멀티 클라우드 방어에서 생성한 역할

역할 생성자: 멀티 클라우드 방어

제공된 스크립트를 사용하여 클라우드 서비스 어카운트를 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 어카운트에 연결하는 데 사용합니다.
- 멀티 클라우드 방어 **FirewallRole** - 클라우드 어카운트에서 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 방어 CloudWatchEventRole이 CloudWatch 이벤트를 전송할 수 있는 권한을 제공한다고 가정합니다.

MCDControllerRole

멀티 클라우드 방어이(가) 클라우드 어카운트에 액세스하여 EC2 인스턴스 생성, 로드 밸런서 생성, Route53 항목 변경 등의 필요한 작업을 수행할 수 있는 교차 어카운트 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"
        "wafv2:Get*"
        "wafv2:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::<ciscomcd-account>:role/ciscomcd-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/ciscomcd_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::<ciscomcd-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "ciscomcd-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:*:<ciscomcd-account>:event-bus/default"
      ]
    }
  ]
}
```

InventoryMonitorRule

멀티 클라우드 방어 컨트롤러가 실행되는 AWS 계정의 이벤트 버스에 복사할 EC2 및 API 게이트웨이에 대한 모든 CloudTrail 인벤토리 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 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
```

Azure IAM 역할

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

CloudFormation 템플릿은 다음 역할을 생성합니다.

- **Custom Role(**사용자 지정 역할**)** - 사용자 지정 역할은 인벤토리 목록 정보를 읽고 리소스(예: VM, 로드 밸런서 등)를 생성할 수 있는 애플리케이션 권한을 제공합니다. 사용자 지정 역할은 여러 방법으로 생성할 수 있습니다.

GCP IAM 역할

이 문서에서는 이전 섹션에서 사용된 CloudFormation 템플릿으로 생성된 서비스 어카운트에 대해 자세히 설명합니다.

CloudFormation 템플릿은 다음 계정을 생성합니다.

- **ciscomcd-controller service account** - 이 어카운트는 멀티 클라우드 방어 컨트롤러가 GCP 프로젝트에 액세스하여 게이트웨이에 대한 리소스(멀티 클라우드 방어 게이트웨이), 로드 밸런서를 생성하고 VPC, 서브넷, 보안 그룹 태그 등에 대한 정보를 읽는 데 사용됩니다.
- **ciscomcd-firewall** 서비스 어카운트 - 이 어카운트는 멀티 클라우드 방어 게이트웨이(컴퓨팅 VM 인스턴스)에 할당됩니다. 계정은 Secret Manager(TLS 암호 해독용 개인 키) 및 스토리지에 대한 액세스를 제공합니다. 또한 여러 게이트웨이에는 (사용자가 구성한 경우) 멀티 클라우드 방어 게이트웨이에서 GCP 로그를 전송하려면 로그 작성자 권한이 필요합니다.