AWS

AWS の概要

Multicloud Defense では、AWS アカウントを Multicloud Defense Controller に接続するときに使用する CloudFormation テンプレートが作成されました。

Multicloud Defense Controller と統合するためにクラウドアカウントを準備するには、特定の手順をクラウドアカウントで実行する必要があります。AWS クラウドアカウントを Multicloud Defense Controller に接続する前に実行する必要がある、前提条件の手順を以下に示します。これは動作の概要を示すことを目的としており、手動で実行することを目的としたものではありません。[CloudFormation] セクションには、展開の詳細情報とパラメータ情報があります。

手順の概要

1. Multicloud Defense Controller がクラウドアカウントを管理するために使用するクロスアカウント IAM ロールを作成します。
2. アカウントで実行される Multicloud Defense Gateway EC2 インスタンスに割り当てられる IAM ロールを作成します。
3. 管理イベントを Multicloud Defense Controller に転送する CloudWatch イベントルールを作成します。
4. 管理イベントの転送を行う権限を付与する、上記の CloudWatch イベントルールで使用される IAM ロールを作成します。
5. 必要に応じて、アカウントに S3 バケットを作成して、CloudTrail イベント、Route53 DNS クエリ、および VPC フローログを保存します。
6. 上記で作成した S3 バケットを接続先とする Route53 DNS クエリロギングを有効にし、クエリロギングを有効にする必要がある VPC を選択します。

7. 上記で作成した S3 バケットにすべての管理イベントを記録するには、CloudTrail を有効にします。
8. 上記で作成した S3 バケットを接続先とする VPC フローログを有効にします。

Multicloud Defense ダッシュボードから Multicloud Defense Controller への AWS アカウントの接続

Multicloud Defense では、AWS アカウントを Multicloud Defense Controller に簡単に接続できる CloudFormation テンプレートが作成されました。

始める前に

AWS アカウントを Multicloud Defense に接続する前に、次の要件を確認してください。

- 開始する前に、CDO テナントの Multicloud Defense Controller を要求しておく必要があります。
- AWS アカウントのクラウドストレージバケットの名前は、3 ー 65 文字である必要があります。バケット名が 65 文字を超えると、接続処理中にエラーが発生します。

（注） Multicloud Defense Gateway バージョン 23.04 以降を使用している場合、Multicloud Defense Controller バージョン23.10 は AWS EC2 インスタンスでデフォルトで IMDSv2 に設定されます。IMDSv1 と IMDSv2 の違いの詳細については、AWS のドキュメントを参照してください。

手順

ステップ 1 CDO の左側のペインで Multicloud Defense をクリックします。

ステップ 2 Multicloud Defense Controller をクリックします。

ステップ 3 [クラウドアカウント（Cloud Accounts）] ペインで、[アカウントの追加（Add Account）] をクリックします。

ステップ 4 [一般情報（General Information）] ページで、[アカウントタイプ（Account Type）] リストボックスから [AWS] を選択します。

ステップ 5 [スタックの起動（Launch Stack）] をクリックして、CloudFormation テンプレートをダウンロードして展開します。これにより、テンプレートを展開するための別のタブが開きます。AWS へのログインが必要です。

ステップ 6 AWS CloudFormation がカスタムの名前を持つ IAM リソースを作成することを認めます。

ステップ 7 次の値を入力します。

- [AWSアカウント番号（AWS Account Number）]：保護するアカウントの AWS アカウント番号を入力します。この番号は、CloudFormation テンプレートの [現在のアカウント（Current Account）] の出力値で確認できます。
- [アカウント名（Account Name）]：オンボーディング後にアカウントに付ける名前を入力します。
- [説明（Description）]：（任意）アカウントの説明を入力します。
- [外部ID（External ID）]：IAM ロールの信頼ポリシーのランダムな文字列。この値は、作成されたコントローラ IAM ロールで使用されます。外部 ID は編集または再生成できます。
- [コントローラIAMロール（Controller IAM Role）]：これは、CloudFormation テンプレート（CFT）の展開中に Multicloud Defense Controller に対して作成された IAM ロールです。CFT スタックで出力値 MCDControllerRoleArm を探します。次のような値となります： `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`。
- [インベントリモニターロール（Inventory Monitor Role）]：これは、CFT の展開時に Multicloud Defense Inventory 用に作成される IAM ロールです。CFT スタックで出力値 MCDInventoryRoleArn を探します。次のような値となります：`arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`。

ステップ 8 [保存して続行（Save and Continue）] をクリックします。
Multicloud Defense ダッシュボードに戻ると、新しい AWS クラウドアカウントが記録されていることがわかります。

次のタスク

トラフィックの可視性を有効化します。

CloudFormation の出力

[出力（Outputs）] タブから次の情報をコピーしてテキストエディタに貼り付けます。

- CurrentAccount（これは、アプリケーションが実行され、Multicloud Defense Gateway が展開される AWS アカウント ID です）
  - MCDControllerRoleArm
  - MCDGatewayRoleName
  - MCDInventoryRoleArn
  - MCDS3BucketArn
  - MCDBucketName

Multicloud Defense によって作成されるロール

提供されたスクリプトを使用してクラウドサービスアカウントを Multicloud Defense Controller にオンボーディングすると、サービス間の通信を確実に保護するために、クラウド サービス プロバイダーのパラメータ内でユーザーロールが作成されます。クラウド サービス プロバイダーに応じて、さまざまなロールと権限が作成されます。

アカウントをオンボーディングすると、次のロールが作成されます。

MCDControllerRole

Multicloud Defense がクラウドアカウントにアクセスし、必要なアクション（EC2 インスタンスの作成、ロードバランサの作成、Route53 エントリの変更など）を実行することを許可するクロスアカウントの IAM ロールです。サービスプリンシパルは、外部 ID が適用された Multicloud Defense-controller-account です。ロールに適用される IAM ポリシーは次のとおりです（たとえば、この例で使用されているコントローラロール名は **Multicloud Defense-controller-role** です）。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "acm:DescribeCertificate",
        "aacm:ListCertificates",
        "apigateway:Get",
        "ec2:*",
        "elasticloadbalancing:*",
        "events:*",
        "globalaccelerator:*"
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "logs:*",
        "route53resolver:*",
        "servicequotas:GetServiceQuota",
        "3: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/*"
    }
  ]
}
```

サービスプリンシパル：

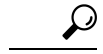
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<ciscomcd-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "ciscomcd-external-id"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

MCDGatewayRole

Multicloud Defense Gateway（ファイアウォール）EC2 インスタンスに割り当てられているロール。このロールは、ゲートウェイインスタンスに、アプリケーションの秘密キーが保存されているシークレットマネージャにアクセスする機能、キーが KMS に保存されている場合は AWS KMS を使用してキーを復号する機能、および PCAP やテクニカルサポートデータなどのオブジェクトを S3 バケットに保存する機能を付与します。このロールのサービスプリンシパルは ec2.amazonaws.com です。ロールに適用される IAM ポリシーは次のとおりです。

```
{
  "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": "*"
    }
  ]
}
```



ヒント CloudFormationテンプレートをダウンロードして編集し、ポリシーをより厳しく制限することができます。たとえば、特定のキーを使用するように復号を制限したり、定義済み/特定の S3 バケットへの PutObject を設定したりすることができます。

MCDInventoryRole

これは、ダイナミックインベントリの目的で使用されるロールであり、CloudTrail イベントをコントローラの AWS アカウントに転送する機能を提供します。次の処理を実行します。

- Multicloud Defense Controller が存在する AWS アカウントのイベントバス上にイベントを配置します。
- ルールに一致するイベントを、顧客の AWS アカウントから Multicloud Defense Controller のウェブフックサーバーに直接送信します。

このロールのサービスプリンシパルは **events.amazonaws.com** です。ロールに適用されるポリシーは次のとおりです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "events:PutEvents",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:events:*:<ciscomcd-account>:event-bus/default"
      ]
    }
  ]
}
```

InventoryMonitorRule

すべての CloudTrail インベントリの変更を EC2 および API ゲートウェイに配置し、Multicloud Defense Controller が実行されている AWS アカウントのイベントバスにコピーするために、

MCDInventoryRole に追加されるルールです。ルールは、顧客の AWS アカウントで発生する特定のイベントパターンと一致する必要があります。一致が発生すると、ルールは、一致したイベントをコントローラのウェブフックサーバー（API ベースの宛先）に送信する必要があることを示します。このルールは、前のセクションで作成した Multicloud Defense MCDInventoryRole を使用して実行されます。

カスタムイベントパターン：

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

Target:

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。