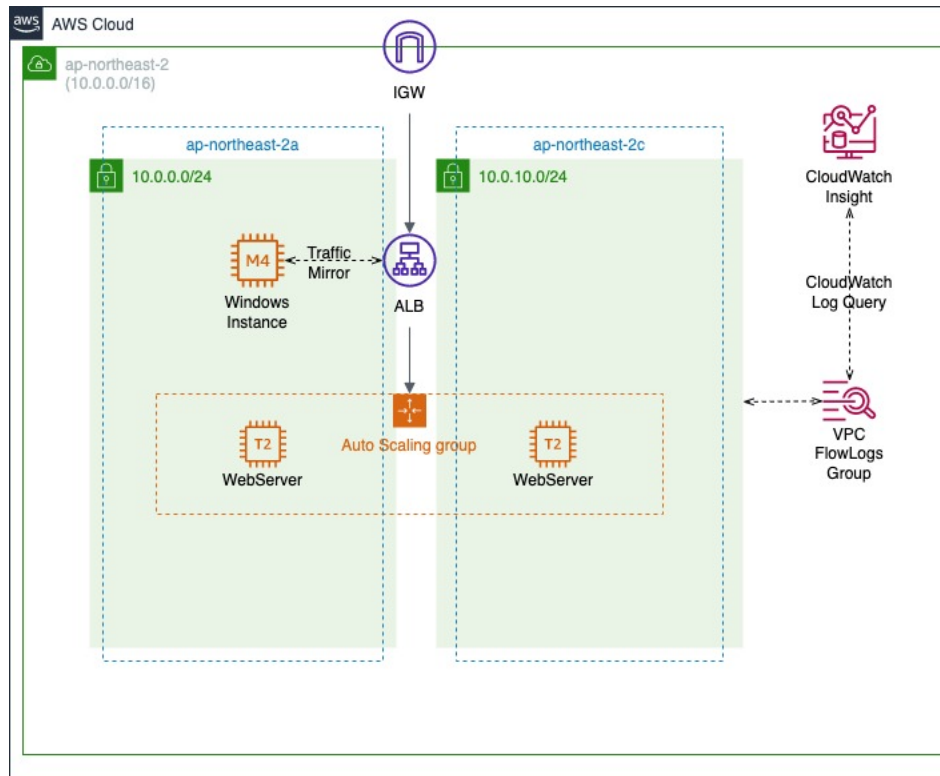


VPC FlowLog&Traffic Mirror Workshop

Introduce

본 워크샵은 VPC FlowLog 및 Traffic Mirror를 실습하기 위하여 준비되었습니다. VPC FlowLog와 Traffic Mirror를 실제로 보기 위해 가상의 3 Tier 웹 어플리케이션을 구성하고 어플리케이션에서 발생하는 Traffic를 실제로 보고 확인해 보겠습니다.

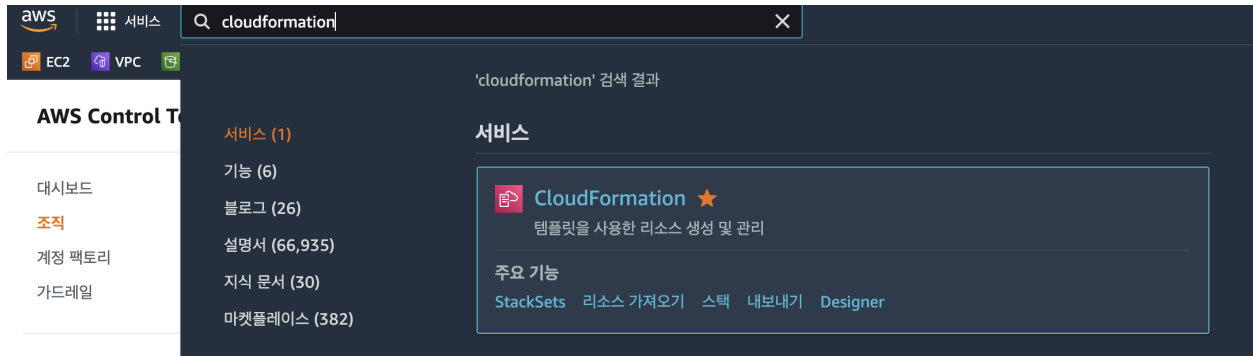


우리는 위와 같은 구성을 생성하여 실습할 것입니다.

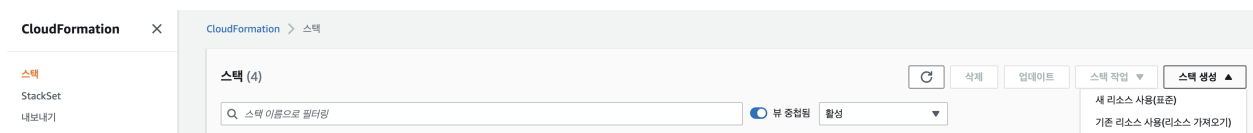
1. CloudFormation Template 수행

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/19f88f60-c80e-46c7-abc1-3ea1f7546f1f/VPC_AutoScaling_and_ElasticLoadBalancer.template

Region : ap-northeast-2



Cloudformation 검색후 해당 콘솔로 이동



스택 생성 클릭 → 새 리소스 사용(표준) 클릭

스택 생성

사전 조건 - 템플릿 준비

템플릿 준비
모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

☒ 준비된 템플릿
 ☐ 샘플 템플릿 사용
 ☐ Designer에서 템플릿 생성

템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

템플릿 소스
템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

☐ Amazon S3 URL
 ☒ 템플릿 파일 업로드

템플릿 파일 업로드

선택한 파일이 없습니다.

JSON 또는 YAML 형식 파일

S3 URL: 템플릿 파일을 업로드하면 생성됩니다.

취소

다음

사전에 다운로드한 템플릿 파일 업로드

스택 이름

스택 이름

스택 이름 입력

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

파라미터

파라미터는 템플릿에서 정의되며, 이를 통해 스택을 생성하거나 업데이트할 때 사용자 지정 값을 입력할 수 있습니다.

InstanceCount

Number of EC2 instances to launch

1

InstanceType

WebServer EC2 instance type

t2.small

KeyName

Name of an existing EC2 KeyPair to enable SSH access to the instances

MirrorInstanceType

WebServer EC2 instance type

m4.large

SSHLocation

Lockdown SSH access to the bastion host (default can be accessed from anywhere)

0.0.0.0/0

VpcName

Name of VPC Name

InstanceCount - ASG에서 생성한 EC2의 수량입니다. 1로 합니다

InstanceType - 생성될 EC2의 Type입니다. t2.small로 설정합니다.

KeyName - EC2의 Key입니다. 사전에 생성한 Key를 자동으로 찾습니다.

MirrorInstanceType - Traffic Mirror Target으로 사용한 EC2의 Type입니다. M시리즈 이상부터 Traffic Mirror 설정이 가능합니다

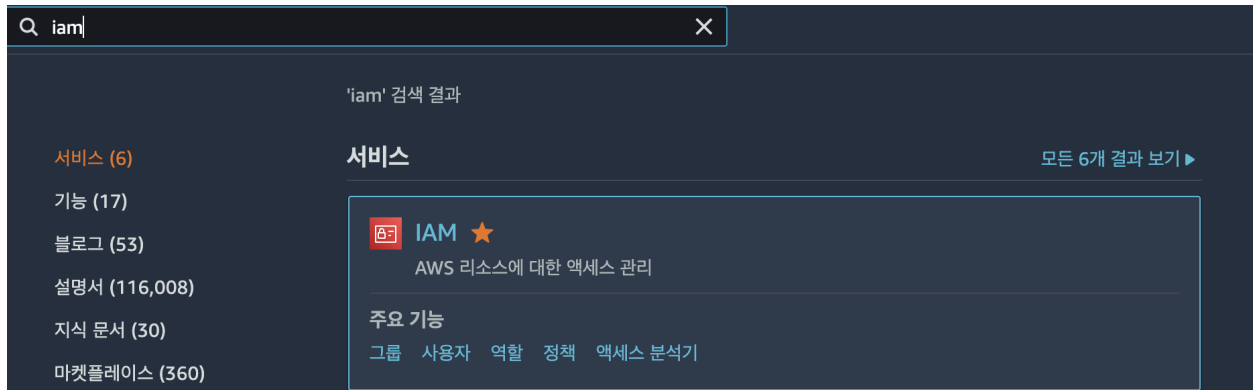
SSHLocation - EC2의 SSH 접근 Source IP입니다. 보안을 위하여 자신의 IP로 변경합니다.

VpcName - 생성될 VPC의 Name입니다.

2. VPC FlowLog

VPC FlowLog 활성화방안

- CloudWatch Logs를 Target으로 하는 경우 사전에 Log Group과 IAM Role 생성이 필요합니다.



IAM 콘솔로 이동

정책 생성

1 2 3

정책은 사용자, 그룹, 또는 역할에 할당할 수 있는 AWS 권한을 정의합니다. 시각적 편집기에서 JSON을 사용하여 정책을 생성하고 편집할 수 있습니다. [자세히 알아보기](#)

시각적 편집기

JSON

[관리형 정책 가져오기](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "logs:CreateLogGroup",
8         "logs:CreateLogStream",
9         "logs:PutLogEvents",
10        "logs:DescribeLogGroups",
11        "logs:DescribeLogStreams"
12      ],
13       "Resource": "*"
14     }
15   ]
16 }

```

보안: 0 오류: 0 경고: 0 추천: 0

정책 생성

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}

```

```
}  
}  
}
```

정책 이름은 **VPCFlowLogToCWLogsPolicy** 로 합니다

신뢰할 수 있는 엔터티 선택

신뢰할 수 있는 엔터티 유형

☐ AWS 서비스

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

☐ AWS 계정

사용자 또는 서드 파티에 속한 다른 AWS 계정의 엔터티가 이 계정에서 작업을 수행하도록 허용합니다.

☐ 웹 자격 증명

지정된 외부 웹 자격 증명 공급자와 연동된 사용자가 이 역할을 맡아 이 계정에서 작업을 수행하도록 허용합니다.

☐ SAML 2.0 연동

기업 디렉터리에서 SAML 2.0과 연동된 사용자가 이 계정에서 작업을 수행할 수 있도록 허용합니다.

☒ 사용자 지정 신뢰 정책

다른 사용자가 이 계정에서 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

사용자 지정 신뢰 정책

다른 사용자가 이 계정에서 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Principal": {},  
8       "Action": "sts:AssumeRole"  
9     }  
10  ]  
11 }
```

다음으로 사이드에 역할을 클릭하여 역할을 생성합니다.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "vpc-flow-logs.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole"  
    }  
  ]  
}
```

권한 추가

권한 정책 (776)새 역할에 연결할 정책을 하나 이상 선택합니다.정책 생성

1 개 일치

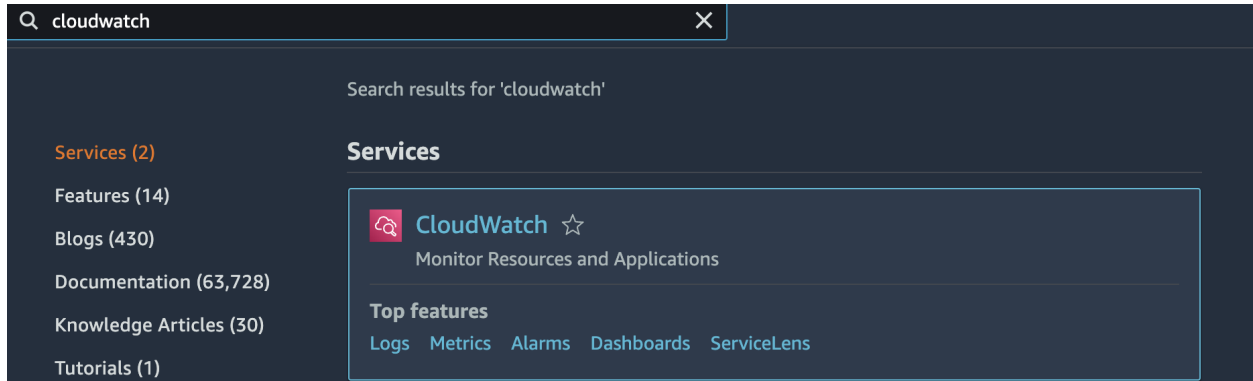
<input type="checkbox"/>	정책 이름	유형	설명
<input type="checkbox"/>	VPCFlowLogToCWLog...	고객 관리형	VPCFlowLogToCWLogsPolicy

이전에 생성한 Policy를 선택합니다. 역할의 이름은 **VPCFlowLogToCWLogsRole** 로 합니다.

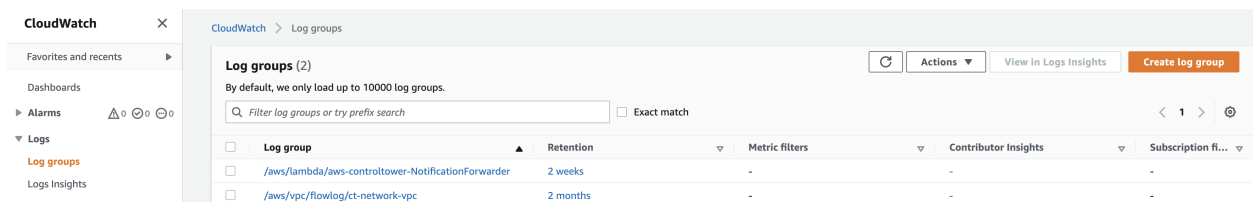
S3를 Target으로 한 경우 별도의 Role, Policy 생성 없이 자동으로 Target S3에 Policy가 생성됩니다.

KDF를 Target으로 할때 Source Account/Different Account로 나뉘어 설정이 가능합니다

- Same Account인 경우 KDF에 Log를 Delivery할수 있는 권한만 부여되면 정상작동합니다.
- Different Account는 Role Federation설정이 되어야만 정상적으로 작동합니다.



생성이 완료된후 CloudWatch Logs Group을 생성해 줘야 합니다. CloudWatch Console로 이동합니다.



Logs Group으로 이동하여 Create log group를 클릭합니다.

Create log group

Log group details

Log group name

Retention setting

KMS key ARN - optional

Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

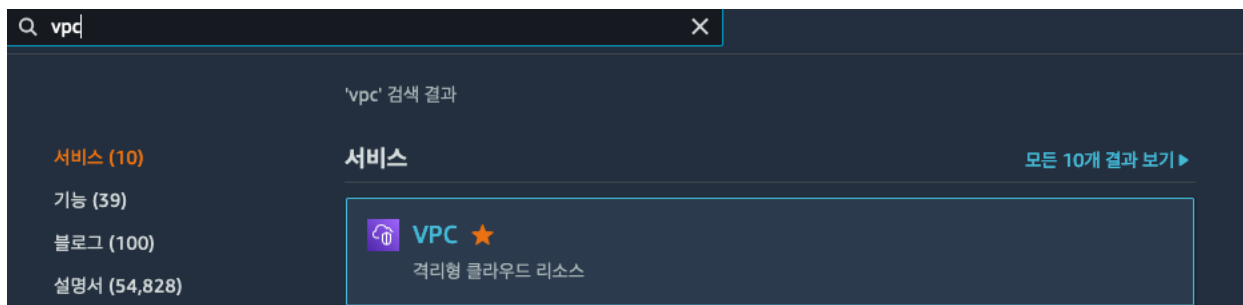
Add new tag

You can add up to 50 more tag(s).

Cancel

Create

로그 그룹 이름을 입력하고 만료기간은 1개월로 설정하여 생성합니다.



VPC Console로 이동합니다

VPC (1/3) **필터**

Q VPC 필터링

Name	VPC ID	상태	IPv4 CIDR	IPv6 CIDR	DHCP 옵션 세트	기본 라우팅 테이블	기본 네트워크 ACL	태그	기본 VPC	소유자 ID
<input checked="" type="checkbox"/> vpc-flow-log-test	vpc-0c41dd9be0560525f	Available	10.0.0.0/16	-	dhcp-0bed526449c0...	rtb-0a3afe3d7386f3ca	acl-04b965faad08deb11a	Default	아니요	322683045347
<input type="checkbox"/> vpc2	vpc-020ce9a07b5b7b3cb	Available	10.0.0.0/16	-	dhcp-0bed526449c0...	rtb-0b6f566ed503527d6	acl-0179a97e518ad989	Default	아니요	322683045347
<input type="checkbox"/> wordpress-vpc	vpc-082f0daf4e21d08ad	Available	10.0.0.0/16	-	dhcp-0bed526449c0...	rtb-04ebc26e12a01642f	acl-03a6591b34069c775	Default	아니요	322683045347

vpc-0c41dd9be0560525f / vpc-flow-log-test

세부 정보 CIDR **플로우 로그** 태그

플로우 로그 **필터**

Q 플로우 로그 필터링

Name	플로우 로그 ID	필터	대상 유형	대상 이름	IAM 역할 ARN	Cross account IAM role	최대 집계 간격	생성
이 리전에서 플로우 로그를 찾을 수 없음								

사전에 CloudFormation Stack으로 생성한 VPC를 선택하고 FlowLog를 생성합니다.

플로우 로그 설정

이름 - 선택 사항

vpc-flow-log

필터
캡처할 트래픽 유형입니다(수락된 트래픽만, 거부된 트래픽만 또는 모든 트래픽).

☐ 수락
☐ 거부
☒ 모두

최대 집계 간격 정보
패킷 플로우가 캡처되어 플로우 로그 레코드로 집계되는 최대 시간 간격입니다.

☐ 10분
☒ 1분

대상
플로우 로그 데이터를 게시할 대상입니다.

☒ CloudWatch Logs로 전송
☐ Amazon S3 버킷으로 전송
☐ Send to Kinesis Firehose in the same account
☐ Send to Kinesis Firehose in a different account

대상 로그 그룹 정보
플로우 로그를 게시하는 Amazon CloudWatch 로그 그룹 이름입니다. 모니터링되는 각 네트워크 인터페이스에 대해 새 로그 스트림이 생성됩니다.

/aws/vpc/flow-log

IAM 역할 정보
Amazon CloudWatch 로그 그룹에 게시할 권한이 있는 IAM 역할입니다. [권한 설정](#)

VPCFlowLogToCWLogsRole

로그 레코드 형식
플로우 로그 레코드에 포함할 필드를 지정합니다.

☐ AWS 기본 형식
☒ 사용자 지정 형식

사전에 생성한 CloudWatch Log Group과 IAM 역할을 선택합니다.

- 로그 레코드 형식은 **사용자 지정 형식**으로 선택하고 **모두 선택**을 클릭 합니다.

/aws/vpc/flow-log

작업 ▼ Logs Insights에서 보기 로그 그룹 검색

▼ 로그 그룹 세부 정보

로그 1개일	생성 시간 4분 전	구독 필터 0
KMS 키 ID -	자료 필터 0	기여자 인사이트 규칙 -
	저장된 바이트 -	ARN arn:aws:logs:ap-northeast-2:322683045347:log-group:/aws/vpc/flow-log*

로그 스트림 | 자료 필터 | 구독 필터 | 기여자 인사이트 | 태그

로그 스트림 (2)

로그 스트림 필터링 또는 쿼리 실행 시도 ☐ 정확히 일치

로그 스트림 삭제 로그 스트림 생성 Search all log streams

<input type="checkbox"/> 로그 스트림	마지막 이벤트 시간
<input type="checkbox"/> eni-0e4957b9001270d04-all	2022-09-26 21:08:57 (UTC+09:00)
<input type="checkbox"/> eni-0c8985efe6873056d-all	2022-09-26 21:08:56 (UTC+09:00)

일정 시간이 흐르면 위와 같이 CloudWatch Log group에 스트림이 생성됩니다.

3. CloudWatch Logs Insights 활용

작업 ▼ **Logs Insights에서 보기** 로그 그룹 검색

구독 필터
0

기여자 인사이트 규칙
-

ARN
arn:aws:logs:ap-northeast-2:322683045347:log-group:/aws/vpc/flow-log*

로그 스트림 삭제 로그 스트림 생성 Search all log streams

1

▼ 마지막 이벤트 시간 ▼

2022-09-26 21:08:57 (UTC+09:00)

2022-09-26 21:08:56 (UTC+09:00)

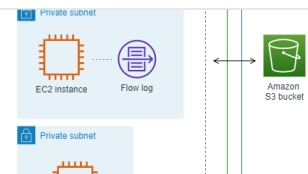
Logs Insights를 클릭합니다.

- VPC Flow logs 상세 정보

VPC 흐름 로그를 사용하여 IP 트래픽 로깅

VPC 흐름 로그는 VPC의 네트워크 인터페이스에서 전송되고 수신되는 IP 트래픽에 대한 정보를 수집할 수 있는 기능입니다. 플로우 로그 데이터는 Amazon CloudWatch Logs 또는 Amazon S3에 게시될 수 있습니다. 플로우 로그를 생성한 다음 선택된 대상의 데이터를 가져와 확인할 수 있습니다. 흐름 로그는 다음과 같은 여러 작업에 도움이 될 수

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/flow-logs.html#flow-log-records



- CloudWatch Insight 쿼리 구문

CloudWatch Logs Insights 쿼리 구문

CloudWatch Logs Insights에서는 로그 그룹을 쿼리하는 데 사용할 수 있는 쿼리 언어를 지원합니다. 쿼리 구문은 일반 함수, 산술 및 비교 연산, 정규 표현식을 포함하되 이에 국한되지 않는 다양한 함수 및 연산을 지원합니다. 여러 쿼리 명령이 포함된 쿼리를 생성할 수 있습니다. UNIX 스타일 파이프 문자(|)를 사용하여 쿼리에서 쿼리 명령을 구분합니다.

 https://docs.aws.amazon.com/ko_kr/AmazonCloudWatch/latest/logs/CWL_QuerySyntax.html

@message를 그대로 사용하면 검색이 어려울 수 있습니다. parse 문을 이용하여 @message의 컬럼을 분리하여 정규화 할 수 있습니다.

```
fields @timestamp
| parse @message "*" as account_id, action, az_id, bytes, dstaddr, dstport, end, fl
| sort @timestamp desc
| limit 20
```

Source와 Destination IP주소 쌍 네트워크의 트래픽을 요약할 수 있습니다.

```
fields @timestamp
| parse @message "*" as account_id, action, az_id, bytes, dstaddr, dstport, end, fl
| stats sum(bytes) as Data_Transferred by srcaddr, dstaddr, flow_direction
| sort by Data_Transferred desc
| limit 2
```

Instance ID별로 분리하여 데이터 통계를 얻을 수 있습니다

```
fields @timestamp
| parse @message "*" as account_id, action, az_id, bytes, dstaddr, dstport, end, fl
| stats sum(bytes) as Data_Transferred by instance_id
| sort by Data_Transferred desc
| limit 5
```

거부된 SSH접근 요청 내역을 요약하여 확인할 수 있습니다.

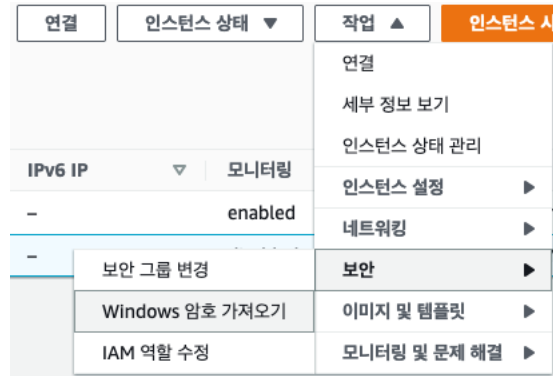
```
fields @timestamp
| parse @message "*" as account_id, action, az_id, bytes, dstaddr, dstport, end, fl
| filter action = "REJECT" and protocol = 6 and dstport = 22
| stats sum(bytes) as SSH_Traffic_Volume by srcaddr
| sort by SSH_Traffic_Volume desc
| limit 2
```

또는 모든 트래픽중 요청이 거부된 내역이 있는 IP를 찾을 수 있습니다.

```
fields @timestamp
| parse @message "*" as account_id, action, az_id, bytes, dstaddr, dstport, end, fl
| filter action="REJECT"
| stats count(action) as redjects by srcaddr
| sort redjects desc
```

4. Traffic Mirror Setting

사전에 생성한 EC2의 암호를 먼저 찾아야 합니다. EC2 Dashboard로 돌아가서 Windows Instance를 선택합니다.



작업 → 보안 → windows암호 가져오기를 클릭합니다. 클릭후에 초기 EC2 생성전 만들어둔 Key를 업로드 합니다.

Windows 암호 가져오기 정보

이 인스턴스에 대한 초기 Windows 관리자 암호를 검색하고 해독합니다.

암호 변경 권장

기본 암호를 변경하는 것이 좋습니다. 참고: 기본 암호를 변경한 경우 이 도구를 사용해 암호를 검색할 수 없습니다. 암호를 기억할 수 있는 새 암호로 변경해야 합니다.

다음 정보를 사용하여 원격 데스크톱을 사용해 Windows 인스턴스에 연결할 수 있습니다.

프라이빗 IP 주소

10.0.0.136

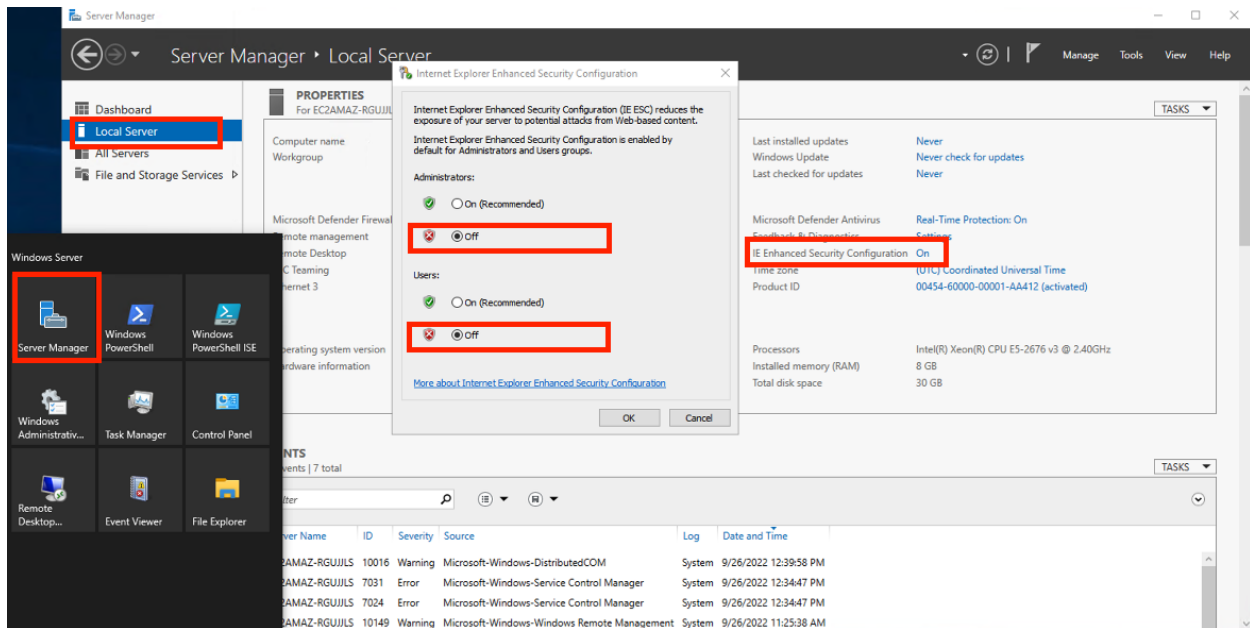
사용자 이름

Administrator

암호

닫기

위와같이 접속 정보를 알 수 있습니다. Mac이라면 Microsoft Remote Desktop을 사용하여 접속합니다.



작업의 편의를 위하여 Internet Explorer Enhanced Security Configuration을 전부 Off시켜줍니다

다음은 Wireshark를 Download및 설치합니다.

1. <https://www.wireshark.org/#download>
2. Windows Installer 64-bit를 전부 Default로 설치합니다.

정상적으로 설치가 되었으면 Wireshark를 실행했을때 Ethernet이 보입니다.

트래픽 미러 대상 생성

대상 설정

트래픽 미러 대상을 파악하는 데 도움이 되는 설명

이름 태그 - 선택 사항

트래픽 미러 대상 이름 지정

설명 - 선택 사항

트래픽 미러 대상 설명

대상 선택

생성 후 대상 유형을 수정할 수 없습니다.

대상 유형

네트워크 인터페이스

대상

Q 대상 선택



태그 - 선택 사항

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

이 리소스에 연결된 태그가 없습니다.

새 태그 추가

50줄(줄) 태그가 더 추가할 수 있습니다.

취소

생성

VPC Console로 돌아가 Mirror Target을 생성합니다. Target은 Network Interface로 선택후 Windows Instance의 eni를 선택합니다.

트래픽 미러 필터 생성

필터 설정
설명 및 활성화된 네트워크 서비스 설정

이름 태그 - 선택 사항
트래픽 미러 필터 이름 지정

설명 - 선택 사항
트래픽 미러 필터 설명

네트워크 서비스 - 선택 사항
☐ amazon-dns

인바운드 규칙 - 선택 사항 Sort rules

번호	규칙 작업	프로토콜	소스 포트 범위 - 선택 사항	대상 포트 범위 - 선택 사항	소스 CIDR 블록	대상 CIDR 블록	설명
100	accept	모든 프로토콜	해당 사항 없음	해당 사항 없음	0.0.0.0/0	0.0.0.0/0	

규칙 추가

아웃바운드 규칙 - 선택 사항 Sort rules

번호	규칙 작업	프로토콜	소스 포트 범위 - 선택 사항	대상 포트 범위 - 선택 사항	소스 CIDR 블록	대상 CIDR 블록	설명
100	accept	모든 프로토콜	해당 사항 없음	해당 사항 없음	0.0.0.0/0	0.0.0.0/0	

규칙 추가

태그 - 선택 사항
태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

이 리소스에 연결된 태그가 없습니다.

새 태그 추가

50용(個) 태그개 더 추가할 수 있습니다.

취소 생성

다음은 Mirror Filter를 생성합니다.

1. Inbound Rule
 - a. 100/ accpet / all protocols / 0.0.0.0/0 / 0.0.0.0/0
2. outbound Rule
 - a. 100/ accpet / all protocols / 0.0.0.0/0 / 0.0.0.0/0

트래픽 미리 세션 생성

세션 설정

설명, 소스 및 대상을 설정합니다.

이름 태그 - 선택 사항

mirror-session

설명 - 선택 사항

트래픽 미리 세션 설명

미러 소스

요리링하려는 리소스입니다.

eni-0225cd534daa4a477

인터페이스 유형의 네트워크 인터페이스만 허용됩니다.

미러 대상

미러링할 트래픽의 대상인 네트워크 인터페이스, Network Load Balancer 또는 게이트웨이 로드 밸런서 엔드포인트입니다.

tmt-0839114cd3d118aae7

대상 생성

추가 설정

우선순위, 패킷 길이 등을 설정합니다.

세션 번호

동일한 리소스에 대한 주를 세션이 평가됩니다.

1

1~32766의 숫자

VNI - 선택 사항

대상으로 전송하는 캡슐화되고 미러링된 패킷에 포함된 고유한 VXLAN 네트워크 식별자입니다.

12345

0~16777215의 숫자

패킷 길이 - 선택 사항

미러링할 각 패킷의 바이트 수입니다.

예: 255바이트 - 패킷 전체가 기본값입니다.

지정하지 않으면 패킷 전체가 미러링됩니다.

필터

미러링되는 트래픽을 결정합니다.

tmf-05fd90b84e9eac33e

필터 생성

다음은 Mirror Session을 생성합니다.

1. Mirror Source : 패킷 수집이 필요한 eni입니다.
2. Mirror Target : 패킷을 수집하여 트래킹할 Target입니다. 사전에 설정한 Target을 지정합니다
3. Session Number: 1 로 기입합니다.
4. VNI : 12345로 기입합니다. 읍서널한 값이지만 구분의 용이를 위하여 설정합니다
5. Filter : 기존에 설정한 Filter를 지정합니다.

Wireshark 3.0.0 (x86_64)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

12345

No.	Time	Source	Destination	Protocol	Length	Info
21799	772.068816	10.0.0.177	54.239.119.4	TCP	124	80 → 21517 [SYN, ACK, ECN] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=3911541556 TSecr=3506626712 WS=256
21790	772.025363	54.239.119.4	10.0.0.177	TCP	116	21517 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=3506626752 TSecr=3911541556
21791	772.025479	54.239.119.4	10.0.0.177	HTTP	613	GET / HTTP/1.1
21792	772.025479	10.0.0.177	54.239.119.4	TCP	116	80 → 21517 [ACK] Seq=1 Ack=808 Win=28160 Len=0 TSval=3911541595 TSecr=3506626752
21793	772.025692	10.0.0.177	10.0.10.131	TCP	124	80 → 39652 [SYN] Seq=0 Win=26883 Len=0 MSS=8961 SACK_PERM=1 TSval=3752382032 TSecr=0 WS=256
21794	772.026542	10.0.10.131	10.0.0.177	TCP	124	80 → 39652 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=2149899158 TSecr=3752382032 WS=128
21795	772.026668	10.0.0.177	10.0.10.131	TCP	116	39652 → 80 [ACK] Seq=1 Ack=1 Win=27136 Len=0 TSval=3752382033 TSecr=2149899158
21796	772.026668	10.0.0.177	10.0.10.131	HTTP	726	GET / HTTP/1.1
21797	772.027397	10.0.10.131	10.0.0.177	TCP	116	80 → 39652 [ACK] Seq=1 Ack=611 Win=28160 Len=0 TSval=2149899159 TSecr=3752382033
21798	772.027620	10.0.10.131	10.0.0.177	HTTP	622	HTTP/1.1. 200 OK (text/html)
21799	772.027747	10.0.0.177	10.0.10.131	TCP	116	39652 → 80 [ACK] Seq=611 Ack=507 Win=28160 Len=0 TSval=3752382034 TSecr=2149899159
21800	772.027747	10.0.10.131	10.0.0.177	TCP	116	80 → 39652 [FIN, ACK] Seq=507 Ack=611 Win=28160 Len=0 TSval=2149899159 TSecr=3752382033
21801	772.027747	10.0.0.177	54.239.119.4	HTTP	627	HTTP/1.1. 200 OK (text/html)
21802	772.027747	10.0.0.177	10.0.10.131	TCP	116	39652 → 80 [FIN, ACK] Seq=611 Ack=507 Win=28160 Len=0 TSval=3752382034 TSecr=2149899159
21803	772.028668	10.0.10.131	10.0.0.177	TCP	116	80 → 39652 [ACK] Seq=508 Ack=612 Win=28160 Len=0 TSval=2149899160 TSecr=3752382034
21804	772.069962	54.239.119.4	10.0.0.177	TCP	116	21517 → 80 [ACK] Seq=808 Ack=512 Win=131584 Len=0 TSval=3506626793 TSecr=3911541598
21811	772.078030	54.239.119.4	10.0.0.177	HTTP	610	GET /favicon.ico HTTP/1.1
21812	772.079808	10.0.0.177	10.0.10.131	TCP	124	39664 → 80 [SYN] Seq=0 Win=26883 Len=0 MSS=8961 SACK_PERM=1 TSval=3752382485 TSecr=0 WS=256
21813	772.079971	10.0.10.131	10.0.0.177	TCP	124	80 → 39664 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=2149899611 TSecr=3752382485 WS=128
21814	772.080096	10.0.0.177	10.0.10.131	TCP	116	39664 → 80 [ACK] Seq=1 Ack=1 Win=27136 Len=0 TSval=3752382486 TSecr=2149899611
21815	772.080096	10.0.0.177	10.0.10.131	HTTP	723	GET /favicon.ico HTTP/1.1

설정이 완료되면 Wireshark의 서버에서 Mirror Session에서 설정한 vni로 filter하여 트래픽을 확인할 수 있습니다 (vxlan.vni==12345)

