Étapes de correction pour la panne du DC d'accès sécurisé à Dubaï

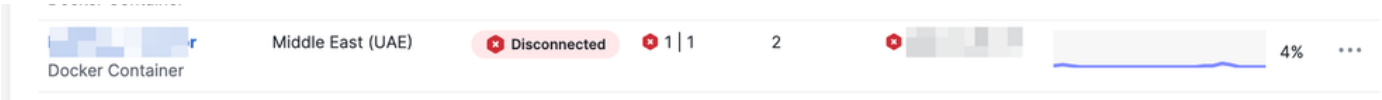
Table des matières

Introduction

Ce document contient les étapes de correction pour l'incident Secure Access Dubai DC du 2 mars. https://status.sse.cisco.com/incidents/7h28mb7mr5zl

Connecteurs de ressources

Les connecteurs de ressources déjà déployés s'affichent comme étant déconnectés du tableau de bord d'accès sécurisé :



Les connecteurs de ressources déployés sont liés à une seule région d'accès sécurisé, et cela ne peut pas être modifié par une modification de la configuration.

Afin de remédier au problème, les clients concernés doivent suivre les étapes décrites ci-dessous :

1. Déployez un nouveau connecteur de ressources

2. Créer des groupes de connecteurs dans une ou plusieurs nouvelles régions (Mumbai ou Hyderabad)

2. Affecter des ressources privées à de nouveaux groupes de connecteurs

Suivez le guide de déploiement de Resource Connector pour connaître les étapes détaillées de

déploiement de Resource Connector :

Profils VPN d'accès à distance

Les clients VPN d'accès à distance peuvent échouer à établir la connexion avec différentes erreurs.

Exemple d'erreur :

Pour les organisations disposant d'un profil VPN d'accès à distance à Dubaï DC uniquement :

Veuillez suivre les étapes suivantes :
· Sélectionnez le data center disponible le plus proche (Mumbai ou Hyderabad) comme cible de migration.
· Configurez les profils et les pools d'adresses IP VPN en fonction de la charge de session actuelle de votre entreprise, en fonction de votre configuration ME-Central existante.

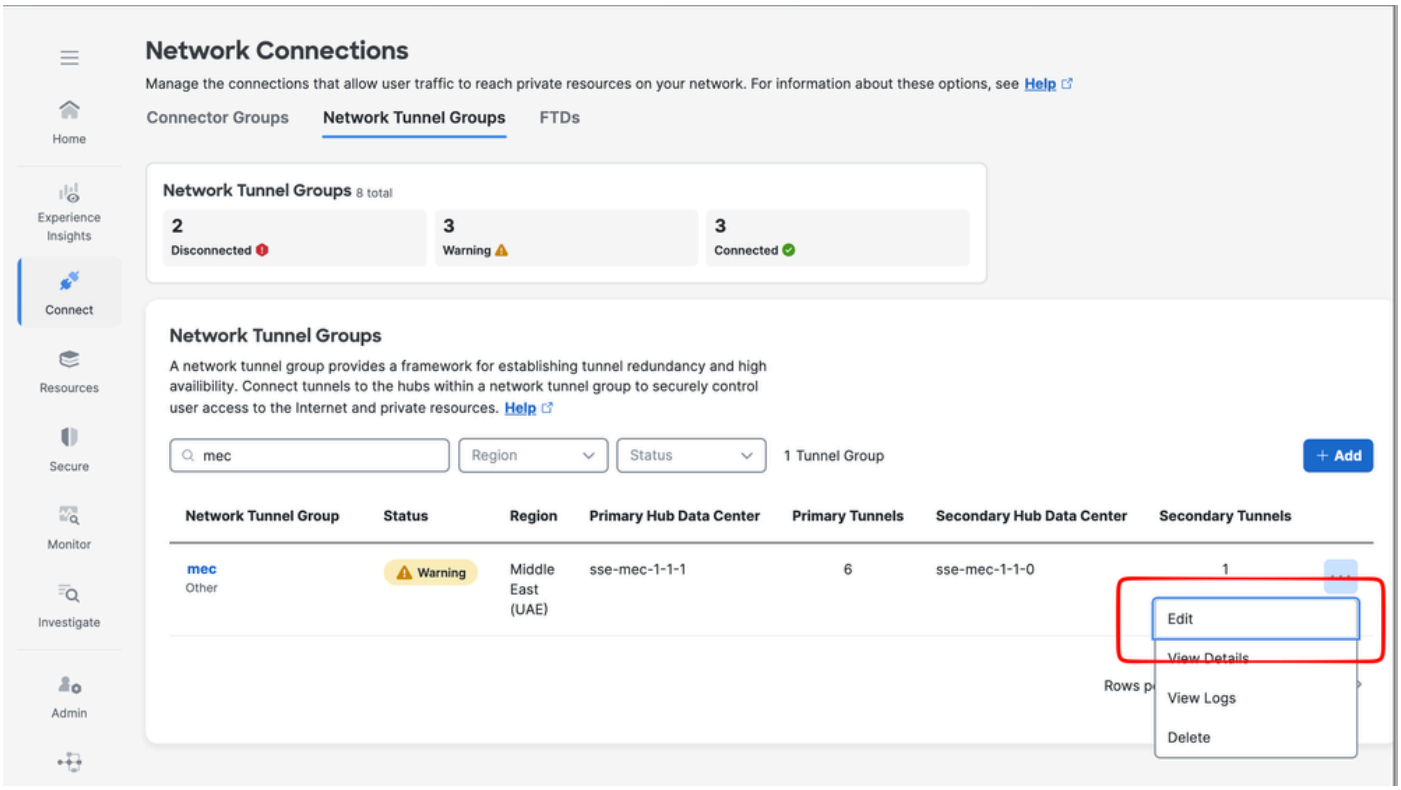
Suivez le guide de déploiement du VPN d'accès à distance pour connaître les étapes détaillées de configuration d'un nouveau profil VPN :

Groupes de tunnels réseau

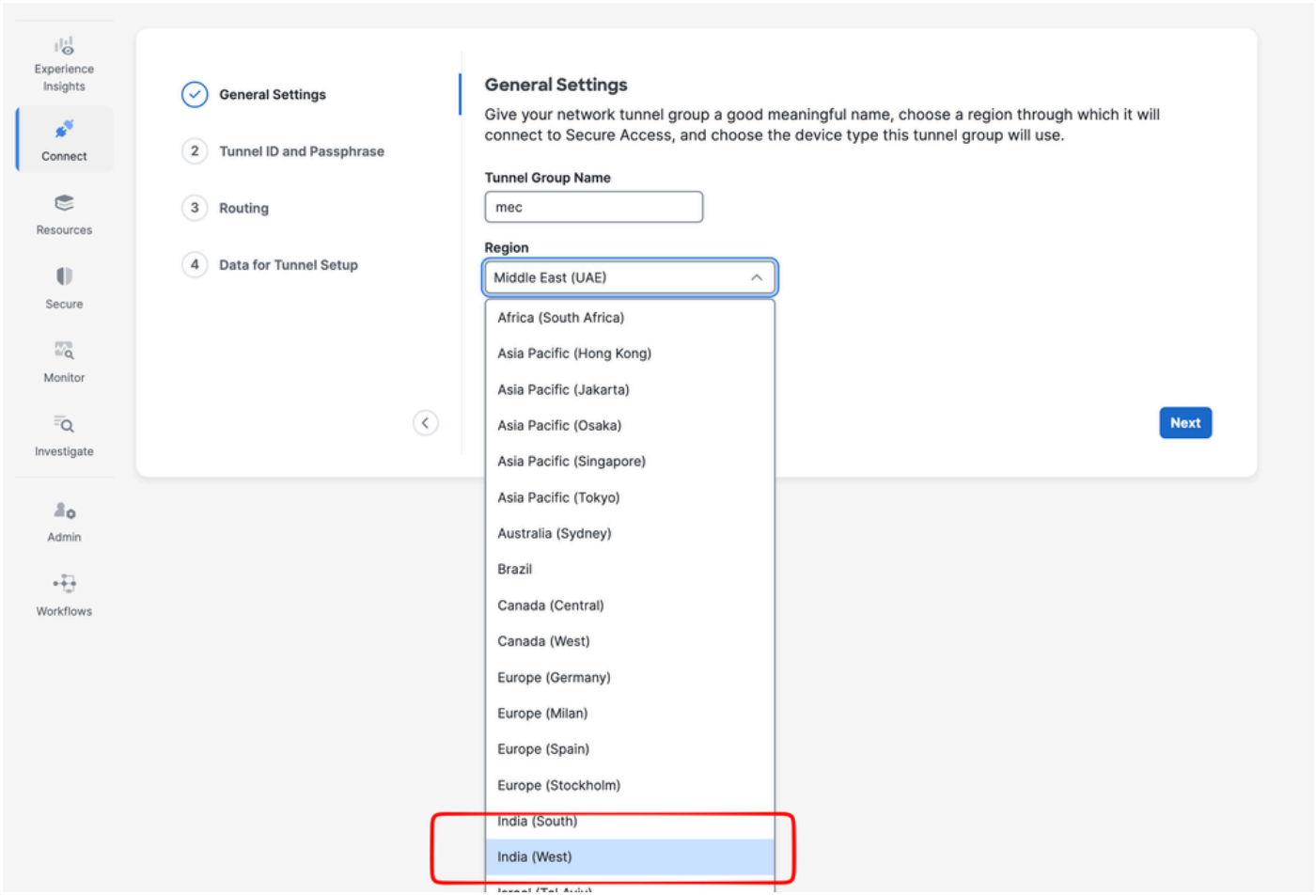
Suivez ces étapes pour modifier la région du groupe de tunnels réseau:

· Accédez aux options NTG comme décrit ici :

· Modifiez votre tunnel existant pour la région du Moyen-Orient (EAU).

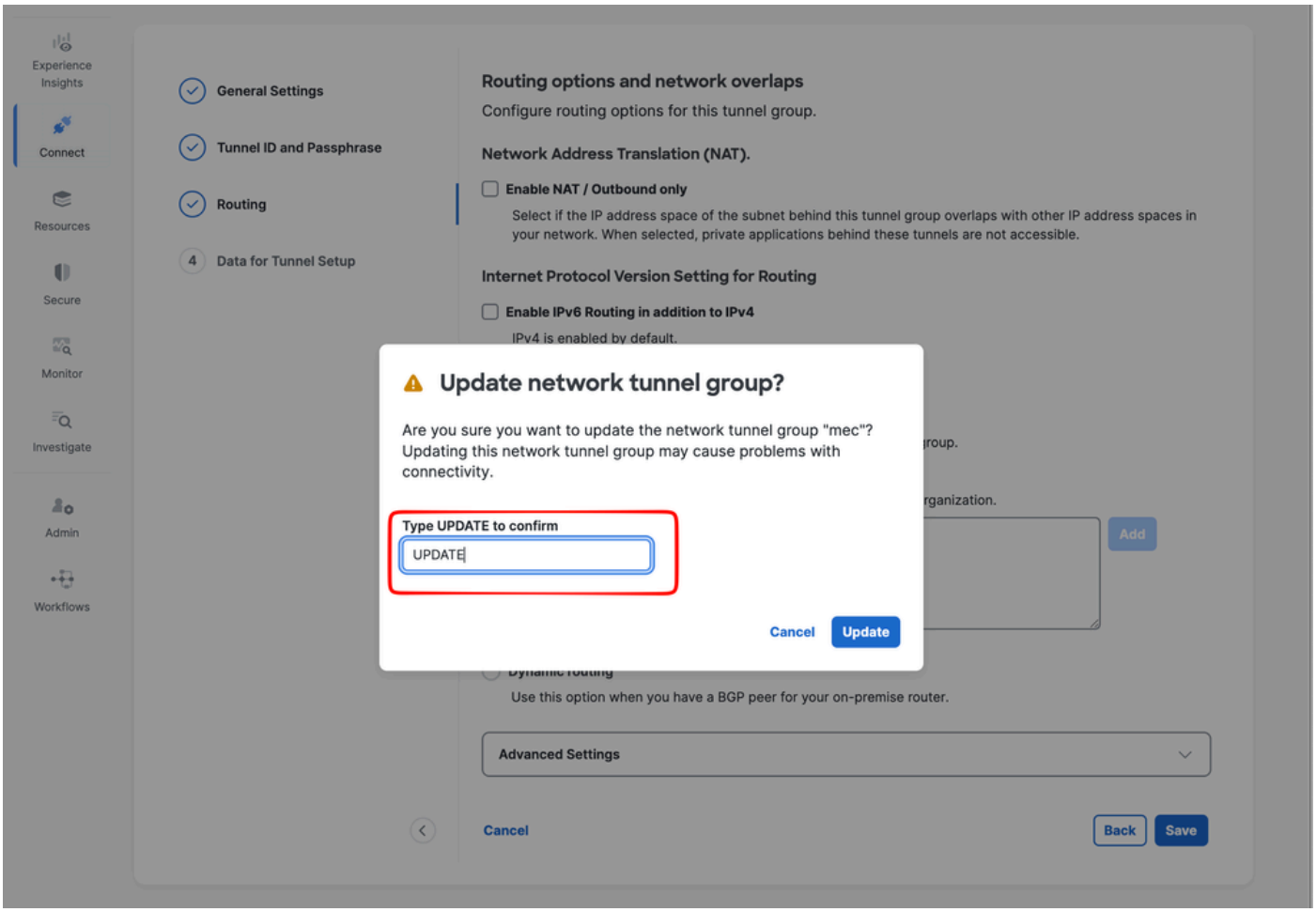


· Faire passer la région du Moyen-Orient (EAU) à l'Inde (Ouest).

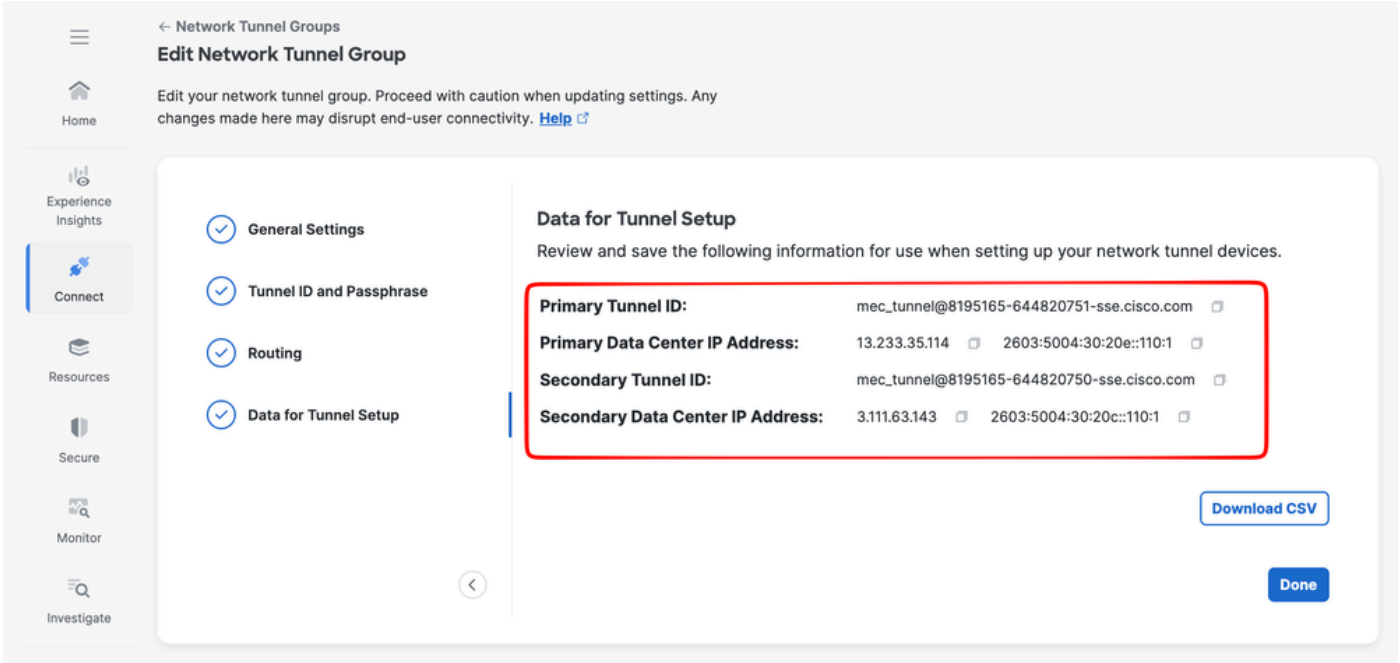


· Ne modifiez pas d'autres paramètres ; enregistrez la configuration.

· Lorsque vous y êtes invité, tapez « UPDATE » et confirmez.



· Utilisez les nouvelles adresses IP de l'Inde (Ouest) indiquées pour mettre à jour votre périphérique CPE IPSEC.



· Si une liaison multirégion ou des cartes de route sont utilisées, mettez à jour les valeurs de la communauté BGP en fonction des nouveaux paramètres de Cisco SSE.

Passerelle Web sécurisée

Les clients utilisant le module de sécurité d'itinérance se connecteront automatiquement au prochain data center à accès sécurisé disponible le plus proche.
Aucune action requise de la part des clients pour le moment.

Clients d'accès sans confiance

Les clients utilisant le module Zero Trust Access se connecteront automatiquement au prochain data center à accès sécurisé disponible le plus proche.
Aucune action requise de la part des clients pour le moment.

Informations connexes

- État de Cisco Secure Access

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.