MCDでのセキュアなファイアウォール展開の分析

内容

概要

前提条件

　要件

　使用するコンポーネント

　関連製品

背景説明

導入のモニタリング

確認

トラブルシューティング

関連情報

概要

このドキュメントでは、使用可能なシステムログを使用してマルチクラウド防御の導入を監視し、導入が進行していることを検証する方法について説明します。

前提条件

これは、AWS、Azure、GCP、Oracleなどのクラウド環境で、Secure Cloud Connectorおよびクラウドで展開されたFirepower Management Center(cdFMC)へのシームレスな統合を可能にします

要件

次の項目に関する知識があることが推奨されます。

- マルチクラウド防御(MCD)導入ワークフロー
- クラウドネットワークとSecure Cloud Connector(SCC)接続の概念
- クラウド導入に関するFMCモニタリングおよび健全性検証

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- マルチクラウド防御
- AWS環境
- クラウドで導入されたFirepower Management Center(cdFMC)
- セキュアクラウドコネクタ(SCC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- マルチクラウド防御
- セキュアクラウドコネクタ(SCC)
- クラウドで導入されたFirepower Management Center(cdFMC)

背景説明

MCDを使用してクラウドプラットフォームにデバイスを導入する場合、導入が正しく進行していることを確認するために確認すべき箇所が複数あります。これらのツールは、展開の監視に役立ち、エラー発生時に追加のコンテキストを提供します。AWS、Azure、およびGCPのデプロイにも同じモニタリング原則が適用されます。

システムログは、MCDでの展開の可視性の主なソースです。これは、クラスタ作成イベント、ゲートウェイ作成アクティビティ、インスタンスの起動、および導入ワークフロー中に発生した例外を確認するのに最適な場所です。また、登録または導入の手順が失敗するとFMCがアラートを発行するため、調査対象エリアを絞り込むことができます。

ヒント：登録タイムアウトが発生した場合、環境自体をトラブルシューティングする前に、MCDシステムログを確認してください。失敗した手順は、ログで識別されることがよくあります。

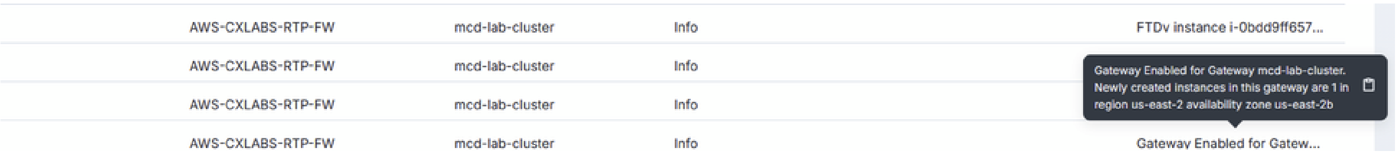
導入のモニタリング

MCDのシステムログを確認して、導入が予想される段階を通して進んでいることを確認します。これは、導入ステータス、ゲートウェイの作成、インスタンスの起動アクティビティ、および記録されたエラーを確認する最初の最も便利な場所です。

次のとおりに移動します。

マルチクラウド防御>調査>システムログ

この例は、ゲートウェイの作成が成功した場合と、クラスタインスタンスが起動される場合を示しています。この場合、ゲートウェイインスタンスはUS-east-2リージョンおよびus-east-2bアベイラビリティーゾーンでホストされます。

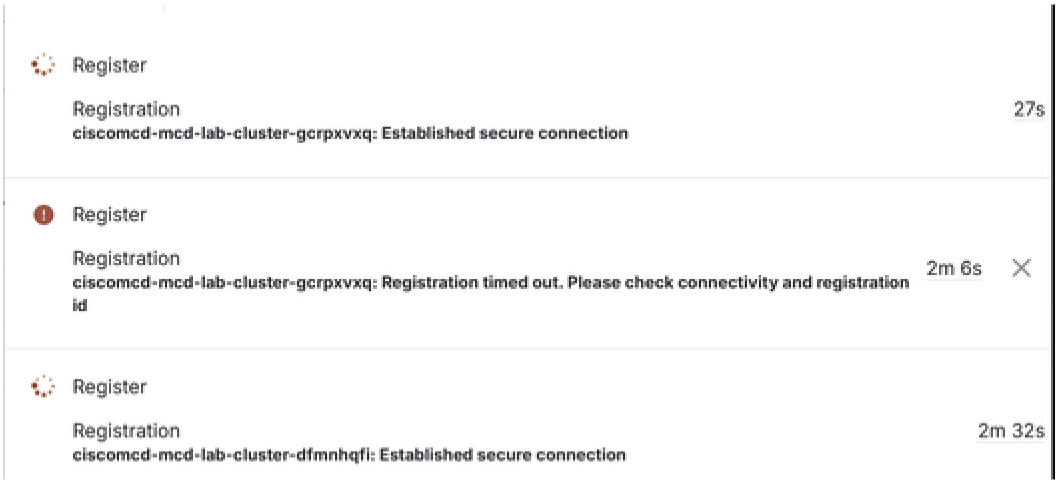


[システムログ]ページを使用して、展開が予期されたサイクルを通過していることを確認し、手順が失敗したときの詳細なエラーメッセージを収集します。

登録のタイムアウトまたは展開の失敗イベントが報告された場合は、FMCで展開エラーを確認します。FMCは、導入が正常に完了しなかったことを示す高レベルのアラートを提供できます。

推奨されるチェックは次のとおりです。

1. クラウドネットワークとSecure Cloud Connector(SCC)の間の接続を確認します。
2. 導入ガイドの各導入ステップが完了していることを確認します。
3. 正しいIAMロールが構成され、使用中であることを確認します。

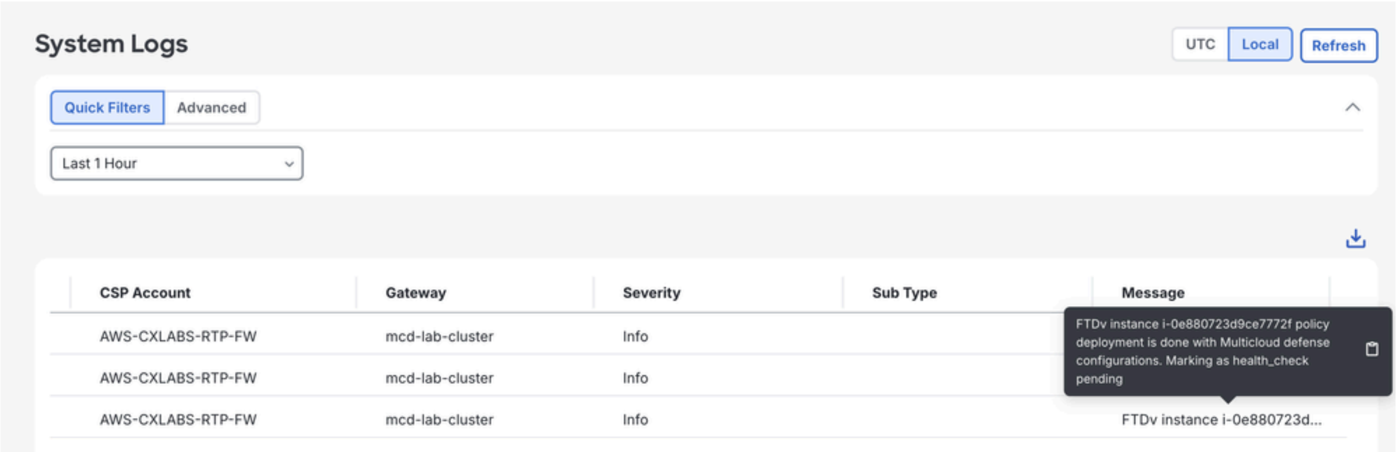


⚠

注意：登録が正常に完了する前に、登録の失敗が1回以上発生する可能性があります。この動作は、クラウドタイマーの動作が原因で発生する可能性があり、必ずしも永続的な問題ではありません。

SCCのFMCが登録タイムアウトを報告する場合、通常はシステムログに特定の障害に関するより詳細な情報が記録されます。ほとんどの場合、問題は接続、IAM、または設定の問題の組み合わせであり、失敗した手順を絞り込むための最適な情報源はログです。

MCDシステムログの最終成功イベントを確認して、導入が正常に完了したことを確認します。導入が成功すると、ログに正常に完了したことを示すイベントが表示されます。



正常に導入されたことをFMCで確認することもできます。このFMCでは、導入されたデバイスのステータスがconnectedと表示され、健全性インジケータが緑色で表示されます。

これにより、クラスタが正常に作成され、デバイスが予期された環境で動作していることを確認できます。

確認

AWSデプロイが正常であることを確認するために確認する場所がいくつかあります。

- システムログには、通常の導入アクティビティとブロッキングエラーがないことが示されます。
- デバイスまたはゲートウェイが、予想されるリージョンとアベイラビリティーゾーンに作成されます。
- FMCは、デバイスが接続済みで正常であると報告します。
- 登録のタイムアウトや導入の失敗に関する警告はログに残りません。

これらの条件がすべて満たされていれば、MCDの導入は成功したと見なすことができます。

トラブルシューティング

展開が正常な状態に達しない場合：

- MCDシステムログで、失敗した手順を確認します。
- FMCで登録アラートまたは接続アラートを確認します。
- クラウドネットワークとSecure Cloud Connectorの接続を確認します。
- IAMロールとすべての前提条件を導入ガイドで検証します。
- クラスターが予期される地域と可用性ゾーンに展開されていることを確認します。

関連情報

- Ciscoマルチクラウド防御アーキテクチャガイド
- Ciscoマルチクラウド防御ホワイトペーパー
- Cisco Multicloud Defenseユーザガイド：システムログ

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。