Using data from the 01 log records, BMC Log Analyzer for IMS enabled the technician to quickly identify that the same client number reissued the same transaction repeatedly. By using BMC Log Analyzer for IMS, the technician saved time by finding pertinent information quickly and easily.

End users at a financial institution were experiencing outages. The IMS system programmer used BMC Log Analyzer for IMS and found that an application was message switching and attempting to run on an IMS system that it was not defined for. Without the product, it could have taken days or weeks to find the cause of the outages.

FINE-TUNE PERFORMANCE

The IMS systems at a telecommunications company performed well, but the company wanted to see if they could save CPU resources and improve application performance. They used BMC Log Analyzer for IMS to analyze checkpoint frequency. From the standard LUOW Summary Report, the IMS system programmer was easily able to determine which applications were taking excessive checkpoints. They found that applications created over 20 years ago used a checkpoint interval based on old CPU speeds. With the new high-speed CPUs, the applications were taking 10-20 times as many checkpoints as needed, thus causing performance problems. To reduce the checkpoint frequency and thereby improve performance, the system programmer implemented BMC APPLICATION RESTART CONTROL for IMS, which enabled a change in checkpoint frequency with no changes to the application program.

AUDIT

An insurance company was conducting an audit and needed to know if a specific user had made updates to a life insurance database at a specific time. The auditor specified the user name and time variable, and BMC Log Analyzer for IMS determined which log tapes were required and which log records to pull, then produced the exact report the auditor needed.

CONCLUSION

IMS log records have all the information you need to find what caused a problem, but it is difficult to manually collect, correlate, and understand the records that are relevant to the problem. BMC Log Analyzer for IMS makes sense of the voluminous IMS log records. You don't need to be an IMS expert to find what caused a problem. Simply enter a set of criteria for the information you need, and BMC Log Analyzer for IMS correlates the log records to give you just what you need, when you need it.

BMC Log Analyzer for IMS automates tedious and difficult tasks that are required for analysis of data in IMS log records. BMC Log Analyzer for IMS

- » Selects only the log records that are relevant for your needs
- » Creates and maintains LUOWs, sorting them for logical presentation, and identifying them with understandable labels
- » Presents the information you need in a way that you can understand it easily

BUSINESS RUNS ON IT. IT RUNS ON BMC SOFTWARE.

Business thrives when IT runs smarter, faster, and stronger. That's why the most demanding IT organizations in the world rely on BMC Software across both distributed and mainframe environments. Recognized as the leader in Business Service Management, BMC offers a comprehensive approach and unified platform that helps IT organizations cut cost, reduce risk, and drive business profit. For the four fiscal quarters ended March 31, 2009, BMC revenue was approximately \$1.87 billion. Visit www.bmc.com for more information.

