セキュアアクセスにおけるドバイDCの機能停止の修復手順

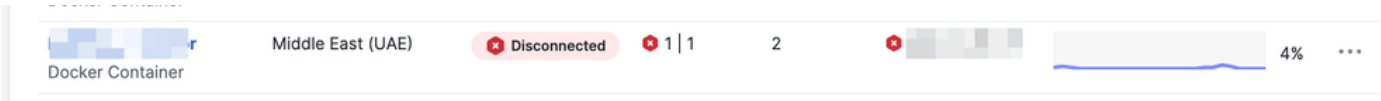
内容

はじめに

本書では、3月2日に発生したSecure Access Dubai DCインシデントの修復手順について説明します。
https://status.sse.cisco.com/incidents/7h28mb7mr5zl

リソースコネクタ

すでに展開されているリソースコネクタは、セキュアアクセスダッシュボードから切断されていることが表示されます。



配備されたリソースコネクタは、単一のセキュアアクセス領域にバインドされます。これは、構成変更によって変更することはできません。

この問題を修正するには、該当するお客様が次に示す手順に従う必要があります。

1. 新しいリソースコネクタを展開する

2. 新しい領域(ムンバイまたはハイデラバード)にコネクタグループを作成する

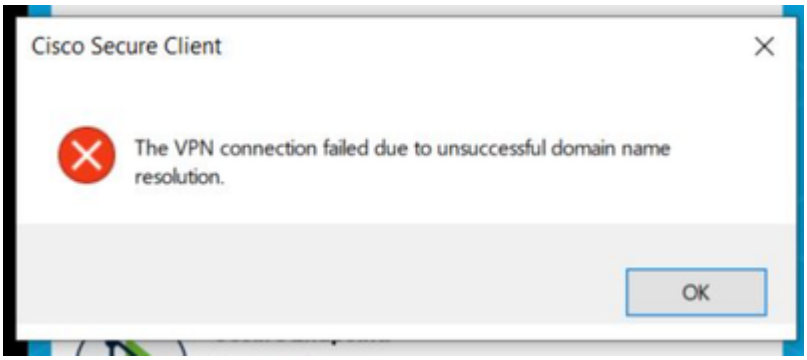
2. プライベートリソースを新しいコネクタグループに割り当てる

リソースコネクタの導入に関する詳細な手順については、『リソースコネクタ導入ガイド』を参照してください。

リモートアクセスVPNプロファイル

リモートアクセスVPNクライアントは、さまざまなエラーが発生すると接続の確立に失敗する可能性があります。

エラー例：



ドバイDCのリモートアクセスVPNプロファイルを持つ組織のみ：

次の手順に従ってください。
・ 移行ターゲットとして最も近い使用可能なデータ・センター（ムンバイまたはハイデラバード）を選択します。
・ 組織の現在のセッション負荷に合わせてVPN IPプールとプロファイルを設定し、既存のME-Central設定をミラーリングします。

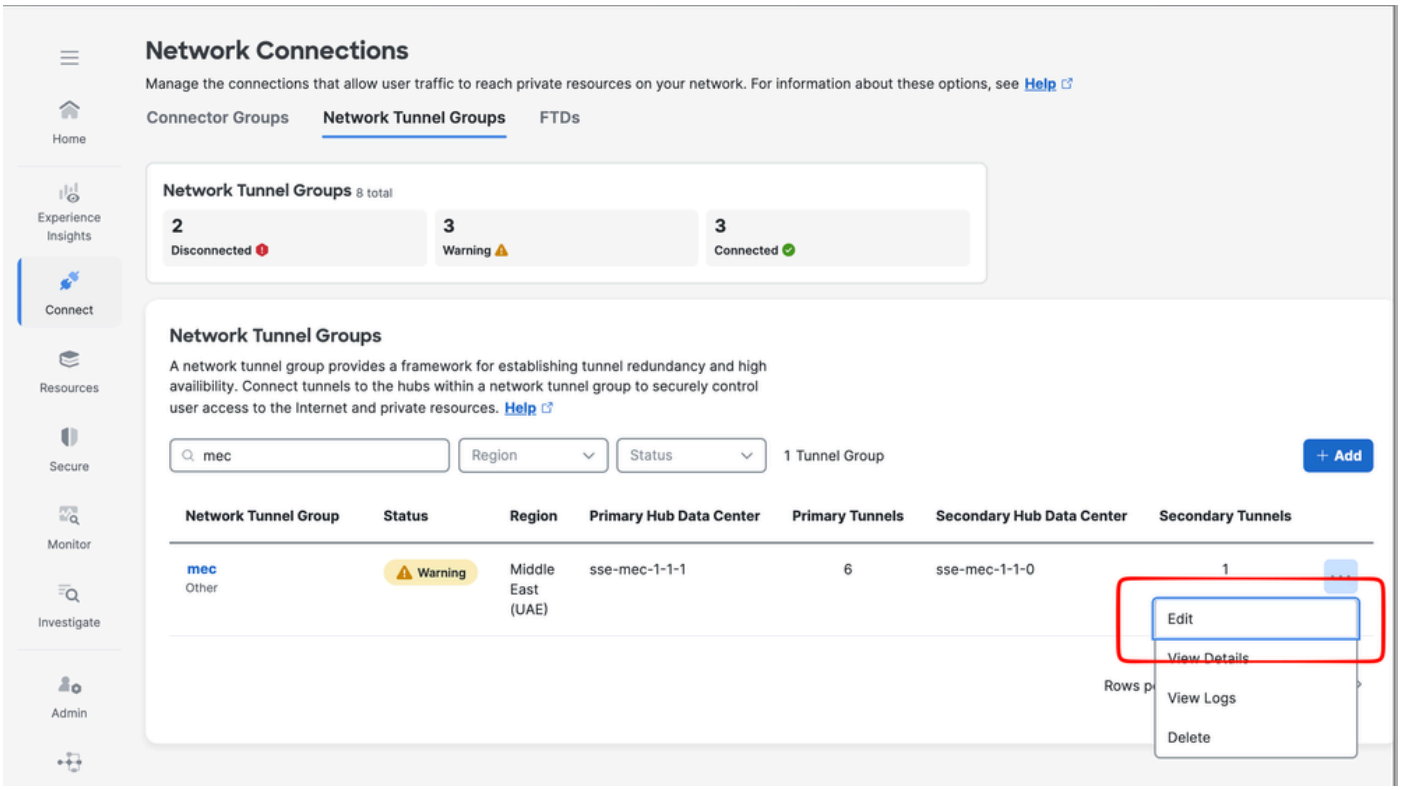
新しいVPNプロファイルの設定に関する詳細な手順については、『リモートアクセスVPN導入ガイド』に従ってください。

ネットワークトンネルグループ

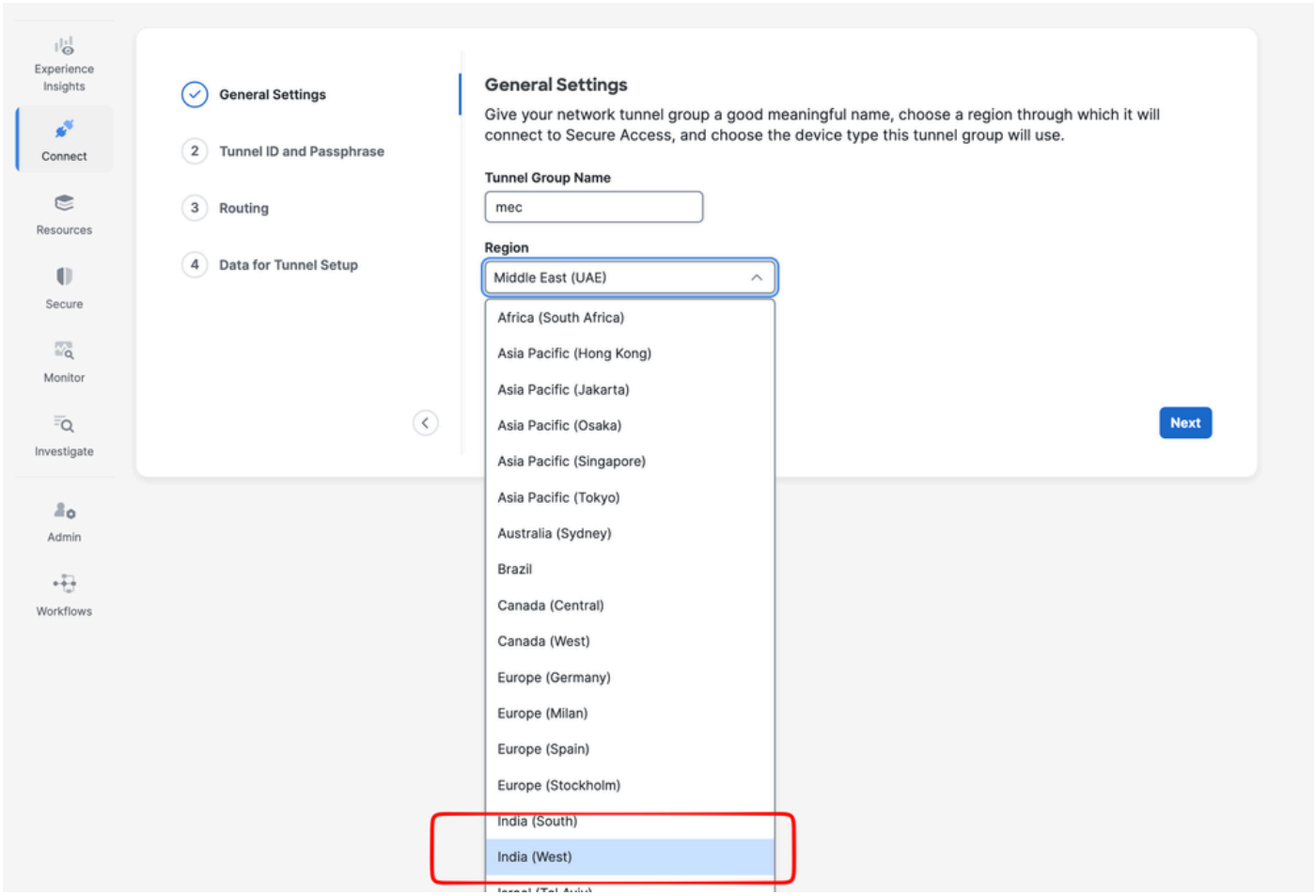
ネットワークトンネルグループ領域を変更するには、次の手順に従ってください:

・ 次の説明に従ってNTGオプションに移動します：

・ 中東(UAE)リージョンの既存のトンネルを編集します。

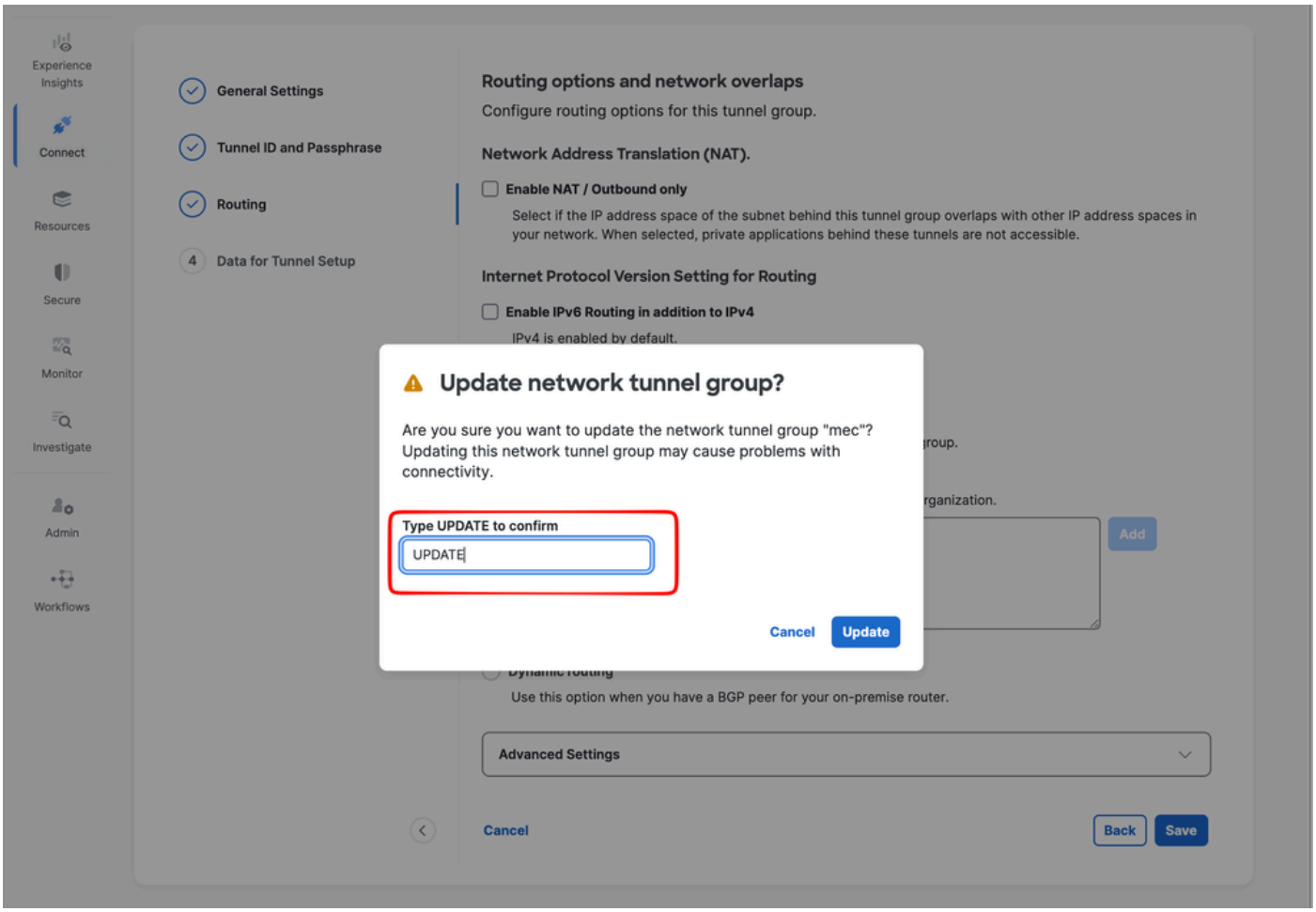


・ 地域を中東(UAE)からインド（西部）に変更します。

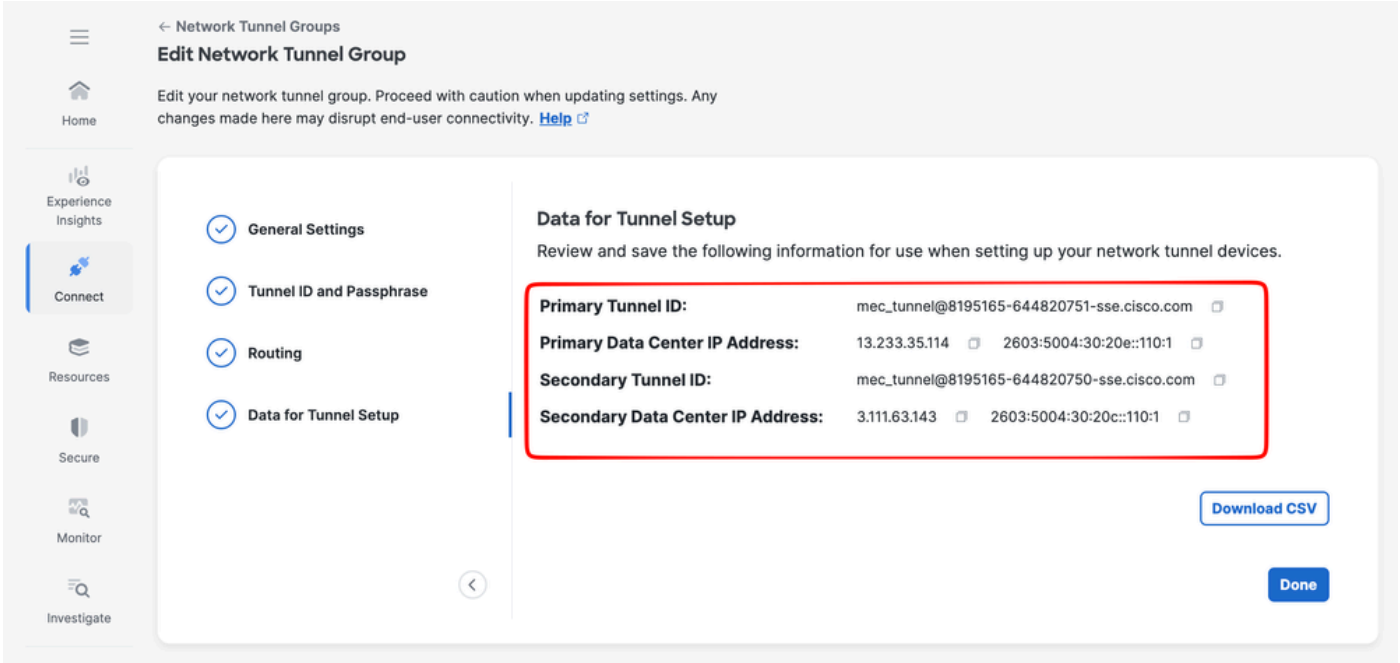


・ 他の設定は変更しないでください。設定を保存します。

・ プロンプトが表示されたら、「UPDATE」と入力して確認します。



・ 表示されている新しいインド（西）のIPアドレスを使用して、IPSEC CPEデバイスを更新します。



・ マルチリージョンバックホールまたはルートマップを使用している場合は、Cisco SSEからの新しい設定に従ってBGPコミュニティ値を更新します。

セキュアWebゲートウェイ

Roaming Security Moduleを使用するクライアントは、次に最も近くて使用可能なセキュアアクセスデータセンターに自動的に接続します。
現時点でお客様からのアクションは不要です。

ゼロトラストアクセスクライアント

ゼロトラストアクセスモジュールを使用するクライアントは、次に最も近くて利用可能なセキュアアクセスデータセンターに自動的に接続します。
現時点でお客様からのアクションは不要です。

関連情報

- ステータスCisco Secure Access

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。