jSONAR
Simplifying Security

tech note

jSonar Integration with Amazon DocumentDB

Yael Kadoshi, jSonar

tech note

1.0 OVERVIEW

With Amazon DocumentDB, you can audit events that were performed in your cluster. When auditing is enabled, Amazon DocumentDB records Data Definition Language (DDL), authentication, authorization, and user management events to Amazon CloudWatch Logs. Amazon DocumentDB exports your cluster's auditing records as JSON documents to Amazon CloudWatch Logs.

Amazon DocumentDB auditing feature is an opt-in feature and records operations that take place within your cluster on objects, such as databases, collections, indexes, and users.
For more information see: https://docs.aws.amazon.com/documentdb/latest/developerguide/event-auditing.html

2.0 ENABLE AUDIT LOGGING ON AMAZON DOCUMENTDB

Auditing is configured on a Cluster level. When you use the jSonar Cloud Sources application to configure DocumentDB cluster for Auditing jSonar will automatically configure the necessary Parameter Groups to enable Audit Logs and will enable Export auditing logs to Amazon CloudWatch.

3.0 jSONAR CONFIGURATION

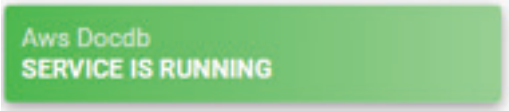
3.1 Configure SonarGateway Service

Enable the docdb gateway service : systemctl enable gateway-aws@docdb.service
Run the docdb gateway service: systemctl restart gateway-aws@docdb.service

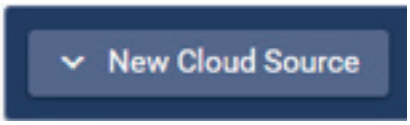
3.2 Add Cloud Source

Login to jSonar GUI as an administrator. In the homepage under "Administration" section, click on "Cloud Sources". Check if the service is running by looking at "Aws Docdb" bar on the top, if it's green then the service is running. You can also check the status of the docdb gateway service in the shell using command:

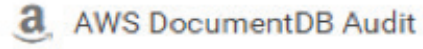
systemctl status gateway-aws@docdb.service -l



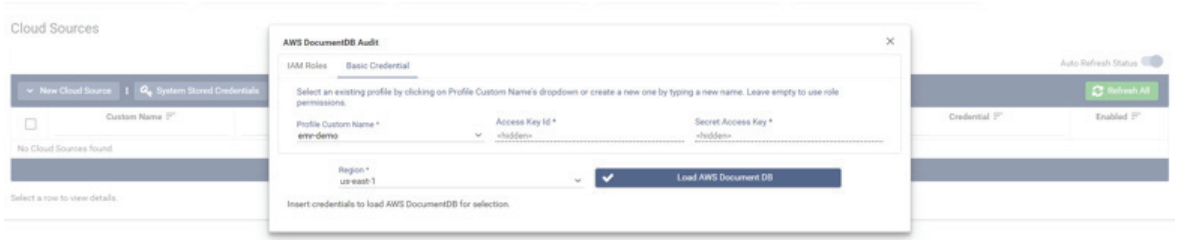
Click on "New Cloud Source" on the top left.



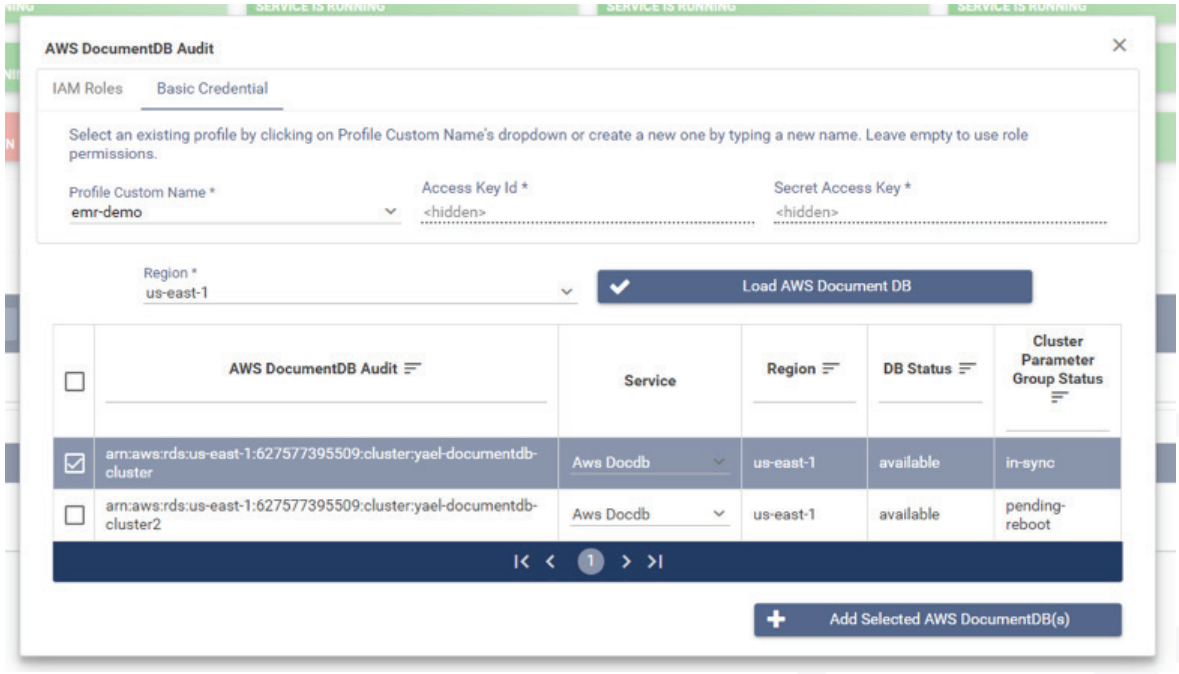
Select from the dropdown "AWS DocumentDB Audit".



Select the Tab for setting up credentials (e.g. "IAM Roles" or, when using keys, "Basic Credential"). Select the relevant "Region" or choose "All Regions" to see the list of all available log groups.



Click "Load AWS DocumentDB"



Check the lines of the cloud ARNs for the DocumentDB clusters which you would like to enable for Auditing for.

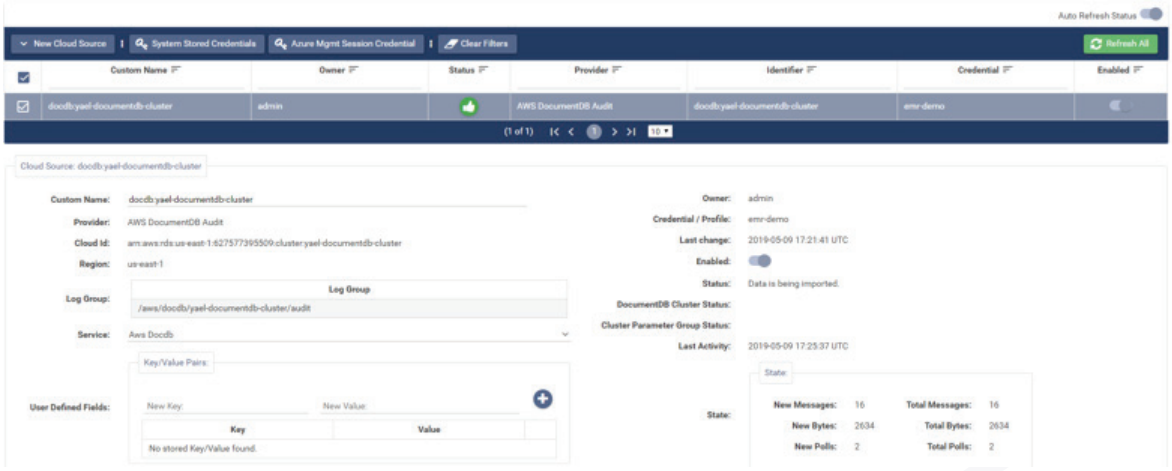
Click "Add Selected AWS DocumentDB(s)"

The selected clusters will be automatically configured to enable Audit Logs and to Export Auditing logs to Amazon CloudWatch if the Audit Logs feature is not configured already on AWS side.

A message will be displayed to confirm the reboot of the instances of the selected DocumentDB clusters.

Click "Yes" to confirm reboot.

A new cloud source will be added to the list. On the right side click on the enable button and watch the status icon, it might take a few seconds to start importing logs and by then the status icon will change to green, you can always click on the refresh to check the status icon.



4.0 FILE LOCATIONS

Log file: /var/log/sonar/gateway/cloud/aws/docdb/sonargateway.log

Logging conf file: /etc/sonar/gateway/cloud/gateway-aws-logging.conf

Mapping file: /etc/sonar/gateway/cloud/aws/docdb.json