

WAPPLES SA(AWS)

AWS WAPPLES SA 설치

I. WAPPLES SA 설치 방법

1. AMI 공유

- 1) 각 고객사 AWS Account ID로 WAPPLES SA AMI 공유 진행
 - A. 펜타시큐리티 진행
 - B. 펜타시큐리티 측으로 고객사의 account id 정보 전달 필요

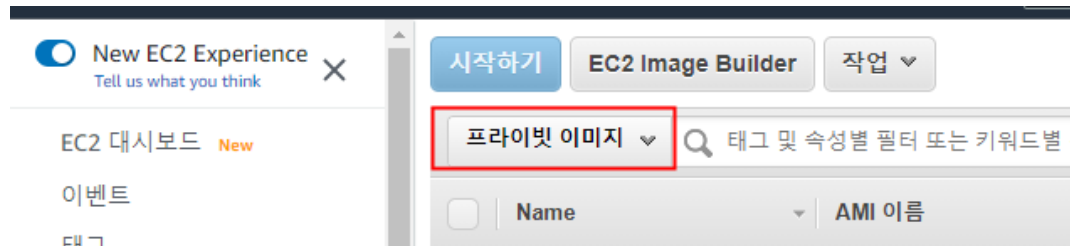
계정 설정

계정 ID: 083049815657
판매자: AWS Inc.
계정 이름: pentasecurity_wapples
암호: *****

Name	AMI 이름	AMI ID	소스	소유자	표시 여부	상태	생성 날짜	플랫폼	루트 디바이스
	[WAPPLES_SA]-6.0.4.6-hotfix4v2	ami-070de63b992c0945a	083049815657/...	083049815657	프라이빗	available	2021년 3월 2일 오후 3시 26...	Other Linux	ebs
	[WAPPLES_SA]-6.0.4.6-hotfix4v3	ami-0b538a6db136676c6	083049815657/...	083049815657	프라이빗	available	2021년 3월 9일 오후 4시 5분...	Other Linux	ebs
	[WAPPLES_SA]-6.0.4.6_v2	ami-0f45c2270268bdfid	083049815657/...	083049815657	프라이빗	available	2021년 1월 29일 오후 5시 2...	Other Linux	ebs
	[WAPPLES_SA]-6.0.4.7-hotfix1	ami-005f850fa5b1bfa8d	083049815657/...	083049815657	프라이빗	available	2021년 3월 11일 오전 11시 2...	Other Linux	ebs
	[WAPPLES_SA]-6.0.4.7-hotfix2	ami-0e783ec17d395f363	083049815657/...	083049815657	프라이빗	available	2021년 4월 13일 오후 4시 4...	Other Linux	ebs
	AP-BASE-DEB8-Freedisk	ami-0a025e6da09cf5ae2	083049815657/...	083049815657	프라이빗	available	2018년 10월 31일 오후 1시 ...	Other Linux	ebs

2. 공유 받은 AMI로 WAPPLES SA 인스턴스 생성

- 1) 공유 받은 AMI는 이미지 -> AMI -> 프라이빗 이미지에 표시됨



AWS WAPPLES SA 설치

I. WAPPLES SA 설치 방법

3. 인스턴스 타입 선정

- 1) 6.0.4.x 버전 지원 인스턴스 타입 : M5, C5
- 2) M5 타입 권장
- 3) WAPPLES SA 스펙이 맞는 인스턴스 타입 선정
- 4) 인터페이스는 1개 사용

모델	인스턴스 타입	CPU	Disk(변동가능)
WAPPLES SA-50	m5.large	2 Core	100G
WAPPLES SA-100	m5.xlarge	4 Core	100G
WAPPLES SA-500	m5.2xlarge	8 Core	100G
WAPPLES SA-1000	m5.4xlarge	16 Core	100G

단계 2: 인스턴스 유형 선택

Amazon EC2는 각 사용 사례에 맞게 최적화된 다양한 인스턴스 유형을 제공합니다. 인스턴스는 애플리케이션을 실행할 수 있는 가상 서버입니다. 이러한 인스턴스에는 CPU, 메모리, 스토리지 및 네트워킹 용량의 다양한 조합이 있으며, 애플리케이션에 사용할 적절한 리소스 조합을 유연하게 선택할 수 있습니다. 인스턴스 유형과 이 인스턴스 유형이 컴퓨팅 요건을 충족하는 방식에 대해 [자세히 알아보기](#).

필터링 기준: **m5** **현재 세대** 열 표시/숨기기

현재 선택된 항목: t2.micro (~ ECU, 1 vCPUs, 2.5 GHz ~, 1 GiB 메모리, EBS 전용)								
	그룹	유형	vCPUs ⓘ	메모리 (GiB)	인스턴스 스토리지 (GB) ⓘ	EBS 최적화 사용 가능 ⓘ	네트워크 성능 ⓘ	IPv6 지원 ⓘ
☐	m5	m5.large	2	8	EBS 전용	예	최대 10기가비트	예
☐	m5	m5.xlarge	4	16	EBS 전용	예	최대 10기가비트	예
☐	m5	m5.2xlarge	8	32	EBS 전용	예	최대 10기가비트	예
☐	m5	m5.4xlarge	16	64	EBS 전용	예	최대 10기가비트	예
☐	m5	m5.8xlarge	32	128	EBS 전용	예	10기가비트	예

AWS WAPPLES SA 설치

I. WAPPLES SA 설치 방법

4. 보안 그룹 설정

1) WAF 인스턴스 생성 시 필수 open 보안 그룹

A. Inbound

Type	Protocol	Port Range	Source IP	용도
Custom TCP rule	TCP	22	관리자 IP	WAF MGMT 접근
Custom TCP rule	TCP	5000, 5001	관리자 IP	
Custom TCP rule	TCP	80	WAF 상단 보안 그룹 또는 any	서비스 운영
Custom TCP rule	TCP	443		

B. Outbound

Type	Protocol	Port Range	Destination IP	용도
Custom TCP rule	TCP	443	(공인망)	PENTA WAF 라이선스 업데이트 서버
Custom TCP rule	ICMP	-	218.145.29.166/32	
Custom TCP rule	TCP	443	(공인망) 218.145.29.101/32	

- 2) WAF 이중화(설정 동기화 기능 사용 시) 또는 Auto Scaling 사용 시 장비 간 5984(Sync) 또는 6984(PLS) 포트 허용 필요

AWS WAPPLES SA 설치

II. WAPPLES SA 접속 방법

1. SSH 접속 방법

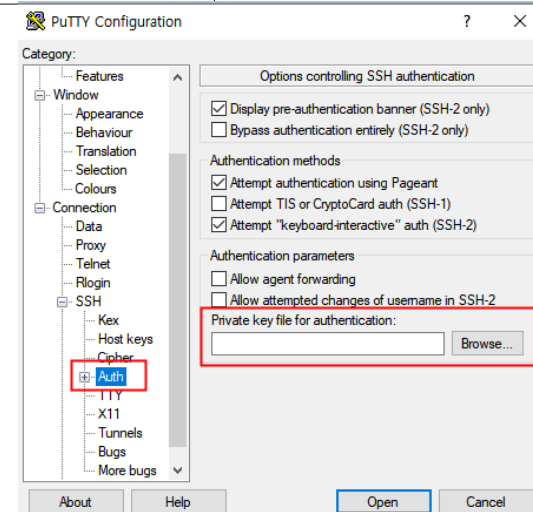
1) 인스턴스 생성 시 ssh 접근을 위한 키 페어 생성

A. 키 페어를 생성하게 되면 pem 형식으로 생성이 되며, puttygen을 통해 ppk 형식으로 변환



1) ppk 파일을 통한 ssh 접근

- A. Putty를 사용하여 ssh 접근 시 key 파일 입력 필요
- B. ssh 계정 : ubuntu(key파일 접근 시 패스워드 없음)
- C. 별도의 pentasec 계정도 존재



AWS WAPPLES SA 설치

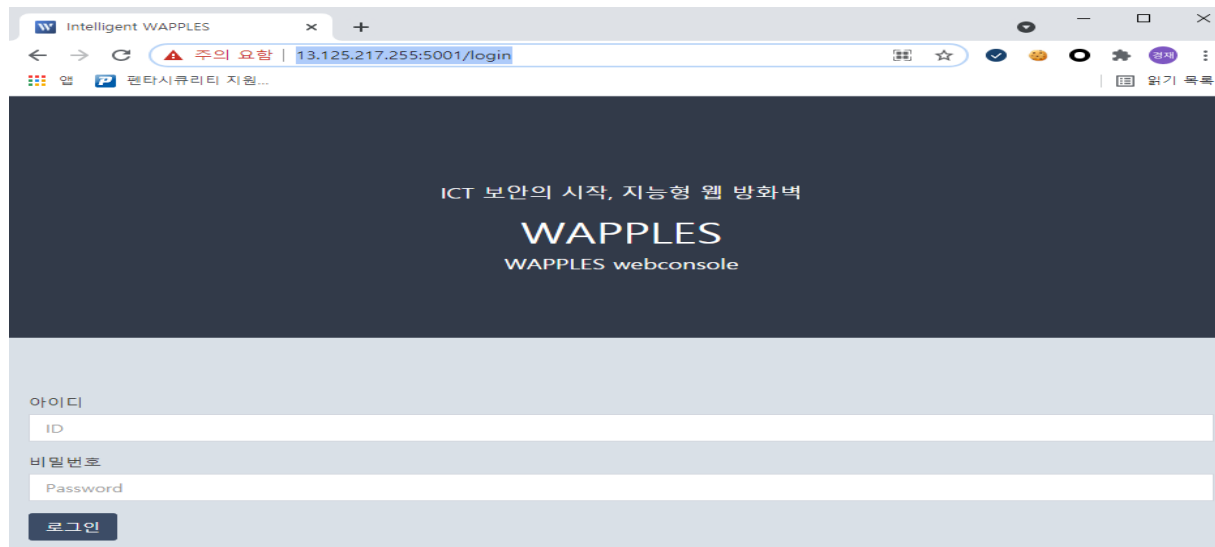
II. WAPPLES SA 접속 방법

2. 관리도구 접속

1) 크롬 브라우저 권장

A. <https://웹방화벽IP:5001>

B. 관리도구 접속 포트 : 5001



AWS WAPPLES SA 설치

III. WAPPLES SA 정상 동작 확인

1. Network(bridge)설정은 자동으로 설정됨
 - 1) Br0 인터페이스에 IP 할당 되어져 있는지 확인
 - 2) Bridge 설정 확인
 - 3) Routing 인터페이스 br0로 설정되어져 있는지 확인

```
pentasec@ip-172-31-31-132:~$ network
pentasec@ip-172-31-31-132:(network)# show bridge
bridge name      bridge id      STP enabled    interfaces
br0              8000.0afc899eb460  no             ens5
pentasec@ip-172-31-31-132:(network)# show if
br0
    LINK - address: 0a:fc:89:9e:b4:60, broadcast ff:ff:ff:ff:ff:ff
    INET - address: 172.31.31.132/20
ens5
    LINK - address: 0a:fc:89:9e:b4:60, broadcast ff:ff:ff:ff:ff:ff
pentasec@ip-172-31-31-132:(network)# show rt
DESTINATION: default, GATEWAY: 172.31.16.1, IFACE: br0
DESTINATION: 172.31.16.0/20, GATEWAY: 0.0.0.0, IFACE: br0
DESTINATION: 172.31.16.1/32, GATEWAY: 0.0.0.0, IFACE: br0
pentasec@ip-172-31-31-132:(network)#
```

2. Sysmon 로그 확인
 - 1) 생성한 스펙의 탐지엔진이 할당 되었는지 확인

```
pentasec@ip-172-31-31-132:(wapples)# show log wapples sysmon.log follow
06 11:01:47 92 5 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 11.0
06 11:01:48 96 2 2 0 3492 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 2.0
06 11:01:49 92 5 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 2.0
[May 06 11:01:50 +0900] ----mem---- status ----engine----- ---engine status-- ---kernel--- through
----time---- idl-us-sy-io free-cache --- |N-|G-|W-|F-|E-| cps-tps-sess-traKB cps-ses-buf put (Kbps)
06 11:01:50 92 5 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 17.0
06 11:01:51 82 13 3 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 8.0
06 11:01:52 93 4 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 100.0
06 11:01:53 92 5 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 12.0
06 11:01:54 93 4 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 6.0
06 11:01:55 93 4 2 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 8.0
06 11:01:56 86 10 3 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 3.0
06 11:01:57 96 2 1 0 3491 2733 --- | 0 | 2 | 0 | 0 | 0 | 0 0 0 0 0 0 0 0 88.0
```

AWS WAPPLES SA 설치

III. WAPPLES SA 정상 동작 확인

3. ID 갱신 확인

- 1) 펜타시큐리티 라이선스 서버와 정상 통신 하여 부팅 시 ID 값이 자동으로 갱신됨
- 2) 아래 캡처 화면과 같이 숫자로 넘버링 되었는지 확인

```
pentasec@ip-172-31-31-132#  
pentasec@ip-172-31-31-132# wapples  
pentasec@ip-172-31-31-132:(wapples)# show id  
WVX-AWS-003352  
pentasec@ip-172-31-31-132:(wapples)#
```

3) 갱신 되지 않았을 경우

- A. telnet 명령어를 통해 라이선스 서버와 통신 여부 확인 후 담당자에게 아웃바운드 허용 요청

- ① 라이선스 서버 정보는 필수 open 포트 정보 참고

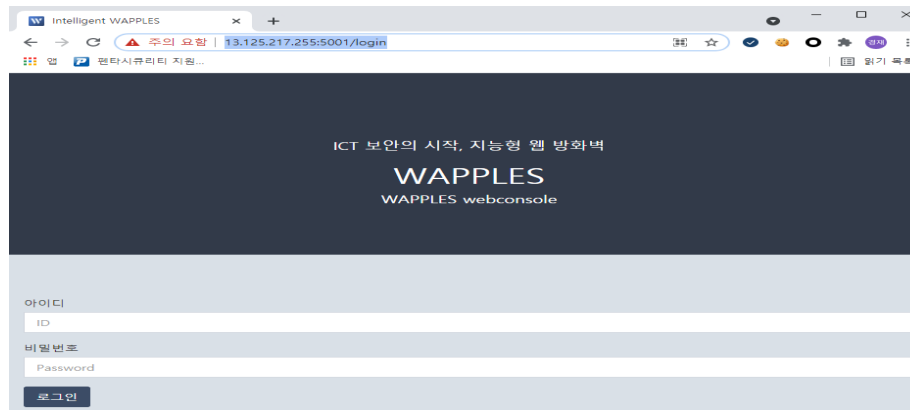
```
Executed Command [telnet 218.145.29.166 443]  
pentasec@ip-172-31-31-132:(wapples)# command telnet 218.145.29.166 443  
Trying 218.145.29.166...  
Connected to 218.145.29.166.  
Escape character is '^]'.  
^CConnection closed by foreign host.  
executed command [telnet 218.145.29.166 443]  
pentasec@ip-172-31-31-132:(wapples)# command telnet 218.145.29.101 443  
Trying 218.145.29.101...  
Connected to 218.145.29.101.  
Escape character is '^]'.  
^CConnection closed by foreign host.
```

AWS WAPPLES SA 설치

III. WAPPLES SA 정상 동작 확인

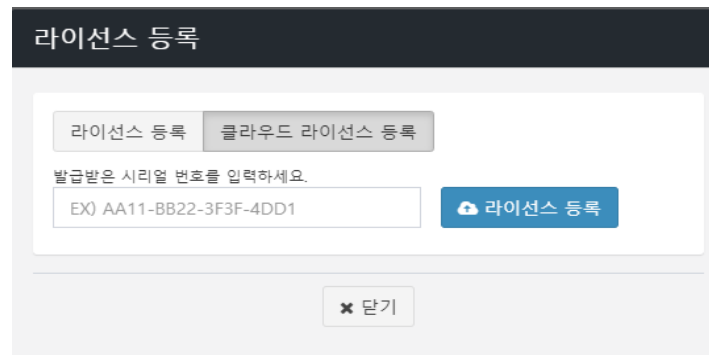
4. 관리도구 접속 확인 및 라이선스(시리얼키) 입력

1) [https://1.1.1.1\(할당IP\):5001](https://1.1.1.1(할당IP):5001) 접속



2) 최초 계정 정보로 접속하여 라이선스 등록

A. 라이선스(시리얼키)는 펜타시큐리티 측으로 부터 전달 받아야 함



AWS WAPPLES SA 설치

III. WAPPLES SA 정상 동작 확인

4. 관리도구 접속 확인 및 라이선스(시리얼키) 입력
 - 3) 시간 동기화 사용 설정
 - A. 최초 로그인 후 시간동기화 설정 필수
 - B. 별도의 서버가 없다면 펜타시큐리티 서버 이용

The screenshot displays the '환경 설정 > 시스템 > 시간 동기화 (WAPPLES 시스템의 시간을 설정합니다.)' configuration page. It features two tabs: '동기화 사용' (highlighted with a red box) and '수동 시간 설정'. Under the '동기화 사용' tab, the '시간 서버 설정' section is visible. It includes two server configuration blocks. '서버 1' has '직접 입력' selected, with 'Penta Server 1' and 'Penta Server 2' buttons, and an 'IP or 도메인' field containing '218.145.29.166'. '서버 2' also has '직접 입력' selected, with 'Penta Server 1' and 'Penta Server 2' buttons, and an 'IP or 도메인' field containing '218.145.29.163'. At the bottom, there are dropdown menus for '표준 시간대' (set to 'Asia') and a city selection (set to 'Seoul').

AWS WAPPLES SA 설치

IV. LB 헬스체크 정보

1. WAPPLES SA 앞단에 LB가 있을 경우 LB에서 WAF 헬스체크 할 수 있도록 정보 제공 필요
 - 1) 헬스체크 프로토콜 : HTTP / HTTPS / TCP
 - 2) 헬스 체크 URL : /
 - 3) 헬스 체크 Port : HTTP - 5000, HTTPS - 5001, TCP - 5000
 - 4) 웹방화벽의 apache 에서 응답을 하므로, 웹방화벽 인스턴스 까지만 헬스체크 진행됨

Targets	Monitoring	Health checks	Attributes	Tags
Health check settings				
Protocol	Path	Port	Healthy threshold	
HTTP	/	5000	5 consecutive health check successes	
Unhealthy threshold	Timeout	Interval	Success codes	
2 consecutive health check failures	5 seconds	30 seconds	200	

t h a n k y o u



KOREA Yeouido, Seoul www.pentasecurity.com (HQ)
U.S.A. Houston, Texas www.pentasecurity.com/en
JAPAN Shinjuku-Ku, Tokyo www.pentasecurity.co.jp