클라우드 서비스 대상 'Golden Configuration' 적용을 위한 Ansible 기반 인프라 코드 생성 시스템

김남준 ○ 한서윤 정찬혁 이나연 윤홍관 박기웅‡

세종대학교 정보보호학과

bunseokbot@sju.ac.kr, qorengkssk@naver.com, jch6637@naver.com,

lny7036@naver.com, dbsghdrhks78@gmail.com, woongbak@sejong.ac.kr‡

Ansible-based infrastructure code generation system for applying 'Golden Configuration' to cloud services

Namjun Kim ○ Seoyoon Han Chanhyeok Jung Nayeon Lee Hongkwan Yoon Ki-Woong Park

Department of Computer and Information Security, Sejong University

요 약

전 세계가 COVID-19로 인해 디지털 트랜스포메이션(Digital Transformation)이 가속화됨에 따라 디지털 환경 기반의 클라우드 인프라로의 전환이 진행되고 있다. 동시에 이러한 클라우드 인프라를 대상으로 하는 공격이 증가하고 있으며 상당수의 보안 사고의 경우 서버의 취약점이 아닌 방화벽 보안 설정 오류와 같은 문제로 인해 발생하고 있다. 이에 따라 본 연구진은 사용자가 안전하게 클라우드 서비스의 Golden Configuration을 쉽게 적용할 수 있도록 클라우드 별로 보안 대상 요소에 대해 선정하고, 이를 쉽게 적용할 수 있도록 Ansible 기반의 인프라 코드를 생성할 수 있는 시스템을 제안하고자 한다

1. 서 론

전 세계가 COVID-19로 인한 새로운 감염병으로 인해 위기 속 대혼란에 빠졌다. 이러한 감염병의 위협 속에 수많은 기업이 재택근무와 시차 근무제를 도입하게 되었다. 이는 전방위적인 디지털 트랜스포메이션(Digital Transformation)이 가속화되는 데 촉매제 역할을 하게 되었다.

마이크로소프트社 의 CEO인 Satya Nadella 는 COVID-19로 인한 영향으로 2년 정도 소요될 것으로 예상되었던 디지털 트랜스포메이션이 단 두 달 만에 전환이 완료되었다고 하였다[1]. 이는 곧 기업과 공공기관이 기존의 레거시 인프라에서 디지털 환경 기반의 인프라로의 전환을 의미한다. 대표적인 클라우드 서비스 제공자(Cloud Service Provider)인 마이크로소프트社 와 구글社은 전체 매출 중 클라우드 부분 매출이 COVID-19 사태 이전과 비교하여 50% 증가하였다고 밝혔다[2].

그러나, IBM Security에서 발표한 2020 클라우드 위협 환경 보고서에 따르면, 클라우드 애플리케이션에 대한 무차별 대입 공격(Brute Force Attack)과 익스플로잇 공격(Exploit Attack)으로 인해 바이러스 감염이 될 수 있으며, 2019년 한 해 클라우드 환경을 잘못 구성하여 10억 개가 넘는 레코드가 유출되었다고 밝혔다[3]. 이에 더불어 해당 보고서에서는 클라우드 보안 사고가 발생할 경우, 기업은 시간당 5만 달러 이상의 비용 손실이 발생할 수 있다고 경고하였다.

그리고, 오라클社와 KPMG에서 발행한 클라우드 위협 분석 보고서 2020[4] 에 따르면 3/4가 넘는 기관이 자체 데이터센터의 보안보다 클라우드 서비스 제공자의 보안이 더 안전하다고 느낀다고 답했다. 그러나 실제로 75%가 넘는 기관에서 데이터 손실을 경험한 적이 있다고 밝혔으며 특히, 보안 설정 오류로 인해 51%가 실제 데이터 손실이 발생하였다고 밝혔다.

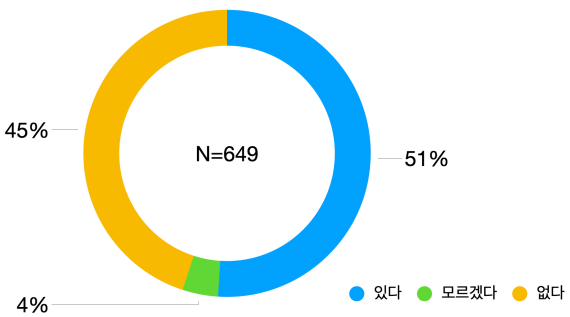

그림 1 클라우드 보안 사고로 인한 데이터 손실 경험

실제로 2019년 7월 미국의 대형 은행 중 하나인 Capital One 社에서는 대표적인 클라우드 서비스인

1) ‡교신저자: 박기웅 (세종대학교 정보보호학과 교수)

* 본 연구는 2019년도 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원(No.2019-0-00273) 및 한국연구재단 연구과제(NRF-2020R1A2C4002737)의 지원을 받아 수행된 연구임

Amazon Web Service(AWS)에 보관하고 있던 1억 600만 명이 넘는 개인정보가 외부 해커에 의해 해킹당했다고 밝혔다. 해당 기업에서 발생한 공격의 경우 클라우드 서버 자체 취약점이 아닌 방화벽 보안 설정의 오류로 인해 발생한 취약점이라고 확인되었다[5].

이에 따라 본 연구진은 클라우드 사용자가 안전하게 클라우드 환경을 사용할 수 있도록 보안 모범 사례가 적용된 Ansible 기반의 인프라 코드 생성 시스템을 제안하고자 한다. 이러한 시스템을 통해 사용자가 편리하게 보안 모범 사례를 클라우드 인프라에 적용하여 보안 사고가 발생하는 것을 예방하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 선행되었던 클라우드 보안 모범 사례와 대표적인 오픈소스 인프라 코드 도구인 Ansible, 그리고 클라우드 서비스 제공자 연동에 관한 방법에 대해 살펴본다. 3장에서는 보안 모범 사례를 적용한 인프라 코드 자동 생성 방법에 대해 제시하고, 마지막으로 4장에서는 결론에 관해 서술한다.

2. 관련 연구

본 장에서는 대표적인 클라우드 보안 모범 사례와 오픈소스 인프라 코드인 Ansible, 그리고 클라우드 서비스 제공자와의 연동 방법을 소개한다.

2.1 클라우드 보안 모범 사례

미국 국가안보국(National Security Agency)에서 2020년 1월 발간한 Mitigating Cloud Vulnerability[6]에서는 클라우드 환경에서 발생할 수 있는 취약점 유형과 기업이 클라우드 환경을 안전하게 보호하는 방법을 소개하고 있다. 해당 문서에서는 클라우드 서비스 제공자에서 제공하는 공통 구성 요소들을 [표 1]과 같이 4개로 구분하여 각각의 요소별로 보안 방법에 대해 권고하고 있으며, 키 관리 방법과 암호화 방법, 그리고 클라우드 환경에서 발생할 수 있는 다양한 취약점에 관해 설명하고 있다.

표 1 공통 클라우드 요소

요소
Identify and Access Management (IdAM)
Compute
Networking
Storage

그리고, 대표적인 클라우드 서비스 제공자인 Amazon Web Service(AWS)에서도 자사의 고객을 대상으로 클라우드 제품 사용 시 적용할 수 있는 보안 모범 사례[7]를 소개하고 있다. 해당 문서도 미국 국가안보국에서 발간한 문서와 유사하게 클라우드 내 데이터와 자산을 보호할 수 있도록 AWS 내의 서비스별로 상세하게 보안 설정과 데이터 보호 방법에 관해 설명하고 있다.

그러나 본 문서들에서 제안하는 모범 사례의 경우 실제 클라우드 사용자가 문서를 참고하여 적용하기에는 그 한계점이 있으며 사용자별로 학습 정도에 따라 적용이 일정하지 못할 수 있다는 한계점이 있다.

2.2 Ansible

Ansible은 Red Hat, Inc.에서 개발한 오픈 소스 프로비저닝 자동화 도구이다[7]. 기존의 인프라 환경 구성의 경우 배시 쉘 스크립트를 작성하여 서버에 배포하는 방식을 사용하였다. 그러나 동시에 많은 서버를 관리해야 하는 조직의 경우에는 배시 쉘 스크립트를 이용하여 같은 환경을 유지하기에는 한계점이 있었다.

이러한 한계점을 해결하기 위해 Ansible의 경우 YAML을 이용하여 자동화된 작업에 대해 선언할 수 있으며, 배포의 경우 SSH를 이용하여 별도의 Agent 설치 없이 간편하게 여러 서버에 같은 환경을 구성할 수 있도록 하였다.

3. 인프라 코드 생성 시스템

본 장에서는 기존의 문서 형태가 아닌 보안 모범 사례를 Ansible 기반의 인프라 코드 자동 생성 시스템을 이용하여 적용할 수 있는 방법을 소개한다.

3.1 보안 사례 적용 제품 선정

클라우드 서비스와 제품의 경우 서비스 제공자별로 상이하지만, 미국 국가안보국의 클라우드 보안 방어 방법에 대한 문서와 기타 클라우드 서비스 제공자에게서 구분하고 있는 요소를 [표 2]와 같이 이용하여 클라우드 서비스에서 공통으로 제공하고 있는 서비스들에 대해 보안 정책을 적용할 수 있도록 하였다.

표 2 보안 사례 적용 요소 목록

요소
Compute
Networking
Database
Storage
Identity and Access Management

이러한 목록을 통해 공통으로 적용할 수 있는 클라우드 서비스에 대해 보안 모범 사례를 적용할 수 있도록 하였다.

3.2 클라우드 서비스 제공자

본 연구에서 제안하는 시스템에서 연동 가능한 클라우드 서비스 제공자를 선정하기 위해 [그림 2]와 같이 Synergy Research Group에서 발간한 클라우드 서비스 제공자 성장성과 시장 점유율 정보에서 점유율이 높은 3개의 서비스 제공자를 선정하여 연동하였다.

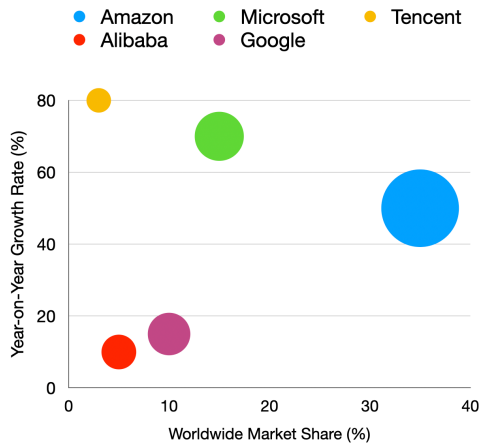

그림 2 클라우드 서비스 별 성장성 및 점유율

이러한 정보를 통해 선정된 클라우드 서비스 제공자는 Amazon, Inc. 의 Amazon Web Service (AWS), Microsoft, Inc. 의 MS Azure, 그리고 Google, Inc. 의 Google Cloud Platform (GCP) 와 같다.

3.3. Ansible 코드 생성

클라우드 서비스 제공자에 대한 Ansible 코드의 경우 사용자가 선택하여 클라우드 서비스 별로 보안 사례를 적용할 수 있도록 표준화된 Template을 제작하였다. 아래 [그림 3] 의 경우 Amazon Web Service 의 EC2와 S3 서비스를 관리하는 Ansible Playbook 스크립트이다.

```
- amazon.aws.ec2:
    key_name: aws-example
    instance_type: t2.micro
    image: aws-ami-example
    wait: yes
    group: kloud-server
    count: 3
    vpc_subnet_id: aws-subnet-example
    assign_public_ip: yes
    instance_tags:
        - kloud

- name: Simple S3 management
  amazon.aws.aws_s3:
    bucket: aws-example-bucket
    object: kloud/example.txt
    src: /tmp/example.txt
    mode: put
```

그림 3 Ansible Code Template (AWS)

위와 같이 제작한 클라우드 템플릿에 사용자가 원하는 서비스를 블록 형태로 결합하는 방식으로 구현할 수 있다. 이러한 방식을 통해 대표적인 클라우드 서비스 요소별로 보안 사례가 적용된 인프라 코드를 사용자에게 제공할 수 있다.

4. 결론 및 추후 연구

본 논문에서는 Ansible을 이용하여 클라우드 사용자가 편리하게 보안 모범 사례를 적용할 수 있는 인프라 코드 자동 생성 시스템에 대해 제안하였다. 이를 통해 다양화된 보안 위협으로부터 클라우드 인프라를 보호할 수 있을 것으로 기대한다. 하지만 클라우드 서비스의 발전 속에서 본 논문에서 제안하는 인프라 코드 생성 시스템을 통해 적용할 수 있는 클라우드 서비스의 종류와 제품 요소가 제한적이라는 한계가 있다. 이를 위해, 더 다양한 클라우드 제품에 대한 보안 사례를 인프라 코드로 적용할 수 있도록 추가 연구를 진행할 계획이다.

참 고 문 헌

[1] Jared Spataro, “2 years of digital transformation in 2 months”, Microsoft 365, 2020

[2] Wavw12, “COVID-19 Impact on IT Spending Survey”, IDC, 2020

[3] “IBM Security X-Force Incident Response and Intelligence Services(IRIS)“, IBM Security, 2020

[4] “Oracle and KPMG Cloud Threat Report 2020”, Oracle and KPMG, 2020

[5] N. N. Neto, S. Madnick, A. M. G. de Paula, and N. M. Borges, “A Case Study of the Capital One Data Breach”, Working Paper CISL#2020-16, 2020

[6] “Mitigating Cloud Vulnerabilities”, National Security Agency, 2020

[7] “Best Practices for Security, Identity & Compliance”, AWS Architecture Center, 2021