

Answer: GetCallerIdentity

Answer: us-east-1,us-east-2

I asked the ChatGPT

Answer: DescribeInstances

I searched for "DescribeInstances"

```
Line 47450: "errorMessage": "You are not authorized to perform this operation. User: arn:aws:iam::94622803460:assumed-role/EC2DatabaseConnection/!-0bd9f116b0b0e943c is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action",
Line 47602: "eventName": "DescribeInstances",
Line 47607: "errorMessage": "You are not authorized to perform this operation. User: arn:aws:iam::94622803460:assumed-role/EC2DatabaseConnection/!-0bd9f116b0b0e943c is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action"
```

Then I took the `errorMessage` and searched for it:

```
Line #06919: *ccrc@csespresso: "User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: codebuild:ListFunctions on resource: ' because no identity-based policy allows the ListFunctions action",
```

```
Line #06920: *ccrc@csespresso: "User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: transfer:ListServers on resource: arnaws:transfer-central:1-909422734ab6:serverz' because no identity-based policy allows the transfer:ListServers
```

```
Line #07320: *ccrc@csespresso: "User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: codebuild:ListProjects because no identity-based policy allows the codebuild:ListProjects action",
```

```
Line #07370: *ccrc@csespresso: "User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: codebuild:ListBuilds because no identity-based policy allows the codebuild:ListBuilds action",
```

```
Line #7400: *ccrc@csespresso: "You are not authorized to perform this operation. User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action",
```

```
Line #7400: *ccrc@csespresso: "You are not authorized to perform this operation. User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action",
```

```
Line #7670: *ccrc@csespresso: "You are not authorized to perform this operation. User: arnawest@194962209460; assumed-role/ECDDatabaseConnection/1-0d8f91c8b5e949e is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action",
```

Then I took the string "is not authorized to perform" and searched for it too

```
Search result - [742 hits]
9 \|Share\daemon_logon (742 hits)
Line 468030 "MicrosoftExchange": "User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: IamdbuildInstanceFunctions because no identity-based policy allows the iamdbuildInstanceFunctions action."
Line 471291 "MicrosoftExchange": "User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: IAM::DescribeInstances because no identity-based policy allows the IAM::DescribeInstances action."
Line 471793 "MicrosoftExchange": "User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: codebuild:BuildProject because no identity-based policy allows the codebuild:BuildProject action."
Line 473792 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeSubnets because no identity-based policy allows the ec2:DescribeSubnets action."
Line 473875 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeAddresses because no identity-based policy allows the ec2:DescribeAddresses action."
Line 474072 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action."
Line 474379 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeRouteTables because no identity-based policy allows the ec2:DescribeRouteTables action."
Line 474793 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeNetworkAcls because no identity-based policy allows the ec2:DescribeNetworkAcls action."
Line 474908 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeVpcEndpoints because no identity-based policy allows the ec2:DescribeVpcEndpoints action."
Line 475002 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeSecurityGroups because no identity-based policy allows the ec2:DescribeSecurityGroups action."
Line 475044 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeRouteTables because no identity-based policy allows the ec2:DescribeRouteTables action."
Line 475047 "MicrosoftExchange": "You are not authorized to perform this operation. User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: ec2:DescribeVpnConnections because no identity-based policy allows the ec2:DescribeVpnConnections action."
Line 475229 "MicrosoftExchange": "User: asini@wznetts:19492203040\asunm=role/EC2DatabaseConnection/L-DBD9116B509436 is not authorized to perform: secretsmanager:ListSecrets because no identity-based policy allows the secretsmanager:ListSecrets action."
```

Answer: 742

After I found the answer for task 10, I checked the ARNs and found only 2 ARNs

```
"errorMessage": "User: admin:sa:19462203460:assumed-role/EC2DatabaseConnection/1-2bd9f116860e945e",
"errorMessage": "User: admin:sa:19462203460:assumed-role/EC2DatabaseConnection/1-2bd9f116860e945e",
"User: admin:sa:19462203460:user/devops-sah",
"User: admin:sa:19462203460:user/devops-sah"
```

Answer: `arn:aws:iam::949622803460:user/devops-ash,arn:aws:sts::949622803460:assumed-role/EC2DatabaseConnection/i-0bdf91168b50e943e`

Task 12:
transactiondb-prod-2024-03-13-06-53.wb-customerdb-prod-2024-03-13-07-59

I searched for snapshotid and found several snapshots. Then I told chat to make me all combinations to the answer

Answer: transactiondb-prod-2024-03-13-06-53-wb-customerdb-prod-2024-03-13-07-59

Task 13:
The Threat Actor successfully exfiltrated the data to their account. Could you specify the account ID that was used?

I searched for `wb-customerdb-prod-2024-03-13-07-59` the snapshot from task 12 and found something that was pretty suspicious in the log inside the field `"attributeValues"`

[illegible]

Answer: 143637014344

Task 14:
Which MITRE Technique ID corresponds to the activity described in Question 13?
I told ChatGPT about the account ID from task 13, showed him part of the log and asked him about the MITRE Technique

The activity described involves exfiltrating data by modifying the attributes of an Amazon RDS snapshot to include an external account ID, which is a form of data exfiltration using cloud services. According to the MITRE ATT&CK framework, this activity can be mapped to the technique:

MITRE Technique ID: T1537

Technique Name: Exfiltration Over Web Service

This technique covers the exfiltration of data using cloud-based services, such as AWS, where attackers can exploit cloud storage and data management services to transfer data out of an organization's environment. In this specific case, modifying RDS snapshot attributes to include an external account ID to exfiltrate data fits this technique.

Answer: T1537