AWS CLOUD OBSERVABILITY WITH LOG ANALYTICS

There are many types of logs in Amazon Web Services (AWS), and the more applications and services you run in AWS, the more complex your logging needs are bound to be. Logs originate from two primary sources—applications running on AWS services, and the AWS services themselves. An AWS centralized logging solution, therefore, becomes essential to manage this complexity. To achieve this kind of end-to-end visibility requires a conscious effort to centralize all the disparate logging data irrespective of their source of origin. AWS provides CloudWatch to centralize this data. CloudWatch is the primary collector that collects logs from different AWS services such as Amazon VPC Flow Logs, Route 53 Logs, Lambda Logs, CloudTrail Logs, and so on, in addition to log data from applications like Nginx or Apache system that you may be using in your AWS deployment.

Once collected in CloudWatch, you can use the BMC Helix Log Analytics solution to monitor and analyze logs and set up alerts. Doing this, you can get the native benefit of AWS log collection and the analytical power of the machine learning (ML)-powered observability platform provided by BMC. The ability to collect logs from CloudWatch allows you to aggregate all your log data combined with data from other sources across hybrid and multi-cloud environments. BMC Helix Log Analytics provides advanced monitoring and alerting capabilities to derive meaningful insights from logs, such as filtering by log metadata; enriching logs to add meaningful context; customizing alert messaging; automated alerting with ML-assisted anomaly detection; and service monitoring with BMC Helix Operations Management with artificial intelligence for IT operations (AIOps).

Centralized AWS logging with BMC Helix Log Analytics

The following diagram shows logs being collected from different applications and services across different AWS regions. CloudWatch collects logs by defining log streams and log groups for each region. A log stream is a sequence of log events coming from the application instance or resource being monitored. For example, a log stream may be associated with an Apache access log on a specific host. Log groups define groups of log streams that share the same retention, monitoring, and access control settings. One or more log streams belong to a log group. If you have a separate log stream for the Apache access logs from each host, you could group those log streams into a single log group called MyWebsite.com/Apache/access log.

Logs are aggregated in CloudWatch, and then collected and stored in BMC Helix Log Analytics for further analysis.

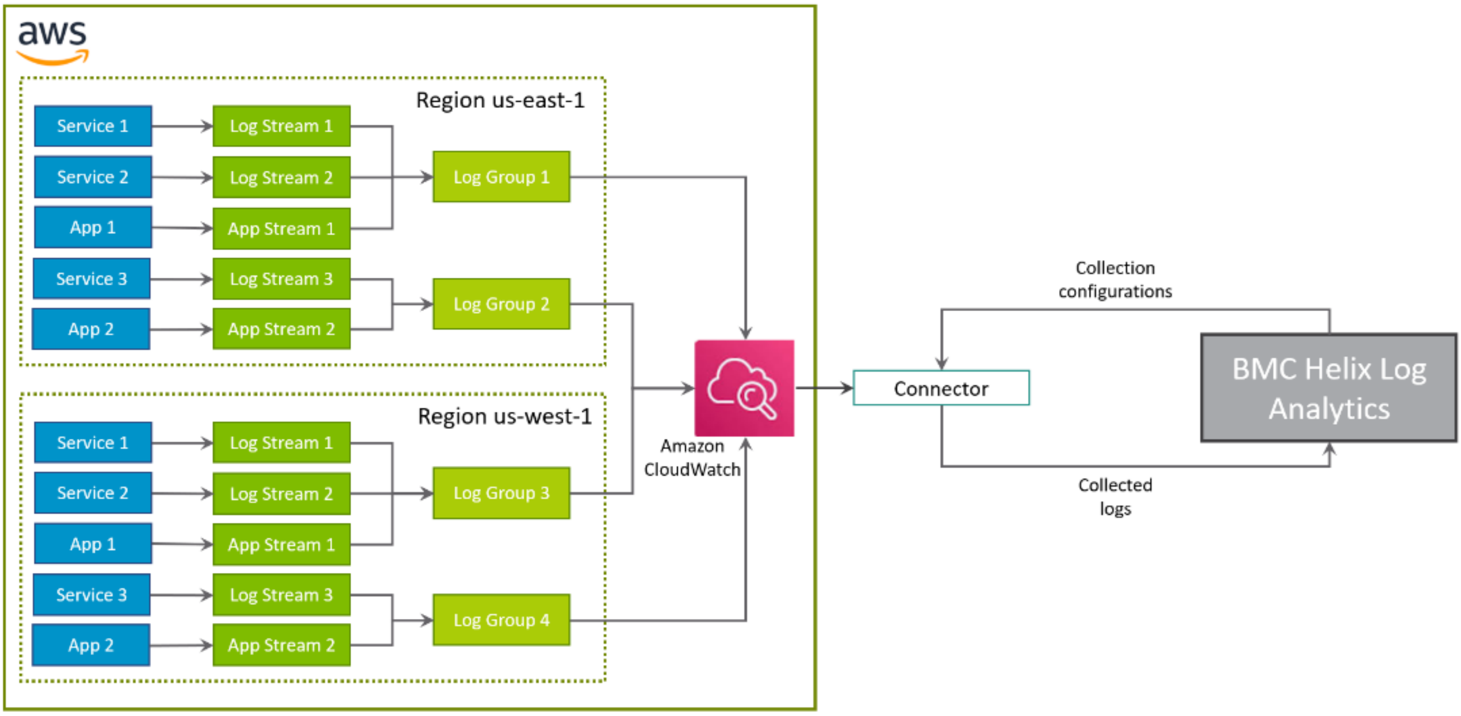
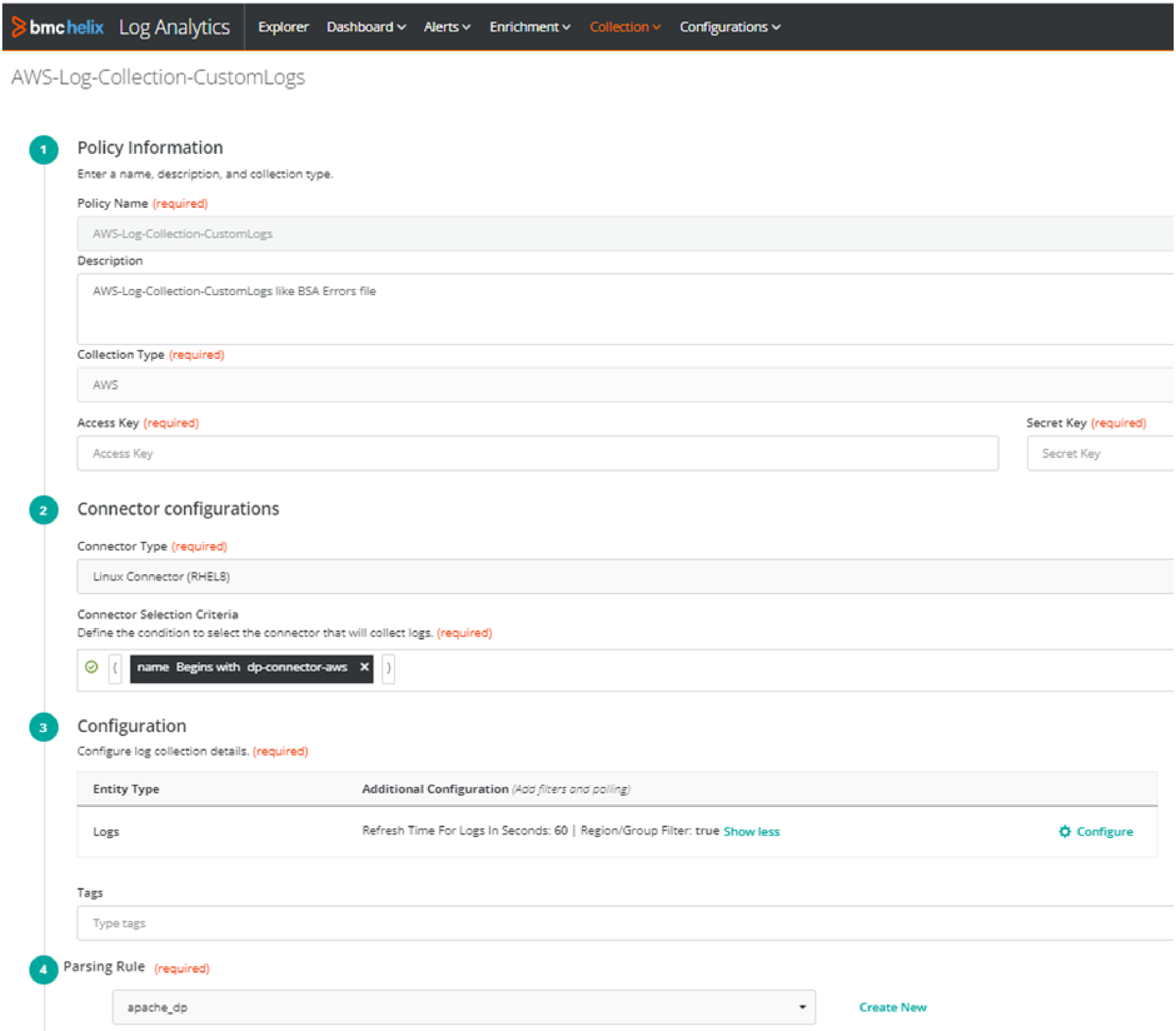


Figure 1. Collecting logs from AWS deployment

Collecting logs

BMC Helix Log Analytics uses a log collection policy to collect logs from AWS CloudWatch. To configure the collection policy, you must provide credentials to access the AWS account that contains the logs to be collected. Next, you would need to download and install the connector on the AWS platform to collect application or services logs for monitoring.



AWS-Log-Collection-CustomLogs

1 Policy Information

Enter a name, description, and collection type.

Policy Name (required): AWS-Log-Collection-CustomLogs

Description: AWS-Log-Collection-CustomLogs like BSA Errors file

Collection Type (required): AWS

Access Key (required): Access Key

Secret Key (required): Secret Key

2 Connector configurations

Connector Type (required): Linux Connector (RHEL8)

Connector Selection Criteria

Define the condition to select the connector that will collect logs. (required)

(name Begins with dp-connector-aws ✕)

3 Configuration

Configure log collection details. (required)

Entity Type	Additional Configuration *(Add filters and polling)*	
Logs	Refresh Time For Logs In Seconds: 60 | Region/Group Filter: true Show less	Configure

Tags: Type tags

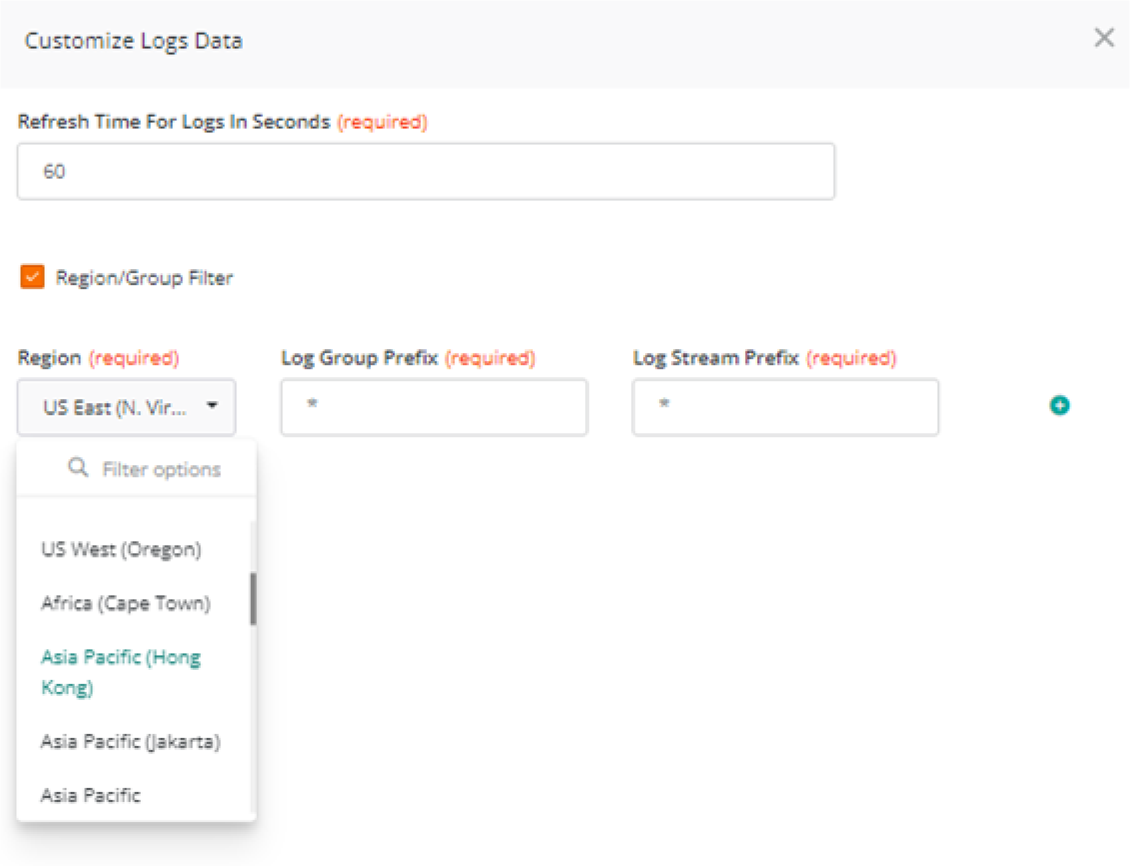
4 Parsing Rule (required)

apache_dp ▾ Create New

Figure 2: Log policy for collecting AWS logs

You may configure the refresh time and provide details of the region, log groups, and log streams for the logs to be collected.

You can also specify the application format to parse logs and provide log filters to include or exclude specific data. Log parsing helps to convert unstructured raw logs into meaningful key-value pairs and make them ready for analysis. It also enables you to get statistics on log message parameter values, conduct faceted searches, and filter logs by specific fields and values.



Customize Logs Data

Refresh Time For Logs In Seconds (required)

60

☑ Region/Group Filter

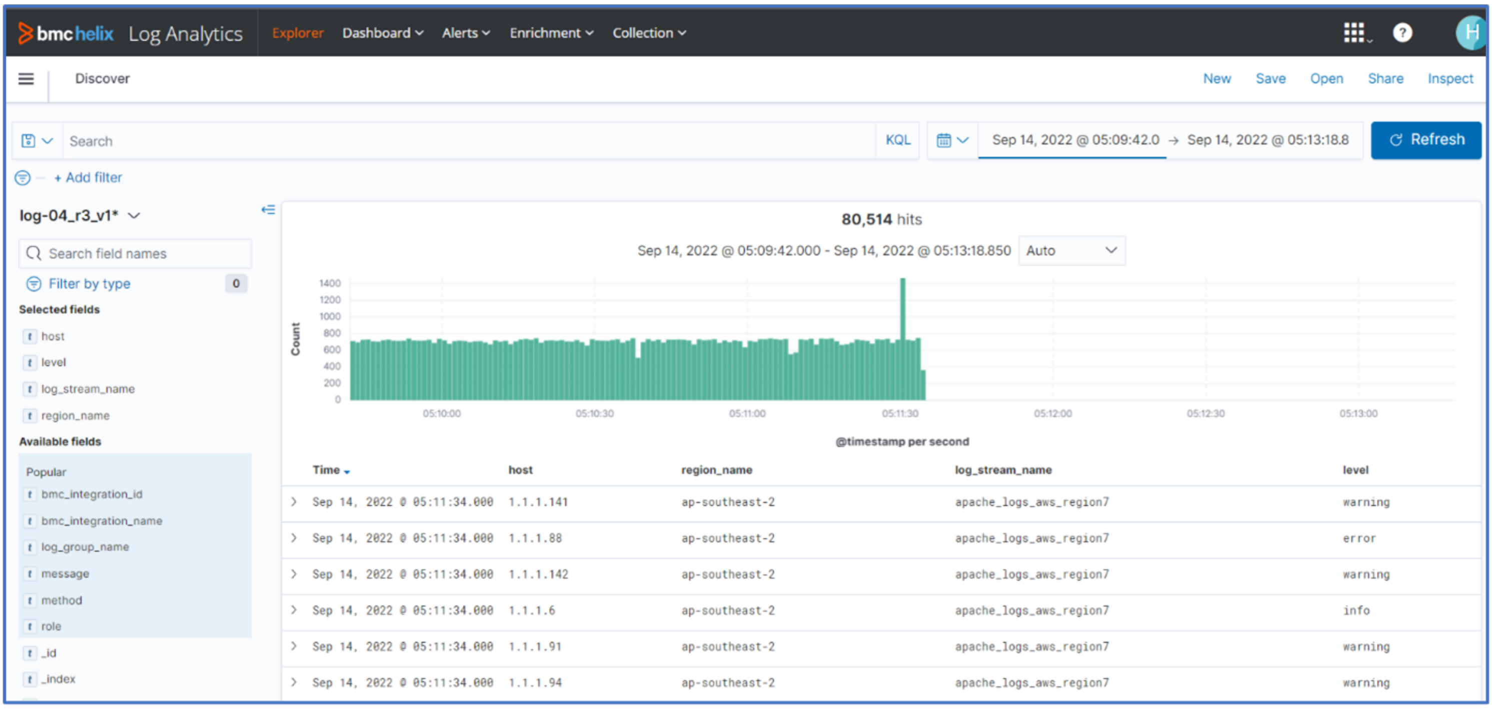
Region (required)	Log Group Prefix (required)	Log Stream Prefix (required)
US East (N. Vir...	*	*

Figure 3: Configure AWS logging

Once the configuration is done, you can see the health status of the log connector and policy configured to ensure there is no error with log collection. Then you can start to analyze logs in Explorer and create alerts and other policies as appropriate.

Monitoring logs

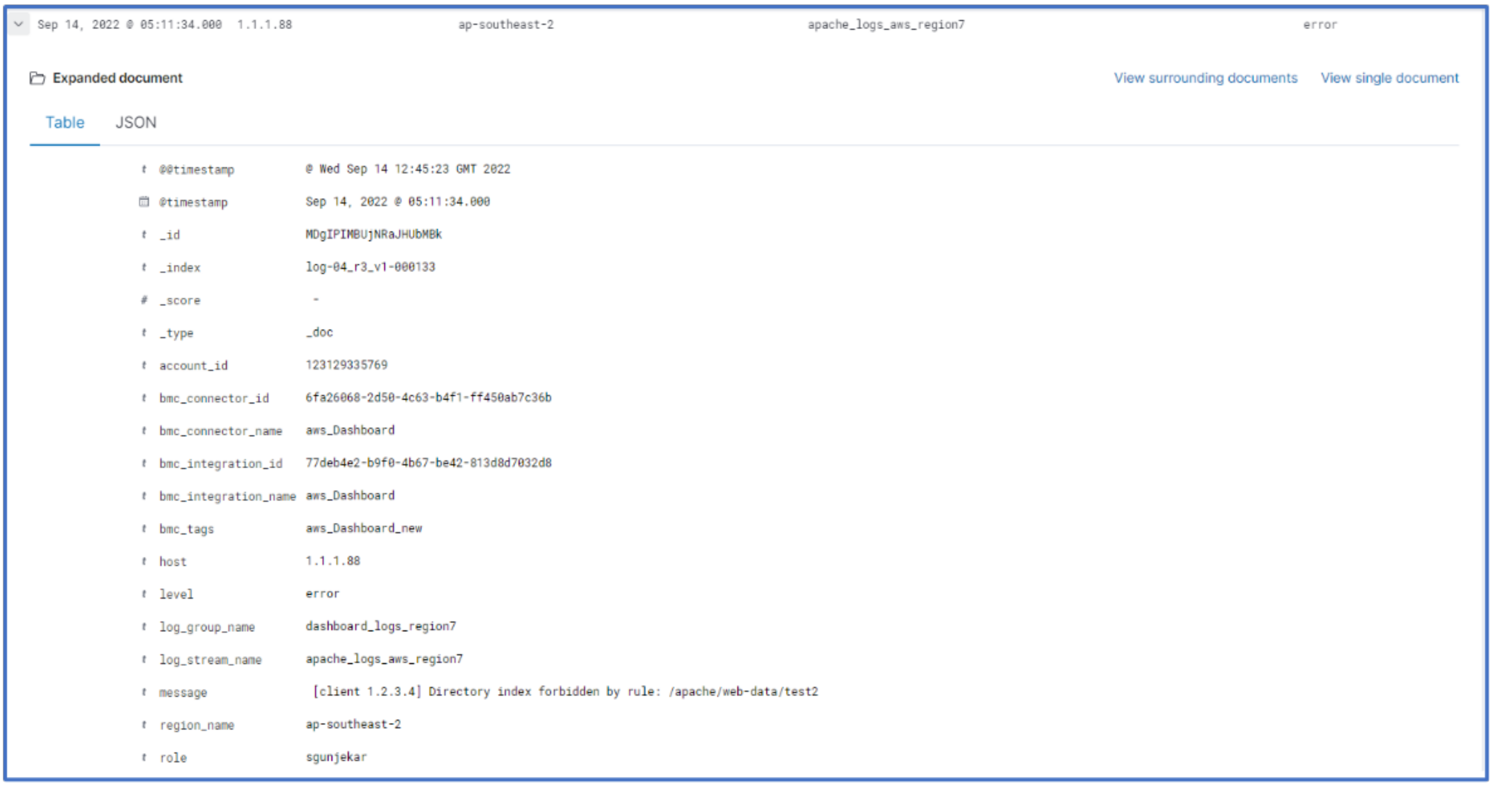
Once the logs are collected and stored, you can further analyze them in the log explorer to search, discover, or query any log record. Insights from logging can provide a great deal of context around the behavior of your applications and services and help you troubleshoot when you are dealing with an outage.



Time	host	region_name	log_stream_name	level
Sep 14, 2022 @ 05:11:34.000	1.1.1.141	ap-southeast-2	apache_logs_aws_region7	warning
Sep 14, 2022 @ 05:11:34.000	1.1.1.88	ap-southeast-2	apache_logs_aws_region7	error
Sep 14, 2022 @ 05:11:34.000	1.1.1.142	ap-southeast-2	apache_logs_aws_region7	warning
Sep 14, 2022 @ 05:11:34.000	1.1.1.6	ap-southeast-2	apache_logs_aws_region7	info
Sep 14, 2022 @ 05:11:34.000	1.1.1.91	ap-southeast-2	apache_logs_aws_region7	warning
Sep 14, 2022 @ 05:11:34.000	1.1.1.94	ap-southeast-2	apache_logs_aws_region7	warning

Figure 4. Discover and search logs in log explorer

You can slice and dice a given log record to see detailed attributes and values, which helps you understand and further troubleshoot your issue.



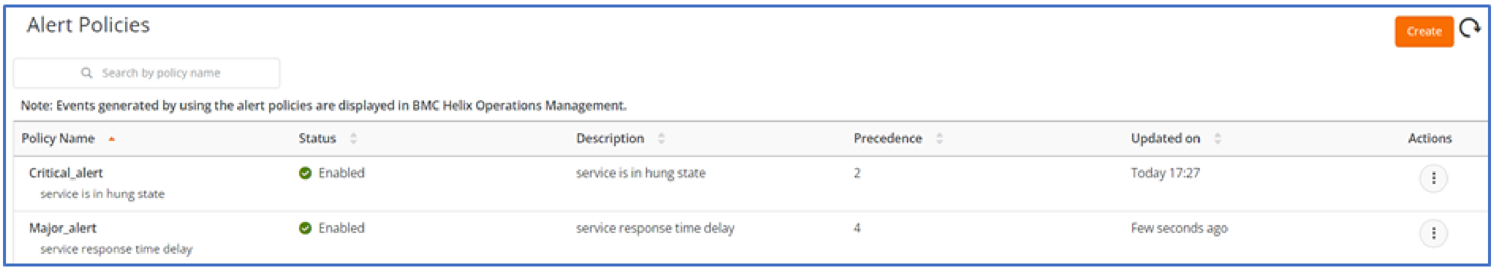
Sep 14, 2022 @ 05:11:34.000	1.1.1.88	ap-southeast-2	apache_logs_aws_region7	error

@@timestamp	@ Wed Sep 14 12:45:23 GMT 2022
@timestamp	Sep 14, 2022 @ 05:11:34.000
_id	MDgIPIMBUjNRaJHUbMBk
_index	log-04_r3_v1-000133
_score	-
_type	_doc
account_id	123129335769
bmc_connector_id	6fa26068-2d50-4c63-b4f1-ff450ab7c36b
bmc_connector_name	aws_Dashboard
bmc_integration_id	77deb4e2-b9f0-4b67-be42-813d8d7032d8
bmc_integration_name	aws_Dashboard
bmc_tags	aws_Dashboard_new
host	1.1.1.88
level	error
log_group_name	dashboard_logs_region7
log_stream_name	apache_logs_aws_region7
message	[client 1.2.3.4] Directory index forbidden by rule: /apache/web-data/test2
region_name	ap-southeast-2
role	sgunjekar

Figure 5. Anatomy of AWS log record

Creating alerts

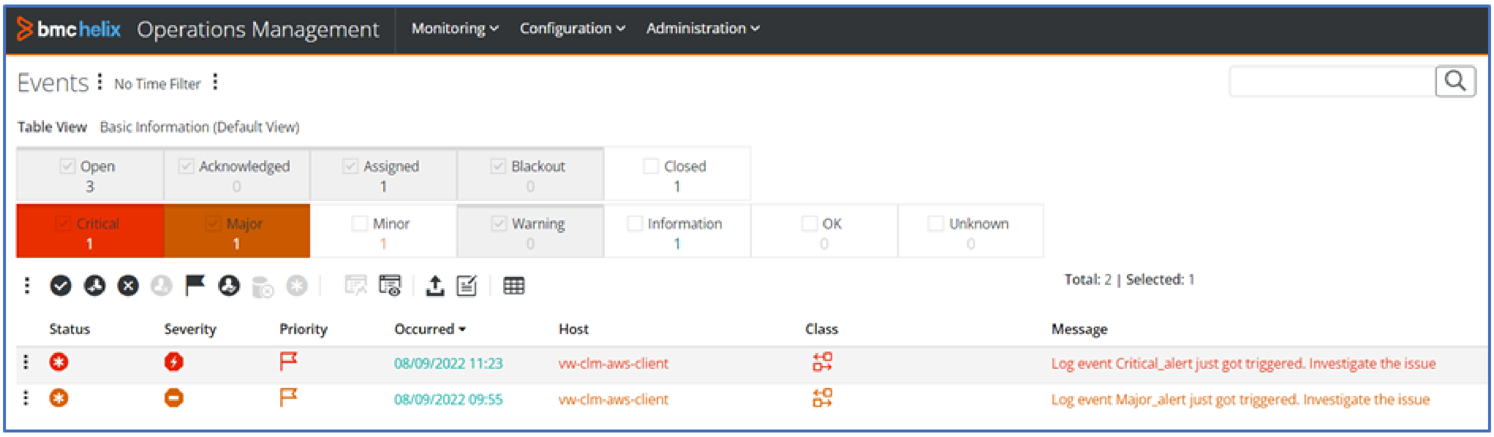
When things go wrong, alerts are essential for reducing response and recovery times. BMC Helix Log Analytics offers the ability to set alarms or alerts on any given condition occurring in the logs. Log events generated from these alerts can be operated in BMC Helix Operations Management, which takes proactive actions and sends notifications to you.



Note: Events generated by using the alert policies are displayed in BMC Helix Operations Management.

Policy Name	Status	Description	Precedence	Updated on	Actions
Critical_alert service is in hung state	Enabled	service is in hung state	2	Today 17:27	⋮
Major_alert service response time delay	Enabled	service response time delay	4	Few seconds ago	⋮

Figure 6. Log alert policies



☑ Open	☑ Acknowledged	☑ Assigned	☑ Blackout	□ Closed		
3	0	1	0	1		
☑ Critical	☑ Major	□ Minor	☑ Warning	□ Information	□ OK	□ Unknown
1	1	1	0	1	0	0

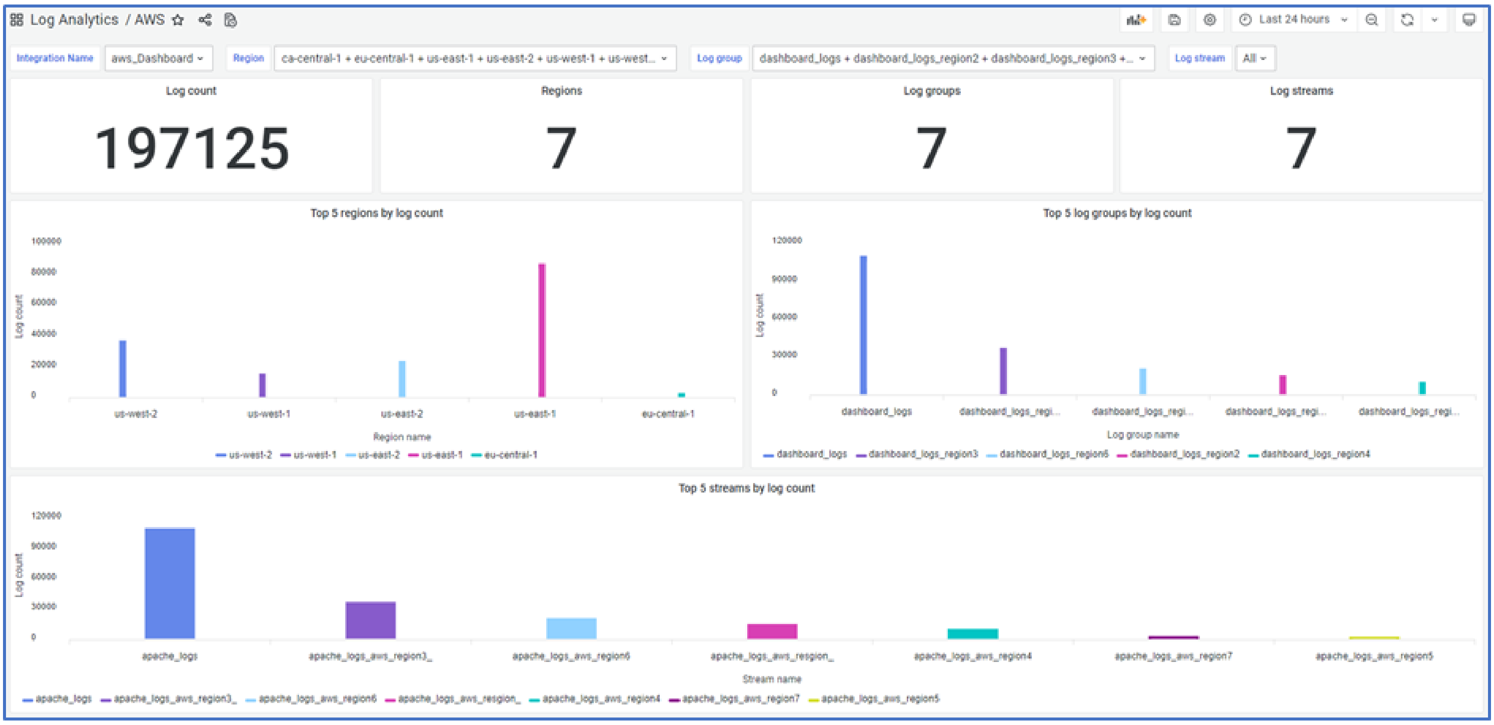
Total: 2 | Selected: 1

Status	Severity	Priority	Occurred	Host	Class	Message
			08/09/2022 11:23	vw-clm-aws-client		Log event Critical_alert just got triggered. Investigate the issue
			08/09/2022 09:55	vw-clm-aws-client		Log event Major_alert just got triggered. Investigate the issue

Figure 7. Analyzing log events in the BMC Helix Operations Management console

Visualizing logs

Dashboards help you track the most important metrics so you are always aware of the state of the system. You can create dashboards to monitor metrics derived from your logs, and visualize the data in the form of a line chart, a stacked chart, or a numerical metric. Taking things further, you can add alarms to widgets for quick and simple monitoring. BMC Helix Log Analytics uses BMC Helix Dashboards to provide out-of-the-box log dashboards that allow you to create self-service dashboards as needed. Here is a self-service dashboard to monitor and visualize logs from an AWS deployment.



Log Analytics / AWS

Last 24 hours

Integration Name: aws_Dashboard

Region: ca-central-1 + eu-central-1 + us-east-1 + us-east-2 + us-west-1 + us-west...

Log group: dashboard_logs + dashboard_logs_region2 + dashboard_logs_region3 +...

Log stream: All

Log count: 197125

Regions: 7

Log groups: 7

Log streams: 7

Figure 8. Self-service AWS log monitoring dashboard

BMC Helix Log Analytics is a great way to manage AWS observability with log monitoring. It acts as an advanced log monitoring solution to collect logs from AWS CloudWatch, perform monitoring and alerting, and deliver meaningful insights to improve and optimize your application. When used with monitoring metrics data from AWS and BMC Helix Operations Management with AIOps, it provides fully contextualized data about the state of your AWS services and the applications running in it.

The BMC Helix platform is an integral part of the BMC observability solution, giving SREs, DevOps engineers, and developers a seamless and streamlined workflow for IT monitoring, troubleshooting, and investigation to easily move from problem detection to resolution in minutes.

To find out more about log collection from AWS, check out our BMC Helix Log Analytics product documentation and video.

To learn more about BMC Helix Log Analytics capabilities, watch our overview video or refer to our product documentation.

Related content

- Observability with Logs to Accelerate MTTR
- Make Your Data Smarter with Log Enrichment