BESTARION

Security classification:

Document code:

Last updated by:

Effective date:

Version:

Template ID:

DOCUMENT CONTROL

TABLE OF CONTENT

INDEX OF TABLES

INDEX OF FIGURES

1. Requirement

- data “terraform_remote_state” “networking”: Synchronize state information with other components of the system.

- allow_cidr_range:
  - “172.20.0.0/16”: CIDR block of the current VPC hosting these resources.
  - “10.0.0.0/16”: CIDR block of the MSS project VPC within the same AWS cloud environment.

- common_tags: Define tags for easier management and governance.

- ami_id: Since there is no specific Linux version requirement, the latest Ubuntu AMI will be used.

- data “aws_subnet” “private_app_a”: Retrieve a private subnet using the VPC ID obtained from S3 (remote state). Filters applied:
  - name = “tag:Name”: Search based on the Subnet’s “Name” tag in AWS.

  - values = [”*prod-private-app-a”]: Find subnets with names ending in “prod-private-app-a”.

- resource “aws_security_group” “other_services”:
  - Declare the name, description, and the associated VPC.

  - Egress: Allow unrestricted outbound access to the internet (allow all).

  - Apply both project-wide common tags and service-specific tags.

- resource “aws_security_group_rule” “allow_ssh”: Allow SSH access from the CIDR ranges defined above.

- resource “aws_security_group_rule” “allow_redis”: Open the port for Redis access from the defined CIDR ranges.

- resource “aws_security_group_rule” “allow_kafka”: Open the port for Kafka access from the defined CIDR ranges.

- resource “aws_security_group_rule” “allow_kafka_ui”: Open the port for Kafka UI access from the defined CIDR ranges.

- module “ec2”:
  - source: Utilize the pre-defined module.

  - instance_name: Assign a name to this EC2 instance.
  - instance_type: Select an instance type with resources appropriate for its workload.

  - ami_id: Use the AMI defined above.

- subnet_id: Place this EC2 into the correct private subnet defined above.
- security_group_ids: Attach the Security Group defined above to this EC2.
- iam_instance_profile: Attach a role enabling communication with AWS Systems Manager (SSM). This allows remote access via the AWS Console, automated patching, and remote command execution.
- ensure_key_pair: Specify the requirement of a key pair for EC2 login.
- key_name: The specific key pair to be used.
- tags: Assign tags to this instance.

2. How to

-

3.

test Ian 2