Multicloud Defense Terraform Providerの機能拡張

バージョン 0.2.9（2024 年 11 月 15 日）（推奨）

修正

このリリースには、次の修正が含まれています。

- `type = DYNAMIC_SECURITY_GROUP` のアドレスオブジェクト（`ciscomd_address_object`）リソースが作成されるが、サブオブジェクトが動的に入力されない問題を修正します。
- 現在の状態と比較して、ゲートウェイ（`ciscomd_gateway`）リソースのブロックの設定順序が変わった場合、変更が行われていなくても Terraform がこれをインフラストラクチャの変更と見なす問題を修正します。設定の順序はゲートウェイの動作には関係ありませんが、Terraform プランを実行するか、変更を適用する必要があるかどうかを検証するために適用する場合は関係します。この修正により、順序がユーザーによって変更されない限り、設定の順序は一貫して変わりません。

バージョン 0.2.8（2024 年 11 月 7 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- security_type 引数を **EGRESS** に設定してゲートウェイ（ciscomd_gateway）リソースの引数 aws_gateway_lb のデフォルト値を false から true に変更します。

修正

このリリースには、次の修正が含まれています。

- ポリシー規則セット（ciscomd_policy_rule_set）リソースの name 引数を変更しても、名前が変更されない問題を修正します。
- アドレスオブジェクト（ciscomd_address_object）リソースの name 引数を変更しても、名前が変更されない問題を修正します。
- ICMP ルールをポリシー規則（ciscomd_policy_rules）リソースに添付すると、機能準拠のエラーメッセージが表示される問題を修正します。
- ダイナミック IP アドレス値への参照を使用して設定された転送プロファイル（ciscomd_profile_log_forwarding）リソースで、IP アドレスの指定を求めるエラーがスローされる問題を修正します。
- BGP ネイバーブロックが指定されていないと BGP プロファイル（ciscomd_profile_bgp）を作成できない問題を修正します。
- サービス VPC（valtix_service_vpc）リソースの CIDR 引数が適切に検証されず、サービス VPC の作成時に適用されない CIDR を許可する問題を修正します。
- アドレスオブジェクト（ciscomd_address_object）リソースとポリシー規則（ciscomd_policy_rules）リソースの両方が同じ適用操作で作成され、規則がアドレスオブジェクトを参照すると、アドレスオブジェクト ID が **0** であるためにエラーがスローされる問題を修正します。アドレスオブジェクトの作成は ID を返さないため、規則に適用されるときの ID は 0 になります。これにより、アドレスオブジェクトと規則を同じ適用で作成および参照できるように、問題が修正されます。

バージョン 0.2.7（2024 年 8 月 21 日）

修正

このリリースには、次の修正が含まれています。

- エッジモードで展開されたゲートウェイ（ciscodmcd_gateway）リソースの instance_details ブロックの順序に関連する問題を修正します。マルチゾーン展開でのブロックの順序がランダムになる可能性があり、Terraform が適用してインフラストラクチャの変更が誤って検出されることになります。この修正により、コードで順序に変更がない場合、インフラストラクチャの変更が検出されないように、ユーザー指定の Terraform コードに基づいて一貫した順序が保証されます。

バージョン 0.2.6（2024 年 2 月 31 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- Windows、Linux、および MacOS の arm64 サポートを追加します。
- GCP での Multicloud Defense Gateway `ciscomcd_gateway` リソースの作成を強化し、ユーザーが提供する IP リソースをロードバランサのフロントエンド IP として使用できるようにします。
- Azure `ciscomcd_spoke_vpc` でのクロスサブスクリプション スポーク VNet ピアリング オーケストレーションのサポートを追加します。これにより、クラウドサービスプロバイダー間での機能の同等性が保証されます。
- OCI でのオーケストレーションのためのアカウント（テナント/コンパートメント）のオンボーディング `ciscomcd_account` および Multicloud Defense Gateway 展開 `ciscomcd_gateway` リソースのサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- FQDN フィルタリング `ciscomcd_profile_fqdn` リソースを作成しようとすると、「プロファイルタイプ FQDN_FILTER の復号プロファイルから不明なアクションが継承されます（unknown action Inherit from decryption profile for profile type FQDN_FILTER）」というエラーメッセージが表示される問題を修正します。
- 復号プロファイル `ciscomcd_profile_decryption` リソースへの変更が、変更を認識せず、「変更なし。インフラストラクチャは設定と一致しています。（No changes. Your infrastructure matches the configuration）」というメッセージが生じる問題を修正します。
- スポーク VPC ピアリングが削除されない、GCP でのスポーク VPC `ciscomcd_spoke_vpc` ピアリングの削除に関する問題を修正します。この問題は、セルフリンクの代わりに VPC ID が使用された場合にのみ発生していました。

バージョン 0.2.5（2023 年 11 月 6 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- フォルダ階層構造内に含まれるすべてのプロジェクトのアセットとトラフィックの検出に対応するために、GCP フォルダ階層のオンボーディングに対する、クラウド サービス プロバイダー アカウント `ciscomcd_cloud_account` リソースのサポートを追加します。GCP

フォルダのオンボーディングにより、アセットとトラフィックの検出は許可されますが、完全なオーケストレーションは許可されません。検出は、GCPプロジェクト内で行われた変更にリアルタイムで適応する動的ポリシーを作成するために有益であり、必要です。プロジェクト内でオーケストレーションを行うには、オーケストレーションが必要な各プロジェクトを個別にオンボーディングする必要があります。

- サードパーティ製SIEMへのMulticloud Defense Gatewayメトリックの送信のサポートを追加します。これにより、ゲートウェイメトリックをSIEMに送信するために、設定しMulticloud Defense Gateway `ciscomcd_gateway` リソースに割り当てることができる新しいメトリック転送プロファイル `ciscomcd_profile_metrics_forwarding` リソースが導入されます。最初の導入では、DatadogをSIEMとしてサポートします。他のSIEMのサポートは、今後のリリースで予定されています。
- Multicloud Defense Gateway `ciscomcd_gateway` リソース `aws_gateway_lb` 引数のデフォルト値をfalseからtrueに変更します。AWS出力ゲートウェイを展開する場合、サポートされるトランジットアーキテクチャはAWSゲートウェイロードバランサ（GWLB）アーキテクチャです。この引数はオプションであり、指定しない場合、デフォルトで適切な値になります。
- 監査ログとシステムログをSplunkに送信するためのサポートを追加します。これにより、type引数の新しい値としてSplunkを追加することで、アラートプロファイル `ciscomcd_alert_profile` リソースが更新されます。
- 監査ログとシステムログをMicrosoft Teamsに送信するためのサポートを追加します。これにより、type引数の新しい値としてMicrosoft Teamsを追加することで、アラートプロファイル `ciscomcd_alert_profile` リソースが更新されます。
- バックエンドTLSセッションをネゴシエートするときにサーバー証明書を検証するように転送プロキシポリシーを拡張します。証明書の検証はデフォルトでは無効になっていますが、すべてのTLSセッションの復号プロファイル `ciscomcd_profile_decryption` リソースで、およびドメイン（またはドメインのセット）ごとにFQDN一致オブジェクト `ciscomcd_profile_fqdn` リソースで設定できます。
- サービスVNet `ciscomcd_service_vpc` リソースの一部としてAzureリソースグループ（RG）を作成するためのサポートを追加します。RGは、Multicloud Defense Controllerによってオーケストレーションされるすべてのリソースを指定した（または新しく作成した）RG内で関連付けるために必要です。

修正

このリリースには、次の修正が含まれています。

- `transport_mode` 引数に割り当てられたセキュアプロキシ（TLS、HTTPS、WEBSOCKETS）値を使用するときに、復号プロファイル `ciscomcd_profile_decryption` をtls_profile引数に割り当てる必要がある転送プロキシ サービス オブジェクトまたはリバース プロキシ サービス オブジェクト `ciscomcd_service_object` リソースを設定するときに、検証が実行されなかった問題を修正します。セキュアなプロキシが設定されている場合は、復号プロファ

イルを割り当てる必要があります。割り当てなかった場合、プロキシはセキュアなプロキシとして動作せず、TLS 暗号化トラフィックは拒否されます。

バージョン 0.2.4（2023 年 8 月 22 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- L4（TCP）および L5（TLS）プロキシに対応するように転送プロキシ サービス オブジェクト `ciscomcd_service_object` リソースを拡張します。この拡張は、`transport_mode` 引数の有効な値として TCP または TLS を指定することにより達成されます。
- assign_public_ip 設定への変更が行われた場合に、青色/緑色ゲートウェイの置換を実行するように Multicloud Defense Gateway `ciscomcd_gateway` リソースを拡張します。

修正

このリリースには、次の修正が含まれています。

- policy 引数のない `mode=MATCH` 引数を持つ FQDN プロファイル `ciscomcd_fqdn_profile` リソースにより、一致するトラフィックが拒否される問題を修正します。policy 引数を指定する必要はなく、Terraform プロバイダーのドキュメントには引数としてリストされていません。
- ポリシー規則 `ciscomcd_policy_rule_set` リソースの更新に時間がかかり、RPC エラーが生成される可能性がある問題を修正します。

バージョン 0.2.4（2023 年 8 月 22 日）

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。