 **Matica Project**

**Architecture Low Level Design**

**Version:** <0.1 27/09/2022>

**Customer**: Matica

**Objective:** the goal of this document is to describe the Cloudformation templates realized for the customer by Criticalcase on AWS Cloud.

**Limits**: the application environment is out of the scope of this document.

Summary

[1 Project scope 3](#_Toc114843536)

[2 Cloud and Infrastructure Services 4](#_Toc114843537)

[2.1 Infrastructural Scope 4](#_Toc114843538)

[2.2 Architecture 5](#_Toc114843539)

[2.3 Cloudformation templates 5](#_Toc114843540)

[ lambda 5](#_Toc114843541)

[ elasticsearch 6](#_Toc114843542)

[ dms\_roles 6](#_Toc114843543)

[ dms 7](#_Toc114843544)

# Project scope

The main goal of Matica is to replicate the infrastructure across different infrastructure environments on AWS Cloud.

The Cloudformation template realized are four:

* lambda
* elasticsearch
* dms\_roles
* dms

# Cloud and Infrastructure Services

## Infrastructural Scope

Criticalcase boundary:

* Creation of Cloudformation templates of all the infrastructure services:
  + [Lambda](https://aws.amazon.com/it/codedeploy/) e EventBridge
  + Elasticsearch
  + DMS (Database Migration Service)

## Architecture

## Cloudformation templates

### lambda

The template will create a lambda inside the VPC with security group rules to allow communication with RDS. This lambda is started by default every 3 minutes by EventBridge and have default permissions for create CloudWatch Logs and create network interface

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| FunctionName | Name of the Lambda |  | Yes |
| Environment | Name of an environment. 'dev', 'staging', 'prod' and any name |  | Yes |
| LambdaHandlerPath | Path of a Lambda Handler | lambda\_function.lambda\_handler | Yes |
| Runtime | The identifier of the function's runtime | python3.9 | Yes |
| Timeout | The amount of time (in seconds) that Lambda allows a function to run before stopping it | 5 | Yes |
| MemorySize | The amount of memory available to the function at runtime | 128 | Yes |
| Architectures | The instruction set architecture that the function supports | x86\_64 | Yes |
| SecurityGroupId | RDS Security group ID |  | Yes |
| VpcId | The ID of the VPC |  | Yes |
| SubnetIds | A list of VPC subnet IDs |  | Yes |
| ScheduleExpression | The scheduling expression | rate(3 minutes) | Yes |
| S3Bucket | Name of S3 bucket where is stored the lambda code |  | Yes |
| S3Key | Path inside the S3 bucket where the code is stored |  | Yes |

**Note:**

* Only one RDS security group can be specified as a parameter
* All related services and resources are created by merging the **FunctionName** with **Environment** parameters
* All resources are associated with AWS tags

### elasticsearch

The template creates an Elasticsearch domain divided on one or more nodes with its own security group. Options such as data encryption, master user will also be defined automatically

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| DomainName | A name for the Amazon ES domain |  | Yes |
| Environment | Name of an environment. 'dev', 'staging', 'prod' and any name |  | Yes |
| ElasticsearchVersion | Elasticsearch version | '7.10' | Yes |
| MasterUserName | Username for the master user |  | Yes |
| MasterUserPassword | Password for the master user. |  | Yes |
| EBSVolumeSize | The size of the EBS volume for each data node. The minimum and maximum size of an EBS volume depends on the EBS volume type and the instance type to which it is attached. | 10 | Yes |
| ClusterInstanceCount | The instruction set architecture that the function supports | 1 | Yes |
| ClusterInstanceType | The instance type for your data nodes. | t3.small.elasticsearch | Yes |
| VpcId | The ID of the VPC |  | Yes |
| SubnetIds | A list of VPC subnet IDs |  | Yes |
| AvailabilityZoneCount | If you enabled multiple Availability Zones (AZs), the number of AZs that you want the domain to use | 2 | Yes |

**Note:**

* The **AvailabilityZoneCount** parameter is used only if **ClusterInstanceCount** is greater than 2. In that case, 3 must be specified as the value, otherwise it is automatically ignored
* Based on the **ClusterInstanceCount** value, enter enough subnets to split the nodes correctly
* All related services and resources are created by merging the **DomainName** with **Environment** parameters
* All resources are associated with AWS tags

### dms\_roles

This template has no input parameters. It takes care of creating two IAM roles that are indispensable for the DMS service: **dms-cloudwatch-logs-role** and **dms-vpc-role**

This template is to be run once per account. They are already present in this account and therefore it will not be necessary to use it; however, it is provided for completeness

### dms

The template will configure a DMS replication instance with its own security group. It also automatically adds the rules in the security groups of the RDS and Elasticsearch to allow communication. It then creates the endpoints to establish the connection and configure the task for data migration. The parameters inputs are divided into various sections. The one dedicated to the replication instance:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| Name | A display name for the resource identifier at the end of the EndpointArn response parameter that is returned in the created Endpoint object |  | Yes |
| Environment | Name of an environment. 'dev', 'staging', 'prod' and any name |  | Yes |
| ReplicationInstanceClass | The compute and memory capacity of the replication instance as specified by the replication instance class. | dms.t3.micro | Yes |
| ReplicationInstanceAllocatedStorage | The amount of storage (in gigabytes) to be initially allocated for the replication instance. | 50 | Yes |
| MultiAZ | Specifies whether the replication instance is a Multi-AZ deployment. You can't set the AvailabilityZone parameter if the Multi-AZ parameter is set to true | false | Yes |
| EngineVersion | The engine version number of the replication instance | 3.4.7 | Yes |
| PreferredMaintenanceWindow | The weekly time range during which system maintenance can occur, in UTC | Format ddd:hh24:mi-ddd:hh24:mi |  | No |
| VpcId | VPC where to setup DMS instance. DMS instance should have connectivity to RDS instance. |  | Yes |
| SubnetIds | Subnets for DMS subnet group. Must contain at least two subnets in two different Availability Zones in the same region. |  | Yes |

One for the MySQL endpoint:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| ServerName | The name of the server where the endpoint database resides |  | Yes |
| Username | The username to be used to log in to the endpoint database. |  | Yes |
| Password | The password to be used to log in to the endpoint database |  | Yes |
| ExtraConnectionAttributes | Additional attributes associated with the connection. Each attribute is specified as a name-value pair associated by an equal sign (=). Multiple attributes are separated by a semicolon (;) with no additional white space |  | No |
| SecurityGroupIdRDS | RDS Security group ID |  | Yes |

One for the Elasticsearch endpoint:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| EndpointUri | The endpoint for the ElasticSearch cluster. Amazon DMS uses HTTPS if a transport protocol (either HTTP or HTTPS) isn't specified. |  | Yes |
| ElasticSearchName | The name of the ElasticSearch cluster |  | Yes |
| SecurityGroupIdElasticsearch | Elasticsearch Security group ID |  | Yes |

One for the Migration Task:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter Name | Description | Default Value | Mandatory |
| ReplicationTaskIdentifier | An identifier for the replication task. |  | Yes |
| CdcStartPosition | Indicates when you want a change data capture (CDC) operation to start. |  | No |
| CdcStopPosition | Indicates when you want a change data capture (CDC) operation to stop. |  | No |
| MigrationType | The migration type. Valid values full-load | cdc | full-load-and-cdc | full-load-and-cdc | Yes |
| ReplicationTaskSettings | Overall settings for the task, in JSON format. |  | No |
| TableMappings | The table mappings for the task, in JSON format. | {"rules": [ { "rule-type": "selection", "rule-id": "1", "rule-name": "1", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "include" } ] } | Yes |

**Note:**

* Only one RDS security group can be specified as a parameter
* Only one Elasticsearch security group can be specified as a parameter
* All related services and resources related to the replication instance are created by merging the **Name** with **Environment** parameters
* All related services and resources related to the migration task are created by merging the **Name** with **Environment** and **ReplicationTaskIdentifier** parameters
* All resources are associated with AWS tags