Cloud DFIR class 1

Cloud goat

담당	NICO
제출일	2024년 08월 13일
트랙	디지털포렌식 트랙
성명	김 동 은

When I first run CloudGoat, the following error occurs:

```
Error: creating IAM Role (glue_ETL_role): operation error IAM: CreateRole, https response error StatusCode: 409, RequestID: 297a8936-4a12-427e-8996-c468695a00cb, EntityAlread
yExists: Role with name glue_ETL_role already exists.

  with aws_iam_role.glue_ETL_role,
  on iam.tf line 74, in resource "aws_iam_role" "glue_ETL_role":
  74: resource "aws_iam_role" "glue_ETL_role" {


Error: creating IAM Role (ssm_parameter_role): operation error IAM: CreateRole, https response error StatusCode: 409, RequestID: 04128aff-8ebd-403f-a36c-381ab2024afc, EntityA
lreadyExists: Role with name ssm_parameter_role already exists.

  with aws_iam_role.ssm_parameter_role,
  on iam.tf line 121, in resource "aws_iam_role" "ssm_parameter_role":
  121: resource "aws_iam_role" "ssm_parameter_role" {


Error: creating IAM Role (s3_to_gluecatalog_lambda_role): operation error IAM: CreateRole, https response error StatusCode: 409, RequestID: f3d216fd-eb5c-46cc-ad5e-182bafb883
46, EntityAlreadyExists: Role with name s3_to_gluecatalog_lambda_role already exists.

  with aws_iam_role.s3_to_gluecatalog_lambda_role,
  on iam.tf line 148, in resource "aws_iam_role" "s3_to_gluecatalog_lambda_role":
  148: resource "aws_iam_role" "s3_to_gluecatalog_lambda_role" {


Error: creating IAM Role (cg-Glue_Privesc-ec2-profile): operation error IAM: CreateRole, https response error StatusCode: 409, RequestID: a95a2a44-1ebf-4ffc-a8ad-c6656eefdefc
, EntityAlreadyExists: Role with name cg-Glue_Privesc-ec2-profile already exists.

  with aws_iam_role.ec2_profile_role,
  on iam.tf line 192, in resource "aws_iam_role" "ec2_profile_role":
  192: resource "aws_iam_role" "ec2_profile_role" {


Error: creating IAM Policy (s3_put_policy): operation error IAM: CreatePolicy, https response error StatusCode: 409, RequestID: b9b9c829-e479-48dc-834c-1f19702a4b74, EntityAl
readyExists: A policy called s3_put_policy already exists. Duplicate names are not allowed.

  with aws_iam_policy.s3_put_policy,
```

```
Error: creating IAM Role (cg-Glue_Privesc-ec2-profile): operation error IAM: CreateRole, https response error StatusCode: 409, RequestID: a95a2a44-1ebf-4ffc-a8ad-c6656eefdefc
, EntityAlreadyExists: Role with name cg-Glue_Privesc-ec2-profile already exists.

  with aws_iam_role.ec2_profile_role,
  on iam.tf line 192, in resource "aws_iam_role" "ec2_profile_role":
  192: resource "aws_iam_role" "ec2_profile_role" {


Error: creating IAM Policy (s3_put_policy): operation error IAM: CreatePolicy, https response error StatusCode: 409, RequestID: b9b9c829-e479-48dc-834c-1f19702a4b74, EntityAl
readyExists: A policy called s3_put_policy already exists. Duplicate names are not allowed.

  with aws_iam_policy.s3_put_policy,
  on iam.tf line 202, in resource "aws_iam_policy" "s3_put_policy":
  202: resource "aws_iam_policy" "s3_put_policy" {


Error: creating RDS DB Instance (terraform-20240812170947584700000005): InvalidParameterCombination: Cannot find version 13.7 for postgres
        status code: 400, request id: a335a60b-dde6-48d5-aca3-dc6ffacd882b

  with aws_db_instance.cg-rds,
  on rds.tf line 1, in resource "aws_db_instance" "cg-rds":
  1: resource "aws_db_instance" "cg-rds" {


Error: creating SSM Parameter (flag): operation error SSM: PutParameter, https response error StatusCode: 400, RequestID: 778c4115-b6f6-40f3-8247-5e5e92034a8b, ParameterAlrea
dyExists: The parameter already exists. To overwrite this value, set the overwrite option in the request to true.

  with aws_ssm_parameter.cg-secret-string,
  on ssm-parameter.tf line 1, in resource "aws_ssm_parameter" "cg-secret-string":
  1: resource "aws_ssm_parameter" "cg-secret-string" {
```

The above error is related to duplication in IAM roles and policies, as well as issues with the version of SSM resources and RDS.

1. IAM

First, remove the policies and roles in IAM that are causing the above errors.

	역할 이름	▲	신뢰할 수 있는 개체	마지막 활동	▽
☐	AWSServiceRoleForRDS		AWS 서비스: rds (서비스 연결 역할)	23분 전	
☐	AWSServiceRoleForSupport		AWS 서비스: support (서비스 연결 역	-	
☐	AWSServiceRoleForTrustedAdvisor		AWS 서비스: trustedadvisor (서비스 '	-	

○	⊞	🗊 AlexaForBusinessGate...	AWS 관리형	권한 정책 (1)	Provide gateway execution access to A...
○	⊞	🗊 AlexaForBusinessLifes...	AWS 관리형	권한 정책 (1)	Provide access to Lifesize AVS devices
○	⊞	🗊 AlexaForBusinessNet...	AWS 관리형	없음	This policy enables Alexa for Business ...
○	⊞	🗊 AlexaForBusinessPoly...	AWS 관리형	권한 정책 (1)	Provide access to Poly AVS devices
○	⊞	🗊 AlexaForBusinessRead...	AWS 관리형	권한 정책 (1)	Provide read only access to AlexaForB...
○	⊞	🗊 AmazonAPIGatewayA...	AWS 관리형	권한 정책 (1)	Provides full access to create/edit/dele...
○	⊞	🗊 AmazonAPIGatewayIn...	AWS 관리형	권한 정책 (1)	Provides full access to invoke APIs in A...
○	⊞	🗊 AmazonAPIGatewayP...	AWS 관리형	없음	Allows API Gateway to push logs to us...
○	⊞	🗊 AmazonAppFlowFullA...	AWS 관리형	없음	Provides full access to Amazon AppFlo...
○	⊞	🗊 AmazonAppFlowRead...	AWS 관리형	없음	Provides read only access to Amazon A...

Once you remove the policies and roles as described above, the issue will be resolved.

2. RDS

```
aws rds describe-db-engine-versions --default-only --engine postgres
```

Using the command mentioned above, find the RDS versions supported in the current region and version, then modify the `rds.tf` code accordingly.

```
resource "aws_db_instance" "cg-rds" {
  allocated_storage      = 20
  storage_type           = "gp2"
  engine                 = "postgres"
  engine_version         = "16.3"
  instance_class         = "db.t3.micro"
  db_subnet_group_name   = aws_db_subnet_group.c
  db_name                = var.rds-database-name
  username               = var.rds_username
  password               = var.rds_password
  parameter_group_name   = "default.postgres16"
```

By following the steps mentioned above, the RDS issue will be resolved..

3. SSM

In the `ssm.tf` file, allow for duplication to resolve the issue.

```
resource "aws_ssm_parameter" "cg-secret-string" {
  name        = "flag"
  description = "this is secret-string"
  type        = "String"
  value       = "Best-of-the-Best-12th-CGV"
  tags = {
    Name     = "cg-secret-string-${var.cgid}"
    Stack    = var.stack-name
    Scenario = var.scenario-name
  }
  lifecycle {
    create_before_destroy = true
  }
}
```

After going through the above steps, you should be able to confirm that everything runs successfully.

```
Apply complete! Resources: 58 added, 0 changed, 0 destroyed.

Outputs:

cg_web_site_ip = "54.165.123.181"
cg_web_site_port = 5000

[cloudgoat] terraform apply completed with no error code.

[cloudgoat] terraform output completed with no error code.
cg_web_site_ip = 54.165.123.181
cg_web_site_port = 5000

[cloudgoat] Output file written to:

    /home/user/cloudgoat/glue_privesc_cgidn774pm2k2a/start.txt
```

The issue is that upon connecting, it is confirmed that the database is not linked as expected.

InFailedSqlTransaction

psycopg2.errors.InFailedSqlTransaction: current transaction is aborted, commands ignored until end of transaction block

Traceback (most recent call last)

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *2552*, in __call__
   return self.wsgi_app(environ, start_response)

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *2532*, in wsgi_app
   response = self.handle_exception(e)

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *2529*, in wsgi_app
   response = self.full_dispatch_request()

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *1825*, in full_dispatch_request
   rv = self.handle_user_exception(e)

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *1823*, in full_dispatch_request
   rv = self.dispatch_request()

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line *1799*, in dispatch_request
   return self.ensure_sync(self.view_functions[rule.endpoint])(**view_args)

File "/home/ec2-user/my_flask_app/my_flask_app/app.py", line *104*, in index
   cur.execute("select * from cc_data")

psycopg2.errors.InFailedSqlTransaction: current transaction is aborted, commands ignored until end of transaction block

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

Now, I plan to resolve the issue with the database not being linked.