AWS 취약점 – Anisible Provisioning

1. Ansible Provisioning

Ansible은 오픈 소스 구성 관리 및 오케스트레이션 도구로, 다양한 시스템 및 클라우드 환경에서 사용된다. 이는 AWS Systems Manager와 같이 IT 운영 및 관리를 자동화하는 데 사용되는 도구이다. IaC라는 개념이 적용된 인프라인데, IaC란 Infrastructure as a Code의 축약어로 컴퓨터의 인프라 구성을 소프트웨어를 개발하는 것처럼 코드로 작성하는 것을 의미한다. Ansible은 자동화 도구를 이용하여 인프라의 설정을 코드로 작성하고 이를 모든 서버에 배포함으로써 특정 환경을 동이랗게 유지할 수 있도록 도와준다.

Ansible 프로비저닝은 **Ansible을 사용하여 컴퓨터 시스템을 자동화하고 설정하는 과정**을 말한다. Provisioning은 사용자의 요구에 맞게 시스템 자원을 할당, 배치, 배포해 두었다가 필요 시 시스템을 즉시 사용할 수 있는 상태로 미리 준비해 두는 것이다.

2. Ansible Provisioning 실습

Master랑 Slave, 두 개의 시스템을 기반으로 Master에 ansible을 설치하여 slave(서버)에 원격으로 접속하도록 할 수 있다. 먼저 Slave에 특정계정을 호스트에 상관없이 비밀번호를 통해 접속할 수 있는 계정을 만들고 Master에서 이 계정을 통해 자신이 생성한 공개키를 slave에 복사해 놓는다. 그러면 master는 개인키를 사용하여 slave에 연결하고, slave는 공개 키를 사용하여 인증을 수행한다. SSH 키 기반 인증이 설정되면 보안이 강화되고 비밀번호 인증을 하지 않아도 된다는 장점이 있다.

전반적인 실습과정은 다음과 같다.

[MASTER] [SLAVE] Master 역할을 수행할 docker container와 Slave 역할을 수행할 ubuntu이미지를 기반으로 한 docker container를 만든다.

텍스트, 소프트웨어, 폰트, 웹 페이지이(가) 표시된 사진

자동 생성된 설명



[MASTER] master 컨테이너에 net-tools, vim, ansible을 설치한다.

- net-tools : 네트워크 관련 유틸리티를 제공(ifconfig, netstat, arp, route등)

- vim : 텍스트 편집기

- ansible : IT자동화 및 구성 관리 도구로 사용. 서버구성, 소프트웨어 설치, 업그레이드 등 다양한 자동화 작업을수행할 수 있다. YAML 구문을 사용하여 작업을 정의하며, SSH 또는 다른 연결 프로토콜을 사용하여 원격시스템에 명령을 보낸다.



[SLAVE] Slave 컨테이너에 ssh, net-tools, sudo, vim을 설치한다.



- ssh : secure shell의 약자로, 원격으로 다른 컴퓨터에 안전하게 연결하고 원격 명령을 실행하는데 사용되는 프로토콜 및 관련 도구를 제공한다.

- sudo : superuser do의 약자로, 리눅스 시스템에 루트 권한으로 명령을 실행하는데 사용되는 명령

[SLAVE] slave 시스템에 test라는 사용자 계정을 생성한다.

텍스트, 스크린샷, 폰트, 메뉴이(가) 표시된 사진

자동 생성된 설명

[SLAVE] test라는 계정에게 어떤 호스트에서든 어떤 명령이든 비밀번호를 입력하지 않고 sudo로 실행할 수 있는 권한을 부여한다.





[MASTER] RSA 암호화 알고리즘을 사용하여 공개키와 개인키쌍이 생성된다. 공개키는 ~/.ssh/id\_rsa.pub 파일에 저장되고, 개인키는 ~/.ssh/id\_rsa 파일에 저장된다. 지금 생성된 공개키를 원격 서버에 등록하여 SSH 키 기반 인증을 활성화.

텍스트, 스크린샷, 폰트, 메뉴이(가) 표시된 사진

자동 생성된 설명

[MASTER] ssh 클라이언트를 사용하여 ip주소로 원격 서버에 연결을 시도한다. 원격 서버로의 연결이 설정되면, 원격 서버와 로컬 시스템 간의 안전한 통신이 가능해진다.

텍스트, 스크린샷, 메뉴, 폰트이(가) 표시된 사진

자동 생성된 설명



[MASTER] 로컬시스템(master)의 ./ssh/id\_rsa.pub에 저장된 RSA 공개키를 원격서버(slave)에 복사하여 SSH키 기반 인증을 사용하여 로컬과 원격서버가 통신하도록 한다. 이 설정을 통해 비밀번호 인증 대신 SSH 기반 인증을 사용하여 원격서버에 접근 가능해 진다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

[MASTER] /etc/ansible/hosts 파일에 clients 그룹과 해당 그룹에 속하는 호스트에 대한 정보를 추가한다. 호스트172.17.0.3을 clients 그룹에 추가하고 이 호스트에 ssh 연결할 때 사용할 사용자는 ‘test’이다.





[MASTER] ansible을 사용하여 clients 그룹에 속한 호스트에 대한 ping 모듈을 실행한다. 호스트가 응답하는 경우 pong 메시지가 나타난다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

[MASTER] ansible을 사용하여 ‘security.yml’이라는 ansible 플레이북을 실행하는 명령이다. 이 명령은 ansible을 사용하여 시스템 보안 설정을 프로비저닝하거나 업데이트하는데 사용된다.

- security.yml : ansible 플레이북의 파일 이름이다. Ansible에서 실행할 작업 및 설정을 정의하는 파일이다.

- name : 플레이의 이름으로, 플레이 실행 중에 표시된다.

- hosts : 플레이북을 실행할 호스트 그룹

- tasks : 플레이에 포함된 작업 목록이다. 첫 번째 작업은 **apt** 모듈을 사용하여 원격 서버의 패키지를 업그레이드한다. 두 번째 작업은 파일 모듈을 사용하여 **/testtest**라는 경로에 빈 파일을 만든다.



텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

[SLAVE] /testtest파일이 생성된걸 확인할 수 있다.

