5min

Incident Response in the Cloud

DigitalForensic Track
김태룡

INDEX

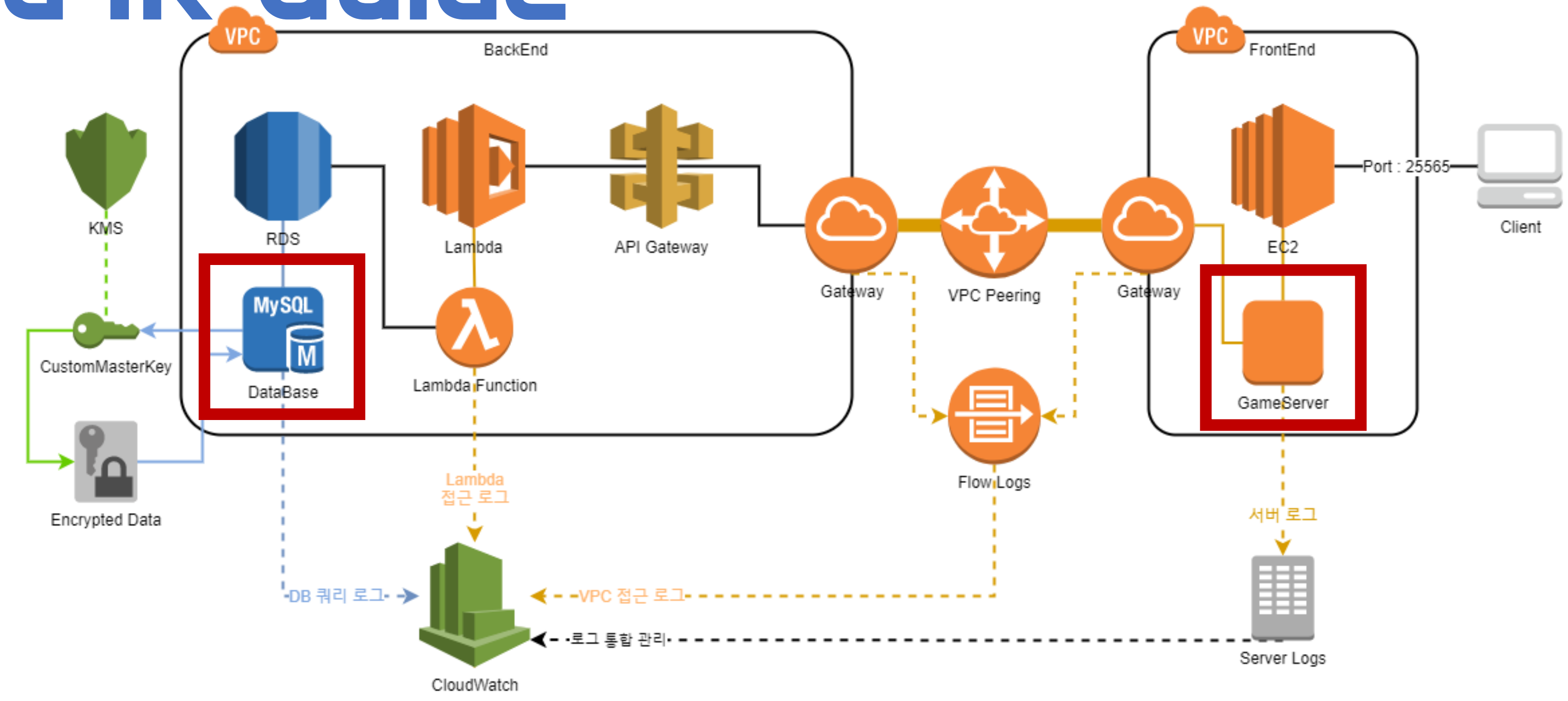
01. Cloud IR Guide

02. Additional Things

Cloud IR Guide

NIST SP 800-83,
Computer Security Incident Handling Guide
(악성 소프트웨어 사고 예방 및 처리 지침)

Cloud IR Guide



Establish response objectives

Work with your stakeholders, legal counsel, and organizational leadership to determine the goal of responding to an incident.
(이해 관계자, 법률 고문 및 조직과 함께 사고 대응 목표를 결정하기)

Cloud IR Guide

Cloud Watch
Indicators

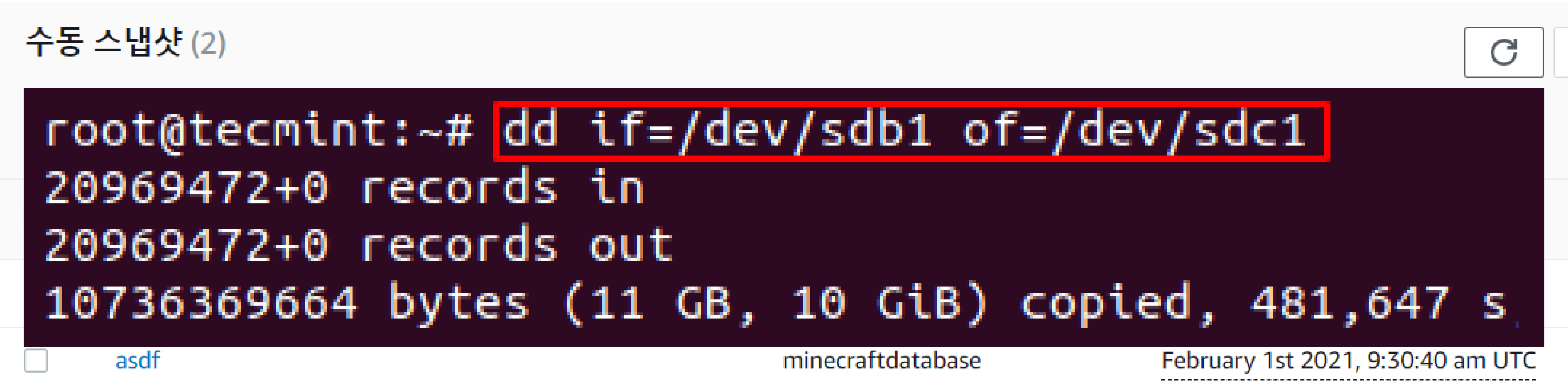
RDS
General.log

EC2
Server Logs

Respond using the cloud

Implement your response patterns where the event and data occurs.
(이벤트 및 데이터가 발생하는 곳을 미리 확인하고, 대응 패턴 파악하기)

Cloud IR Guide



수동 스냅샷 (2)

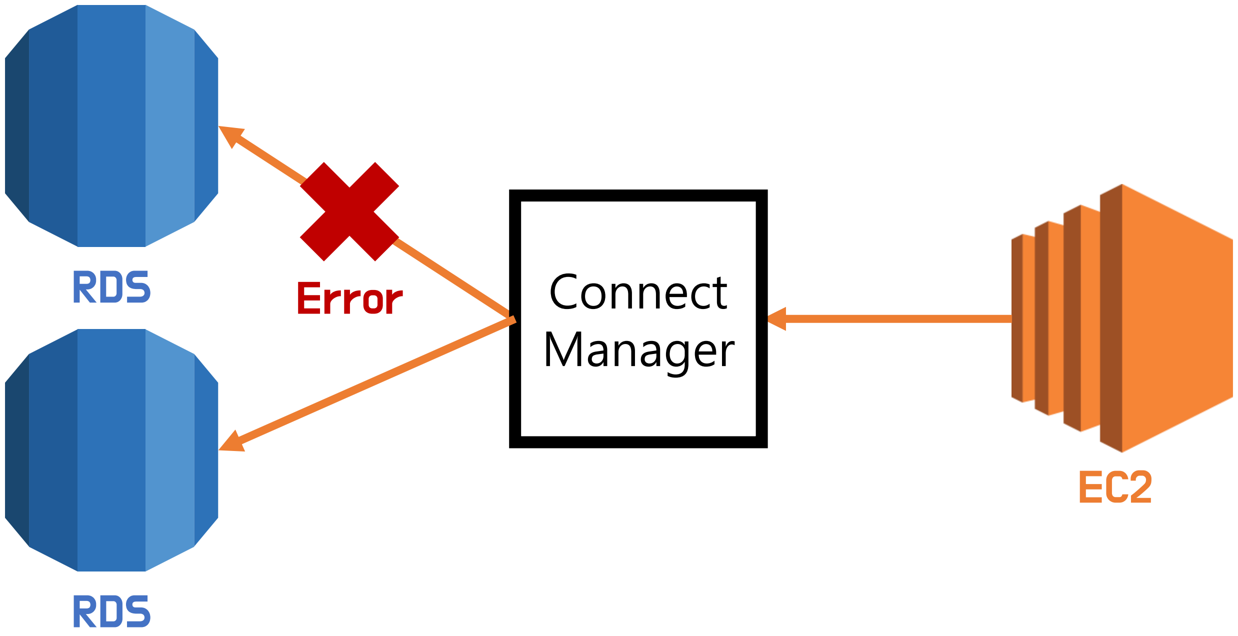
```
root@tecmint:~# dd if=/dev/sdb1 of=/dev/sdc1
20969472+0 records in
20969472+0 records out
10736369664 bytes (11 GB, 10 GiB) copied, 481,647 s
```

□ asdf minecraftdatabase February 1st 2021, 9:30:40 am UTC

Know what you have and what you need

Preserve logs, snapshots, and other evidence by copying them.
(로그, 스냅 샷 및 기타 필요한 증거를 복사하여 보존)

Cloud IR Guide



Use redeployment mechanisms

Make response mechanisms safe to execute
more than once and on unknown states.
(응답 메커니즘이 안전하게 수행 될 수 있도록 하기)

Cloud IR Guide

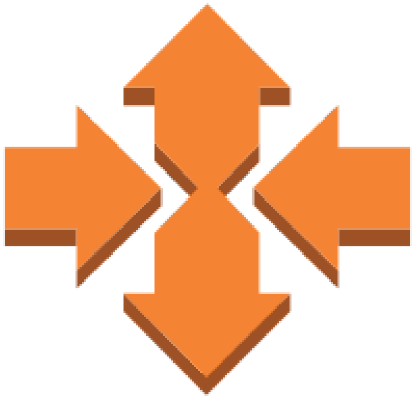
Cloud Trail

Cloud Watch

Automate where possible

As you see issues or incidents repeat,
build mechanisms that programmatically.
(사고가 반복되면 프로그래밍 방식으로 상황을 분류하고 대응하기)

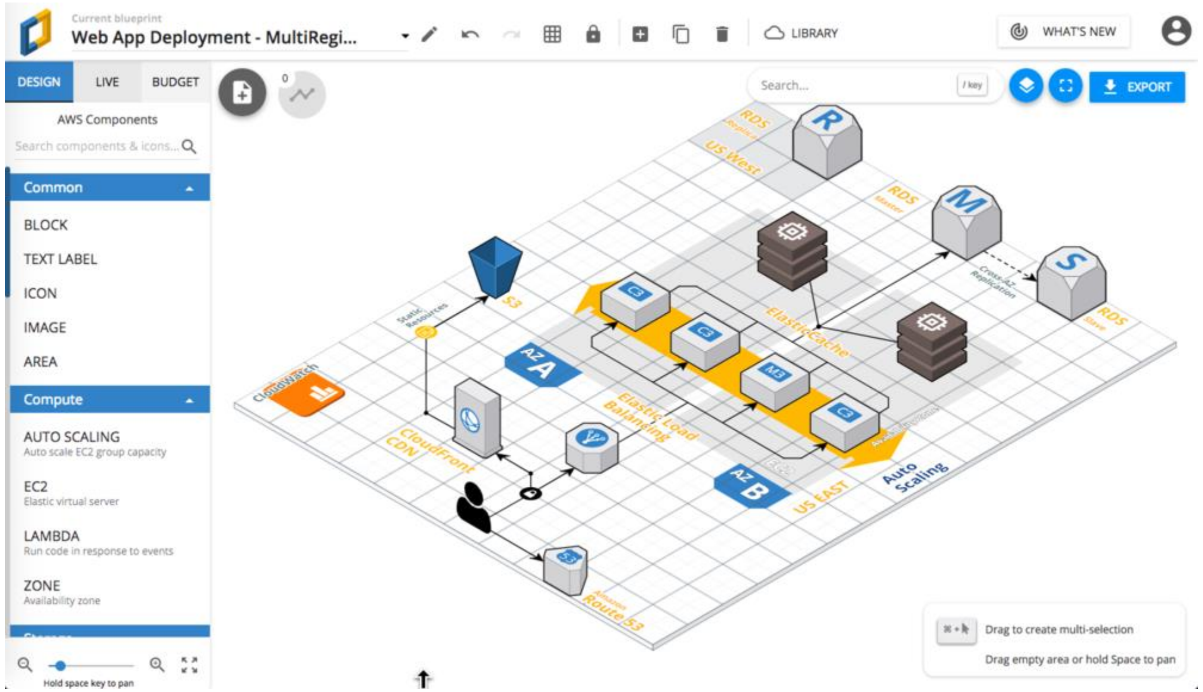
Cloud IR Guide



Choose scalable solutions

Strive to match the scalability of
organization's approach to cloud computing.
(조직의 확장 성에 맞는 솔루션 선택하기)

Cloud IR Guide



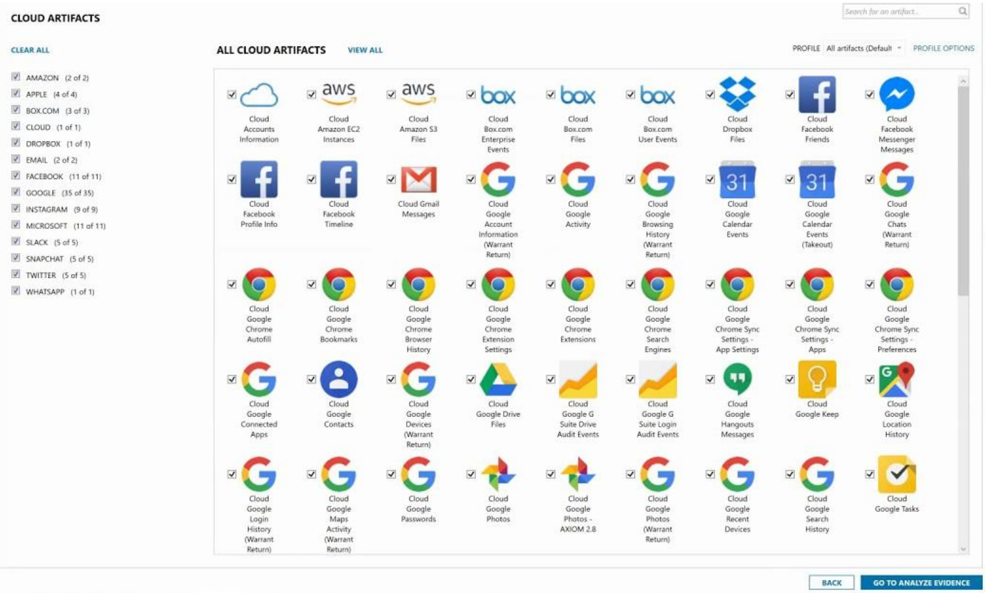
Drag to create multi-selection

Drag empty area or hold Space to pan

Learn and improve process

Simulations are safe methods to find gaps and improve processes.
(시뮬레이션 및 학습을 통해 클라우드 프로세스를 개선한다)

Additional Things


CLOUD ARTIFACTS

- ☑ AMAZON (2 of 2)
- ☑ APPLE (4 of 4)
- ☑ BOX.COM (3 of 3)
- ☑ CLOUD (1 of 1)
- ☑ DROPBOX (1 of 1)
- ☑ EMAIL (2 of 2)
- ☑ FACEBOOK (11 of 11)
- ☑ GOOGLE (35 of 35)
- ☑ INSTAGRAM (9 of 9)
- ☑ MICROSOFT (11 of 11)
- ☑ SLACK (5 of 5)
- ☑ SNAPCHAT (5 of 5)
- ☑ TWITTER (5 of 5)
- ☑ WHATSAPP (1 of 1)

ALL CLOUD ARTIFACTS

PROFILE All artifacts (Default

- ☑ Cloud Accounts Information
- ☑ Cloud Amazon EC2 Instances
- ☑ Cloud Amazon S3 Files
- ☑ Cloud Box.com Enterprise Events
- ☑ Cloud Box.com Files
- ☑ Cloud Box.com User Events
- ☑ Cloud Dropbox Files
- ☑ Cloud Facebook Friends
- ☑ Cloud Facebook Messenger Messages
- ☑ Cloud Facebook Profile Info
- ☑ Cloud Facebook Timeline
- ☑ Cloud Gmail Messages
- ☑ Cloud Google Account Information (Warrant Return)
- ☑ Cloud Google Activity
- ☑ Cloud Google Browsing History (Warrant Return)
- ☑ Cloud Google Calendar Events
- ☑ Cloud Google Calendar Events (Takeout)
- ☑ Cloud Google Chats (Warrant Return)
- ☑ Cloud Google Chrome Autofill
- ☑ Cloud Google Chrome Bookmarks
- ☑ Cloud Google Chrome Browser History
- ☑ Cloud Google Chrome Extension Settings
- ☑ Cloud Google Chrome Extensions
- ☑ Cloud Google Chrome Search Engines
- ☑ Cloud Google Chrome Sync Settings - App Settings
- ☑ Cloud Google Chrome Sync Settings - Apps
- ☑ Cloud Google Chrome Sync Settings - Preferences
- ☑ Cloud Google Connected Apps
- ☑ Cloud Google Contacts
- ☑ Cloud Google Devices (Warrant Return)
- ☑ Cloud Google Drive Files
- ☑ Cloud Google G Suite Drive Audit Events
- ☑ Cloud Google G Suite Login Audit Events
- ☑ Cloud Google Hangouts Messages
- ☑ Cloud Google Keep
- ☑ Cloud Google Location History
- ☑ Cloud Google Login History (Warrant Return)
- ☑ Cloud Google Maps Activity (Warrant Return)
- ☑ Cloud Google Passwords
- ☑ Cloud Google Photos
- ☑ Cloud Google Photos - AXIOM 2.8
- ☑ Cloud Google Photos (Warrant Return)
- ☑ Cloud Google Recent Devices
- ☑ Cloud Google Search History
- ☑ Cloud Google Tasks

Think about responding to an incident or a forensics event

In some cases, this means you may have multiple organizations, accounts, and tools specifically set up for these response tasks.
(포렌식 관점으로도 생각 해 보고, 다양한 도구를 찾아 사용 해 보기)

Thankyou