AWS

- AWS 개요, on page 1
- 멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 AWS 계정을 연결합니다., on page 4

AWS 개요

멀티 클라우드 방어에서 AWS 계정을 멀티 클라우드 방어 컨트롤러에 연결할 때 사용하는 CloudFormation 템플릿을 만들었습니다.

멀티 클라우드 방어 컨트롤러과의 통합을 위한 클라우드 계정을 준비하려면 클라우드 계정에서 수행해야 하는 특정 단계가 있습니다. 다음은 AWS 클라우드 계정을 멀티 클라우드 방어 컨트롤러에 연결하기 전에 수행해야 하는 사전 요건 단계입니다. 이는 작업의 개요를 제공하기 위한 것이며 수동으로 수행할 수 없습니다. CloudFormation 섹션에 구축 세부 정보 및 매개변수 정보가 있습니다.

단계 개요

1. 멀티 클라우드 방어 컨트롤러에서 사용하는 교차 계정 IAM 역할을 생성하여 클라우드 계정을 관리합니다.
2. 계정에서 실행되는 멀티 클라우드 방어 게이트웨이 EC2 인스턴스에 할당될 IAM 역할을 생성합니다.
3. 관리 이벤트를 멀티 클라우드 방어 컨트롤러(으)로 전송하는 CloudWatch 이벤트 규칙을 생성합니다.
4. 관리 이벤트 전송을 수행할 권한을 제공하는 위의 CloudWatch 이벤트 규칙에서 사용하는 IAM 역할을 생성합니다.
5. 필요에 따라 계정에 S3 버킷을 생성하여 CloudTrail 이벤트, Route53 DNS 쿼리 로그 및 VPC 플로우 로그를 저장할 수 있습니다.
6. 대상을 위에서 생성한 S3 버킷으로 하여 Route53 DNS 쿼리 로깅을 활성화하고 쿼리 로깅을 활성화해야 하는 VPC를 선택합니다.
7. CloudTrail을 활성화하여 모든 관리 이벤트를 위에서 생성한 S3 버킷에 로깅합니다.

8. 위에서 생성한 대상이 S3 버킷인 VPC 플로우 로그를 활성화합니다.

VPC 설정

멀티 클라우드 방어 게이트웨이 인스턴스에는 가용성 영역당 2개의 보안 그룹과 2개의 서브넷이 필요합니다. 이는 애플리케이션과 동일한 VPC에 멀티 클라우드 방어 게이트웨이을(를) 구축하려는 경우에만 필요합니다.

VPC 리소스의 세부 정보

Subnets(서브넷)

멀티 클라우드 방어 구축에 필요한 2개의 서브넷은 *management* 및 *datapath*입니다. 게이트웨이 구축 중에 컨트롤러에서는 이러한 서브넷의 이름을 제공하도록 요청합니다. 각 가용성 영역에는 이러한 2개의 서브넷이 필요합니다.

관리 서브넷은 퍼블릭 서브넷이며 인터넷 게이트웨이에 대한 기본 경로가 있는 라우트 테이블과 연결되어야 합니다. 멀티 클라우드 방어 게이트웨이 인스턴스에는 컨트롤러와의 통신을 위해 이 서브넷에 연결된 네트워크 인터페이스가 있습니다. 이는 컨트롤러와 게이트웨이 간의 정책 가져오기 및 기타 관리 및 원격 측정 활동에 사용됩니다. 고객 애플리케이션 트래픽은 이 인터페이스/서브넷을 통과하지 않습니다. 인터페이스는 관리 보안 그룹과 연결됩니다(아래 섹션에서 설명).

데이터 경로 서브넷은 퍼블릭 서브넷이며, 인터넷 게이트웨이에 대한 기본 경로가 있는 라우트 테이블과 연결되어야 합니다. 멀티 클라우드 방어 컨트롤러은(는) 이 서브넷에 네트워크 로드 밸런서를 생성하고 게이트웨이 인스턴스에 이 서브넷에 연결된 네트워크 인터페이스가 있습니다. 고객 애플리케이션 트래픽은 이 인터페이스를 통해 흐릅니다. 멀티 클라우드 방어 게이트웨이 보안 정책은 이 인터페이스를 통해 인그레스하는 트래픽에 적용됩니다. 인터페이스는 *datapath(*데이터 경로*)* 보안 그룹과 연결됩니다(아래 섹션에서 설명).

보안 그룹

관리 및 데이터 경로 보안 그룹은 위에서 설명한 대로 게이트웨이 인스턴스의 인터페이스에 연결됩니다.

관리 보안 그룹은 게이트웨이 인스턴스가 컨트롤러와 통신할 수 있도록 아웃바운드 트래픽을 허용해야 합니다.

데이터 경로 보안 그룹은 데이터 경로 인터페이스에 연결되며 게이트웨이 인스턴스로의 트래픽을 허용합니다. 현재 이 보안 그룹은 컨트롤러에서 관리하지 않습니다. 이 인터페이스의 트래픽 이그레스를 허용하는 아웃바운드 규칙이 있어야 합니다. 멀티 클라우드 방어 보안 정책에서 구성하는 각 포트에 대해 인바운드 포트를 열어야 합니다. 예를 들어 포트 443에서 수신하도록 멀티 클라우드 방어 서비스를 구성하는 경우에는 데이터 경로 보안 그룹에서 포트 443을 열어야 합니다.

CloudFormation 템플릿

신규 또는 "녹색 필드" 구축의 경우 이 CloudFormation 템플릿을 실행합니다. 이 템플릿은 테스트 애플리케이션용 EC2를 생성할 수 있는 추가 옵션도 제공합니다. CFT에 사용되는 매개변수에 대한 설명은 아래의 세부 정보를 참조하십시오.

1. VPC

2. 인터넷 게이트웨이로 이동하여 VPC에 연결합니다.
3. 관리 서브넷 가용성 영역 1.
4. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 관리 서브넷 가용성 영역 1에 연결된 관리 경로 테이블 가용성 영역 1입니다.
5. 관리 서브넷 가용성 영역 2.
6. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 관리 서브넷 가용성 영역 2에 연결된 관리 경로 테이블 가용성 영역 2입니다.
7. 데이터 경로 서브넷 가용성 영역 1.
8. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 데이터 경로 서브넷 가용성 영역 1에 연결된 데이터 경로 라우트 테이블 가용성 영역 1입니다.
9. 데이터 경로 서브넷 가용성 영역 2.
10. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 데이터 경로 서브넷 가용성 영역 2에 연결된 데이터 경로 라우트 테이블 가용성 영역 2입니다.
11. 앱 서브넷 가용성 영역 1.
12. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 앱 서브넷 가용성 영역 1에 연결된 앱 라우트 테이블 가용성 영역 1입니다.
13. 앱 서브넷 가용성 영역 2.
14. 인터넷 게이트웨이에 대한 기본 경로를 사용하여 앱 서브넷 가용성 영역 2에 연결된 앱 라우트 테이블 가용성 영역 2입니다.
15. 아웃바운드 규칙이 있는 관리 보안 그룹을 통해 트래픽을 허용합니다.
16. 포트 80 및 443에 대한 트래픽 아웃 및 인바운드 규칙을 허용하는 아웃바운드 규칙이 포함된 데이터 경로 보안 그룹입니다.
17. 22, 80, 443, 8000 포트에 대한 트래픽 아웃 및 인바운드 규칙을 허용하는 아웃바운드 규칙이 있는 앱 보안 그룹입니다.
18. CentOS를 기반으로 하는 기본 멀티 클라우드 방어 이미지를 사용하여 앱 서브넷에 EC2 인스턴스를 생성합니다. 필요한 경우 고유한 AMI를 선택할 수 있습니다.

서브넷은 두 개의 가용성 영역에서 생성되므로 여러 가용성 영역에서 멀티 클라우드 방어 게이트웨이와 앱을 작동할 수 있습니다.

이 템플릿을 여러 번 실행하여 중앙 집중식 보안(허브) 구축 아키텍처를 위해 AWS Transit Gateway에 연결할 수 있는 여러 VPC를 생성할 수 있습니다.

CloudFormation 매개변수

1. **Stack Name(**스택 이름**)** - 스택의 이름을 제공합니다(예: 멀티 클라우드 방어-dp-resources).
2. **Prefix(**접두사**)** - 모든 리소스의 이름 태그에 적용할 접두사입니다(예: 멀티 클라우드 방어).

3. 멀티 클라우드 방어 리소스 생성 - 예/아니요. **Yes(**예**)**를 선택하면 mgmt/dp 서브넷, mgmt/dp 보안 그룹이 생성됩니다. **No(**아니요**)**를 선택하면 이러한 리소스가 생성되지 않습니다.
4. **Create Bastion Host(**배스티온 호스트 생성**)** - 앱 VM에 SSH를 사용하는 데 사용할 수 있는 배스티온 호스트(앱 VM은 이미 공인 IP를 가지고 있으며 인터넷 게이트웨이에 대한 경로를 가지고 있습니다. 나중에 이 경로를 삭제하면 VM을 비공개로 설정할 수 있습니다. 배스티온 호스트를 사용하여 이러한 VM에 SSH할 수 있습니다).
5. **VPC CIDR** - VPC의 CIDR.
6. **Subnet Mask Bits(**서브넷 마스크 비트**)** - 각 서브넷에 사용할 비트 수입니다. 이는 서브넷 마스크가 아닙니다. VPC CIDR에 /16이 있고 서브넷의 마스크 /24를 원하는 경우 비트에 8을 선택합니다. VPC CIDR 마스크에 여기에 있는 값을 더해 서브넷 마스크를 구성합니다.
7. 가용성 영역 **1** 및 영역 **2** - 가용성 영역을 선택합니다.
8. **AMI for App Instance(**앱 인스턴스용 **AMI)** - 멀티 클라우드 방어-기본 AMI는 us-east1, us-east2, us-west1 및 us-west2에서 사용할 수 있습니다. 도커가 포함된 CentOS 7 및 `Hello World` 애플리케이션 샘플입니다. 자체 AMI 또는 지역의 다른 AMI를 제공할 수 있습니다.
9. **Instance Type(**인스턴스 유형**)** - 옵션을 선택합니다. 선택 사항이 제한된 경우 CloudFormation 템플릿을 다운로드하고 편집하여 새 선택 사항을 추가할 수 있습니다.
10. **EC2 Key Pair(EC2** 키 쌍**)** - EC2 인스턴스에 연결할 SSH 키 쌍을 선택합니다.

멀티 클라우드 방어 대시보드에서 멀티 클라우드 방어 컨트롤러에 **AWS** 계정을 연결합니다.

멀티 클라우드 방어이(가) AWS 계정을 멀티 클라우드 방어 컨트롤러에 쉽게 연결할 수 있는 CloudFormation 템플릿을 생성했습니다.

Before you begin

시작하기 전에 CDO 테넌트에 대해 멀티 클라우드 방어 컨트롤러을(를) 요청해야 합니다.

Note 멀티 클라우드 방어 컨트롤러 버전 23.10은 멀티 클라우드 방어 게이트웨이 버전 23.04 이상을 사용하는 경우 AWS EC2 인스턴스에서 기본적으로 IMDSv2를 사용합니다. IMDSv1과 IMDSv2의 차이점에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **1** CDO 메뉴 바에서 멀티 클라우드 방어을(를) 클릭합니다.

단계 **2** 멀티 클라우드 방어 컨트롤러 버튼을 클릭합니다.

단계 **3** Cloud Accounts(클라우드 계정) 창에서 **Add Account(**계정 추가**)**를 클릭합니다.

단계 **4** **General Information(**일반 정보**)** 페이지에 있는 **Account Type(**계정 유형**)** 목록 상자에서 AWS를 선택합니다.

단계 **5** **Launch Stack(**스택 실행**)**을 클릭하여 CloudFormation 템플릿을 다운로드하고 구축합니다. 이렇게 하면 템플릿을 구축할 수 있는 다른 탭이 열립니다. AWS에 로그인해야 합니다.

단계 **6** AWS CloudFormation이 맞춤형 이름으로 IAM 리소스를 생성할 수 있음을 확인합니다.

단계 **7** 다음 값을 입력합니다.

- **AWS Account Number(AWS** 계정 번호**)**: 보호하려는 계정의 AWS 계정 번호를 입력합니다. 이 번호는 CloudFormation 템플릿의 출력 값 CurrentAccount에서 찾을 수 있습니다.
- **Account Name(**계정 이름**)**: 온보딩된 계정에 지정할 이름을 입력합니다.
- **Description(**설명**):**(선택 사항) 계정 설명을 입력합니다.
- **External ID(**외부 **ID)**: IAM 역할의 신뢰 정책에 대한 임의 문자열입니다. 이 값은 생성된 컨트롤러 IAM 역할에서 사용됩니다. 외부 ID를 편집하거나 다시 생성할 수 있습니다.
- **Controller IAM Role(**컨트롤러 **IAM** 역할**)**: 이 역할은 CFT(CloudFormation Template) 구축 중에 멀티 클라우드 방어 컨트롤러에 대해 생성되는 IAM 역할입니다. CFT 스택에서 출력 값 MCDControllerRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.
- **Inventory Monitor Role(**재고 목록 모니터 역할**)**: 이 역할은 CFT 구축 중에 멀티클라우드 방어 재고 목록에 대해 생성된 IAM 역할입니다. CFT 스택에서 출력 값 MCDInventoryRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

단계 **8** **Save and Continue(**저장 후 계속 진행**)**를 클릭합니다.
새 AWS 클라우드 계정이 기록되었음을 확인할 수 있는 멀티 클라우드 방어 대시보드로 돌아갑니다.

What to do next

트래픽 가시성을 활성화합니다.

CloudFormation 출력

Outputs(출력**)** 탭에서 다음 정보를 복사하고 텍스트 편집기에 붙여넣습니다.

- CurrentAccount(애플리케이션이 실행되고 멀티 클라우드 방어 게이트웨이이 구축될 AWS 계정 ID)
  - MCDControllerRoleArn
  - MCDGatewayRoleName
  - MCDInventoryRoleArn
  - MCDS3BucketArn
  - MCDBucketName

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 계정을 멀티 클라우드 방어 컨트롤러에 온보딩할 경우 서비스 간 통신이 보호되도록 클라우드 서비스 제공자의 매개변수 내에서 사용자 역할이 생성됩니다. 클라우드 서비스 제공자에 따라 서로 다른 역할 및 권한이 생성됩니다.

계정을 온보딩할 때 다음 역할이 생성됩니다.

AWS IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 IAM 역할에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 3개의 IAM 역할과 1개의 CloudWatch 이벤트 규칙을 생성합니다.

- 멀티 클라우드 방어**ControllerRole** - 멀티 클라우드 방어에서 AWS 클라우드 계정에 연결하는 데 사용합니다.
- 멀티 클라우드 방어**FirewallRole** - 클라우드 계정에서 실행 중인 멀티 클라우드 방어 인스턴스에서 S3, SecretsManager, KMS에 액세스하는 데 사용됩니다.
- 멀티 클라우드 방어**CloudWatchEventRole** - CloudWatch 이벤트 규칙에서 사용하여 인벤토리 변경 사항을 멀티 클라우드 방어(으)로 전송합니다.
- 멀티 클라우드 방어**CloudWatchEventRule** - 인벤토리 변경 사항을 멀티 클라우드 방어(으)로 전송하기 위해 CloudWatch 이벤트에서 생성하는 규칙입니다. 규칙에서는 위에서 정의한 멀티 클라우드 방어CloudWatchEventRole이 CloudWatch 이벤트를 전송할 수 있는 권한을 제공한다고 가정합니다.

MCDControllerRole

멀티 클라우드 방어이(가) 클라우드 계정에 액세스하여 EC2 인스턴스 생성, 로드 밸런서 생성, Route53 항목 변경 등의 필요한 작업을 수행할 수 있는 교차 계정 IAM 역할입니다. 서비스 보안 주체는 외부 ID가 적용된 멀티 클라우드 방어-controller-account입니다. 역할에 적용되는 IAM 정책은 다음과 같습니다(예: 이 예에서 사용된 컨트롤러 역할 이름은 멀티 클라우드 방어-***controller-role***).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aacm:ListCertificates",
        "apigateway:GET",
        "ec2:*",
        "elasticloadbalancing:*",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "globalaccelerator:*",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
```

```
        "logs:*",
        "route53resolver:*",
        "servicequotas:GetServiceQuota",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::<valtix-account>:role/valtix-controller-role"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<S3Bucket>/*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::<customer- account>:role/valtix_firewall_role"
    },
    {
      "Action": "iam:CreateServiceLinkedRole",
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

서비스 보안 주체:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<valtix-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "valtix-external-id"
        }
      }
    }
  ]
}
```

MCDGatewayRole

멀티 클라우드 방어 게이트웨이 (방화벽) EC2 인스턴스에 할당된 역할입니다. 역할은 게이트웨이 인스턴스에 애플리케이션의 개인 키가 저장되어 있는 secretsmanager에 액세스하는 기능, 키가 KMS에 저장된 경우 AWS KMS를 사용하여 키를 암호 해독하는 기능, 그리고 PCAP 같은 개체와 기술 지원 데이터를 S3 버킷에 저장하는 기능을 제공합니다. 이 역할의 서비스 보안 주체는 ec2.amazonaws.com입니다. 역할에 적용되는 IAM 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*/*"
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Tip CloudFormation 템플릿을 다운로드하고 편집하여 특정 키를 사용하도록 암호 해독을 제한하거나 PutObject를 정의된/특정 S3 버킷으로 제한하는 등 정책을 더 제한적으로 만들 수 있습니다.

MCDInventoryRole

이는 동적 인벤토리용으로 사용되며 컨트롤러의 AWS 계정으로 CloudTrail 이벤트를 전송할 수 있는 기능을 제공하는 역할입니다. 다음 작업을 수행합니다.

- 멀티 클라우드 방어 컨트롤러이(가) 있는 AWS 계정의 이벤트 버스에 이벤트를 배치합니다.
- 규칙과 일치하는 이벤트를 고객의 AWS 계정에서 직접 멀티 클라우드 방어 컨트롤러의 webhook 서버로 전송합니다.

이 역할의 서비스 보안 주체는 **events.amazonaws.com**입니다. 역할에 적용되는 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Action": "events:PutEvents",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:events:*:<valtix-account>:event-bus/default"
      ]
    }
  ]
}
```

InventoryMonitorRule

멀티 클라우드 방어 컨트롤러가 실행되는 AWS 계정의 이벤트 버스에 복사할 EC2 및 API 게이트웨이에 대한 모든 CloudTrail 재고 목록 변경 사항을 저장하기 위해 MCDInventoryRole에 추가되는 규칙입니다. 규칙은 고객의 AWS 계정에서 발생하는 특정 이벤트 패턴과 일치해야 합니다. 일치가 발생하면 규칙이 일치하는 이벤트를 컨트롤러의 webhook 서버(API 기반 대상)로 전송하도록 규정합니다. 이 규칙은 이전 섹션에서 생성된 멀티 클라우드 방어MCDInventoryRole을(를) 사용하여 실행됩니다.

사용자 지정 이벤트 패턴:

```
{
  "detail-type": [
    "AWS API Call via CloudTrail",
    "EC2 Instance State-change Notification"
  ],
  "source": [
    "aws.ec2",
    "aws.elasticloadbalancing",
    "aws.apigateway"
  ]
}
```

대상:

```
Event Bus in another AWS Account (mcd-account) using the MCDInventoryRole
```

재고 목록 및 검색 기능

재고 목록 및 검색 기능(멀티 클라우드 방어에서 활성화 권장)을 활성화하면 클라우드 리소스(예: 보안 그룹, 라우팅 테이블, 애플리케이션 등)에 대한 인사이트를 얻고 이러한 리소스가 규칙을 위반할 때 경고하는 규칙을 설정할 수 있습니다. 예를 들어 보안 그룹에 0.0.0.0/0(퍼블릭) 액세스에 대해 SSH(포트 22)에서 트래픽을 허용하는 인바운드 규칙이 있으면 규칙(멀티 클라우드 방어은(는) 사전 정의된 규칙 집합 제공)을 설정하여 알릴 수 있습니다.

또한 동적 검색 기능을 사용하면, 새로운 리소스가 생성되어 보안 정책에서 사용되는 경우 해당 리소스를 검색할 수 있습니다. 예를 들어 `Name = prod`로 태그가 지정된 EC2 인스턴스의 모든 이그레스 트래픽을 삭제하도록 방화벽 보안 정책을 설정할 수 있습니다. 위의 태그로 새 인스턴스가 생성되면 멀티 클라우드 방어 게이트웨이 인스턴스는 자동으로 이를 탐지하고 이그레스 트래픽을 삭제하는 보안 정책 규칙에 이 인스턴스를 추가합니다.

DNS 쿼리 로깅을 사용하면 VPC에서 이그레스되는 트래픽에 대한 통찰력을 얻을 수 있습니다. 멀티 클라우드 방어 컨트롤러은(는) BrightCloud URL 범주 데이터베이스를 사용하여 HTTP 트래픽을 분류합니다.

마지막으로 VPC 플로우 로그는 VPC로 들어오고 나가는 모든 트래픽에 대한 보고서를 제공합니다.

스택 생성 중에 S3 버킷을 제공하면 CloudFormation 템플릿은 위의 모든 기능을 활성화합니다.

1. S3 버킷을 생성합니다.
2. 대상을 위에서 생성한 S3 버킷으로 사용하여 Route53 쿼리 로깅을 활성화하고 트래픽 인사이트를 원하는 모든 VPC를 선택합니다.
3. CloudTrail을 생성하여 모든 관리 이벤트를 활성화합니다.