Dépannage des alertes de défaillance 802.1X récentes sur le périphérique Meraki

Contenu

Introduction

Ce document décrit comment résoudre la récente alerte de défaillance 802.1X dans le périphérique Meraki.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comprendre la solution de base SDWAN (Wide Area Network) définie par logiciel Meraki
- Comprendre la stratégie d'accès de base et l'authentification Radius

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

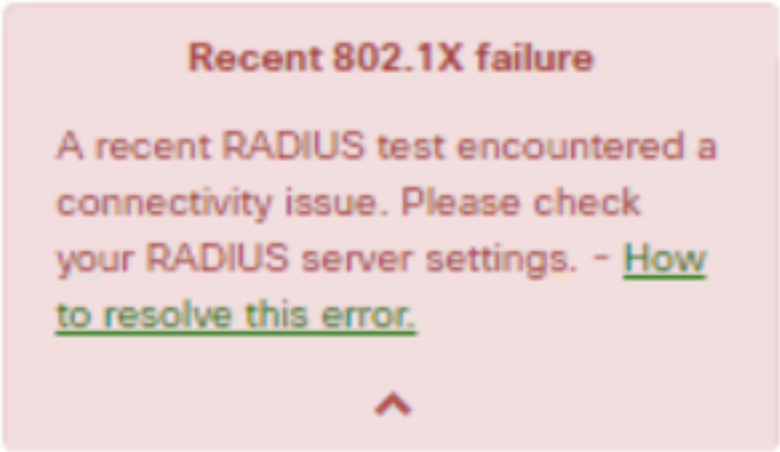
Problème

Les périphériques Meraki utilisent la configuration de la stratégie de serveur AAA radius pour authentifier l'utilisateur final.

Quel est le test RADIUS dans les appareils Meraki ?

L'alerte d'échec 802.1X récente indique que si les messages de demande d'accès périodiques envoyés aux serveurs RADIUS configurés sont inaccessibles, vous devez utiliser un délai d'expiration de 10 secondes.

Les périphériques Meraki envoient régulièrement des messages de demande d'accès aux serveurs RADIUS configurés qui utilisent l'identité **meraki_8021x_test** pour s'assurer que les serveurs RADIUS sont accessibles. Ces demandes d'accès ont un délai d'attente de 10 secondes et si le serveur RADIUS ne répond pas, il considère que les serveurs RADIUS sont inaccessibles et invite le message d'alerte « Récent échec 802.1X ». Reportez-vous à la capture d'écran de l'alerte affichée sur le périphérique :



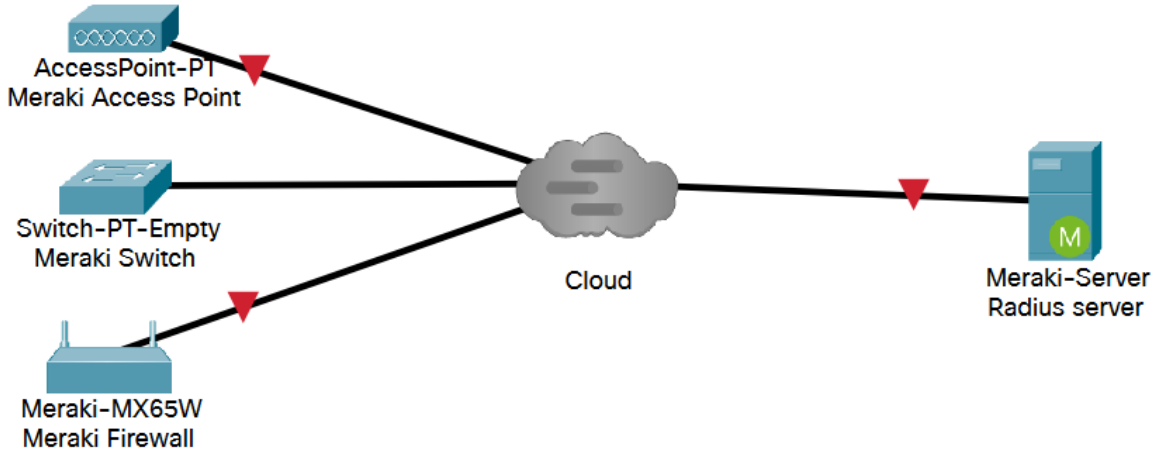
Un test est considéré comme réussi si le périphérique Meraki reçoit une réponse RADIUS légitime (Access-Accept/Reject/Challenge) du serveur.

Lorsque le test RADIUS est activé, tous les serveurs RADIUS sont maintenus en série sur chaque noeud au moins une fois par 24 heures, quel que soit le résultat du test. Si un test RADIUS échoue pour un noeud donné, il teste à nouveau toutes les heures jusqu'à ce qu'un résultat qui passe se produise. Une passe ultérieure marque le serveur accessible, efface l'alerte et revient au cycle de test de 24 heures.

Configuration

Diagramme du réseau

Voici un schéma de topologie simple qui décrit la configuration :



Vérifiez et dépannez

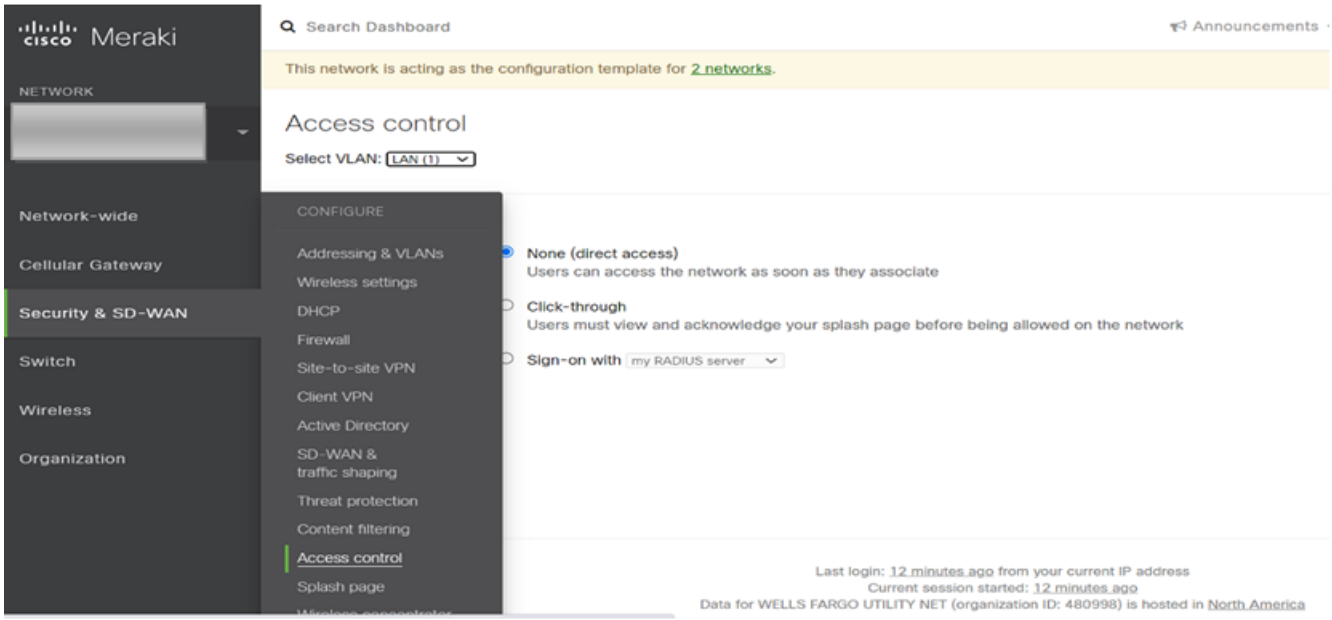
Configuration 802.1X

La configuration RADIUS 802.1X se trouve dans le chemin indiqué qui dépend du modèle de produit Meraki.

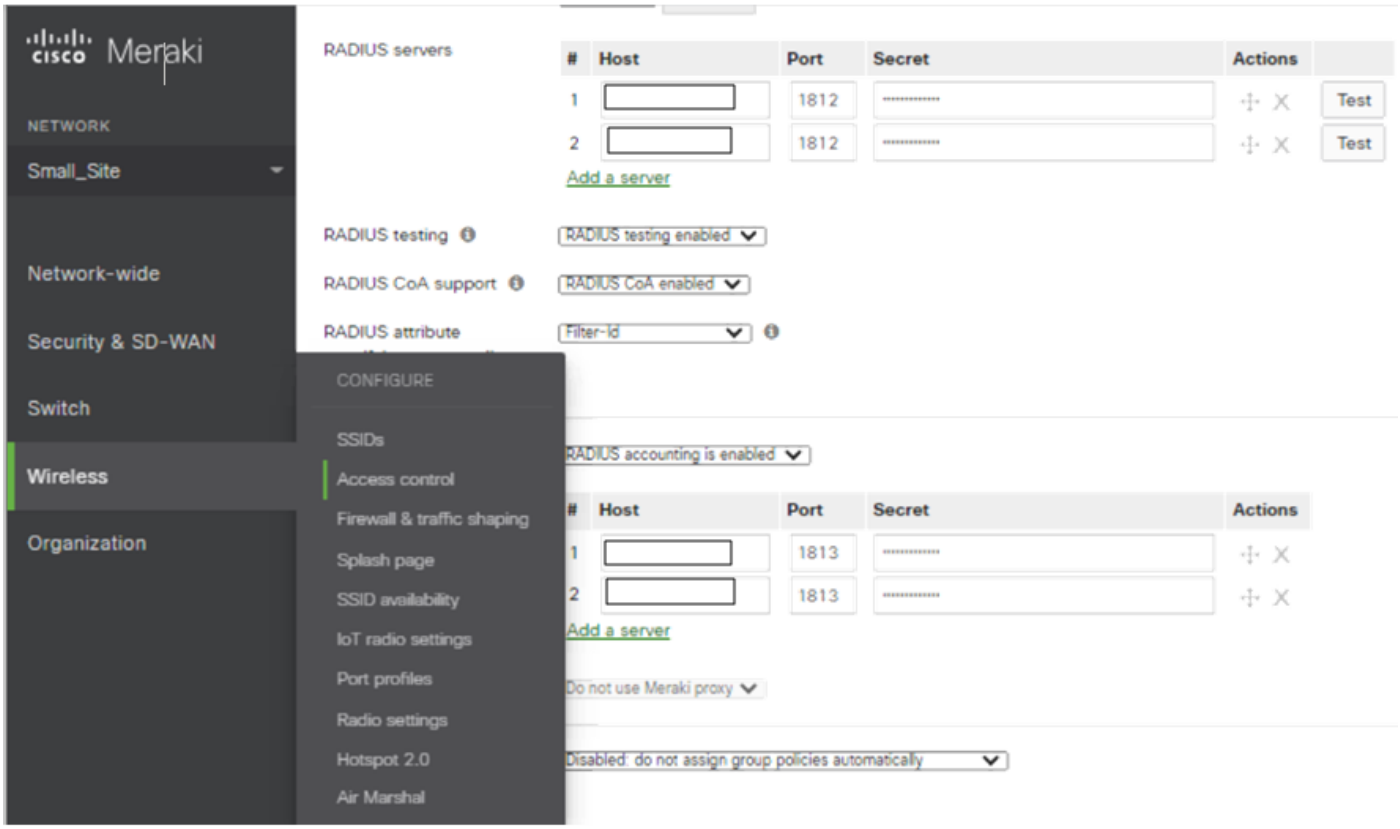
1. Dispositif de sécurité MX (configuré pour les ports d'accès ou sans fil)

- Pour les ports d'accès
  Sécurité et SD-WAN > Adressage et VLAN

- Pour les réseaux sans fil
  Sécurité et SD-WAN > Paramètres sans fil

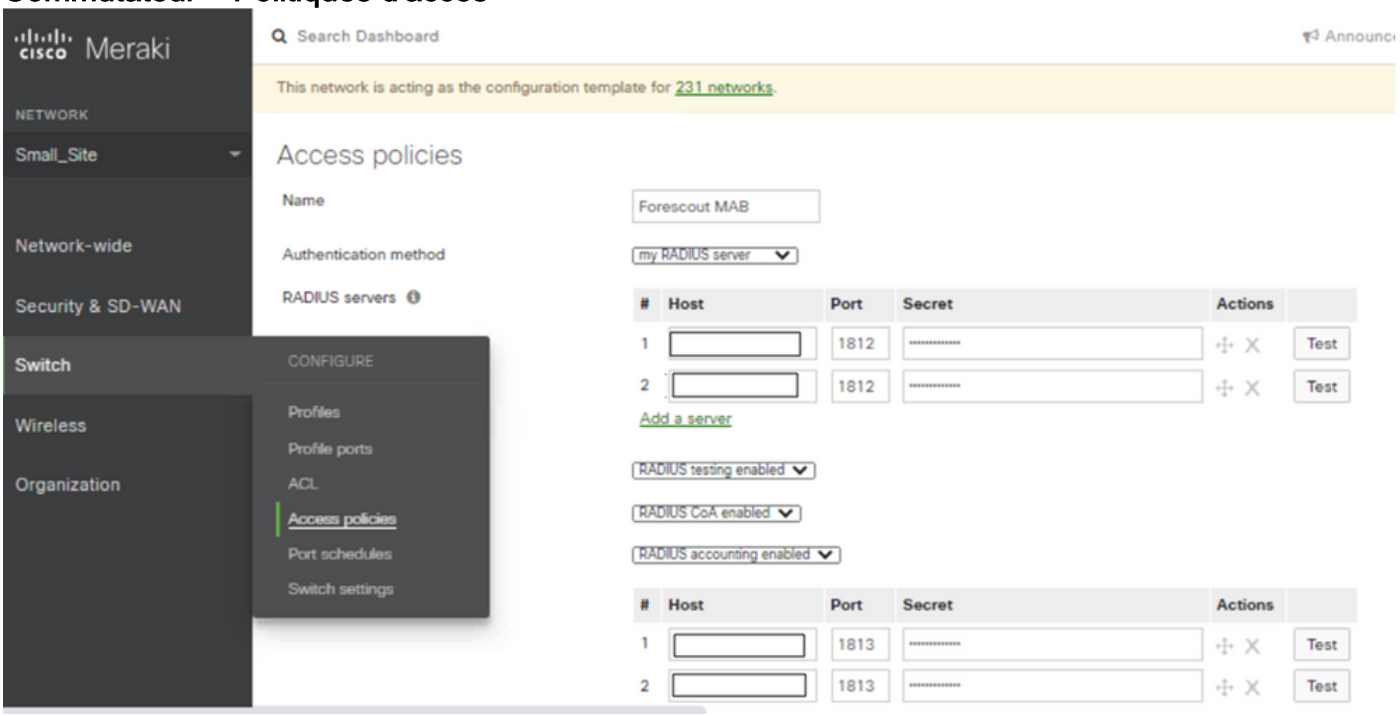


2. Points d'accès MR (activés par SSID (Service Set Identifier) :
Sans fil > Contrôle d'accès



3. Commutateurs MS

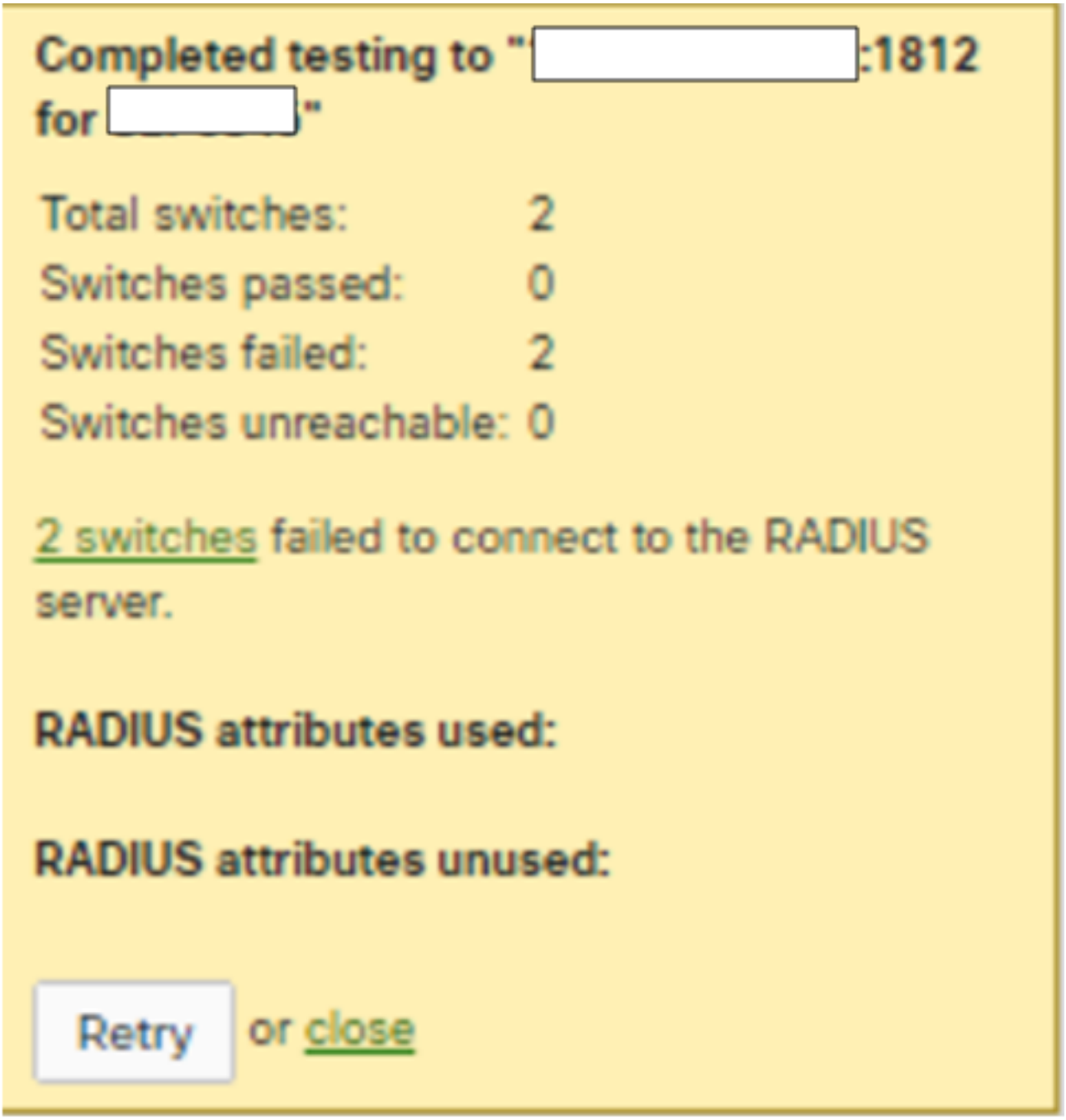
Commutateur > Politiques d'accès



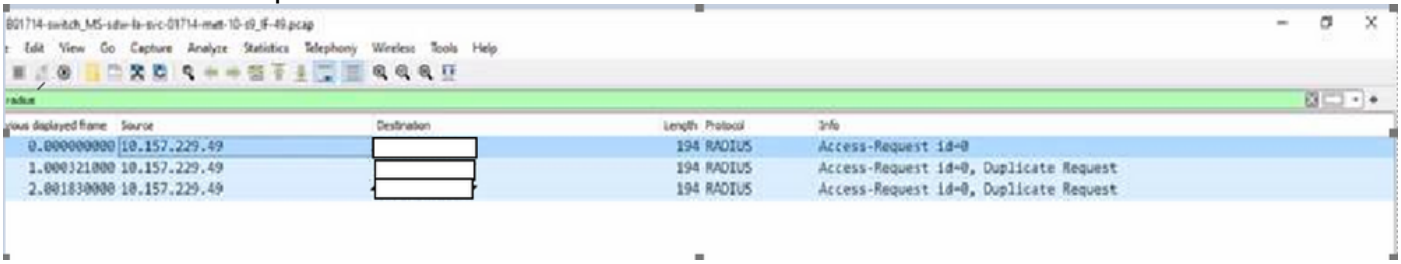
Test de vérification de configuration 802.1X

- **Tableau de bord Meraki > Modèle de réseau > Commutateur > Stratégies d'accès > Serveurs Radius > Tester**
- **Tableau de bord Meraki > Modèle de réseau > Accès sans fil > Contrôle d'accès > Serveurs Radius > Tester**

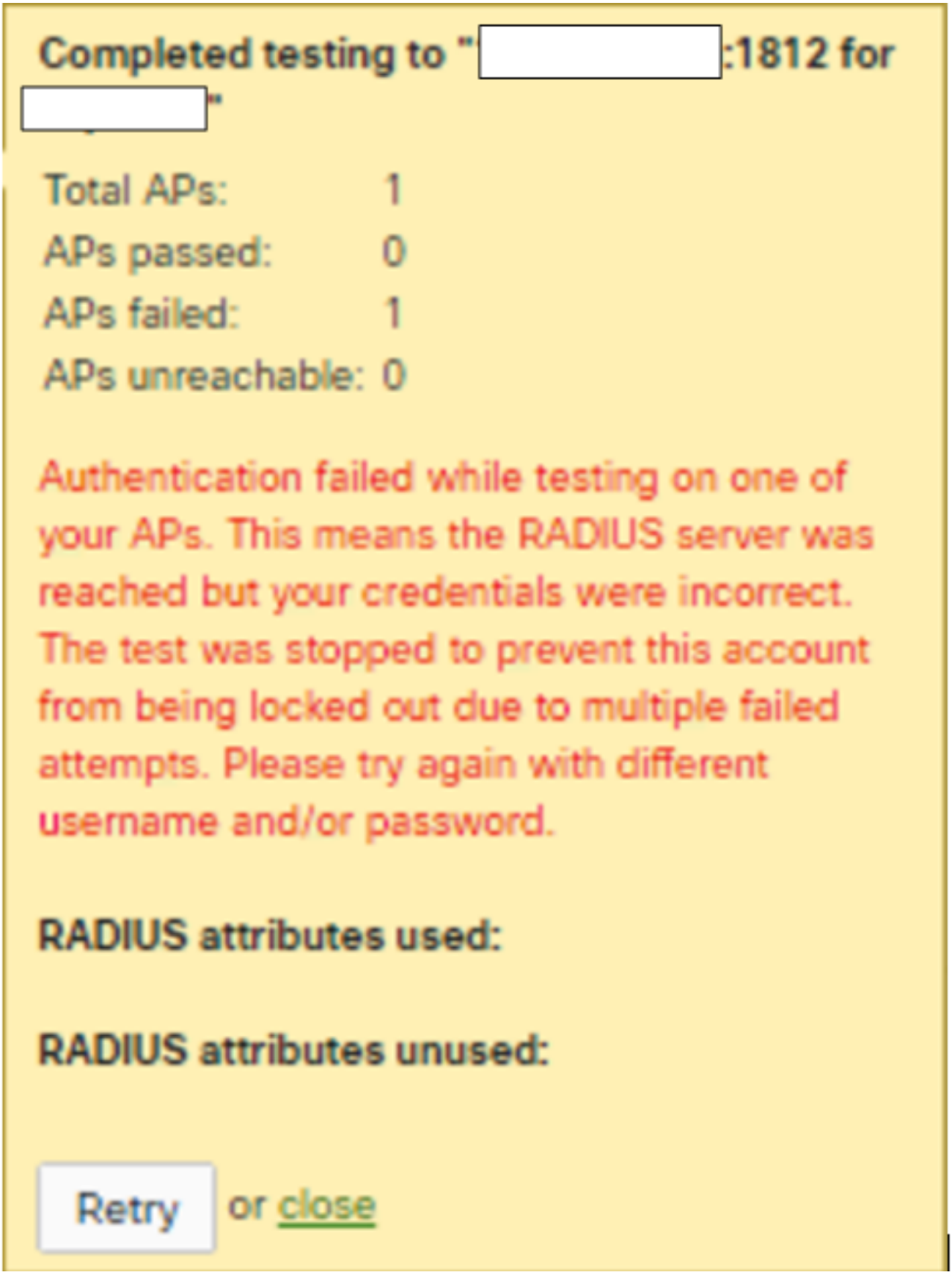
1. Si le résultat du test est remarqué alors que **All AP n'a pas réussi à connecter le serveur radius**, vous devez vérifier où la demande d'accès a été abandonnée.



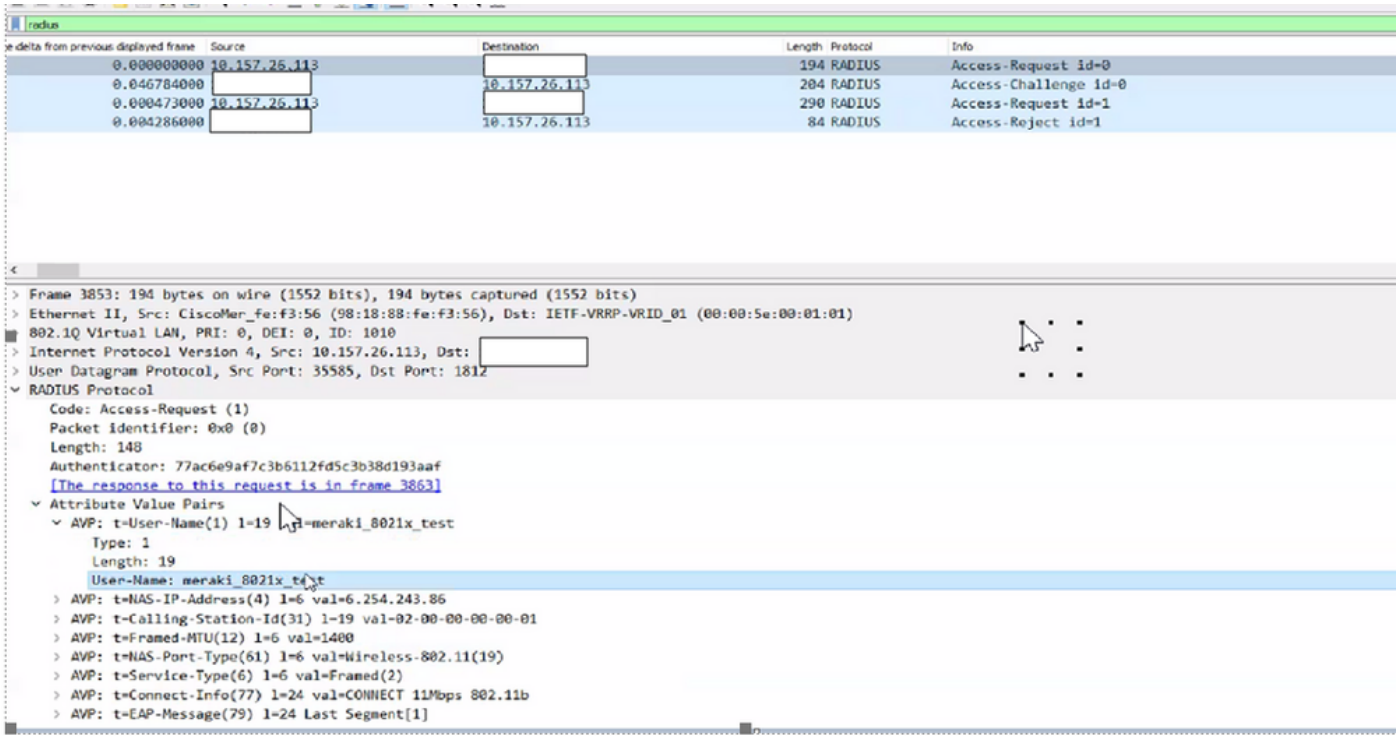
2. Exécutez la capture de paquets sur le port de liaison ascendante et vérifiez le flux de demande d'accès. Reportez-vous à la capture d'écran de l'accès à la capture de paquets : la requête n'obtient aucune réponse.



3. Si le résultat de test remarqué reçoit une réponse en tant qu'informations d'identification d'acceptation/rejet/refus/réponse/incorrectes, cela signifie que le serveur radius est actif.

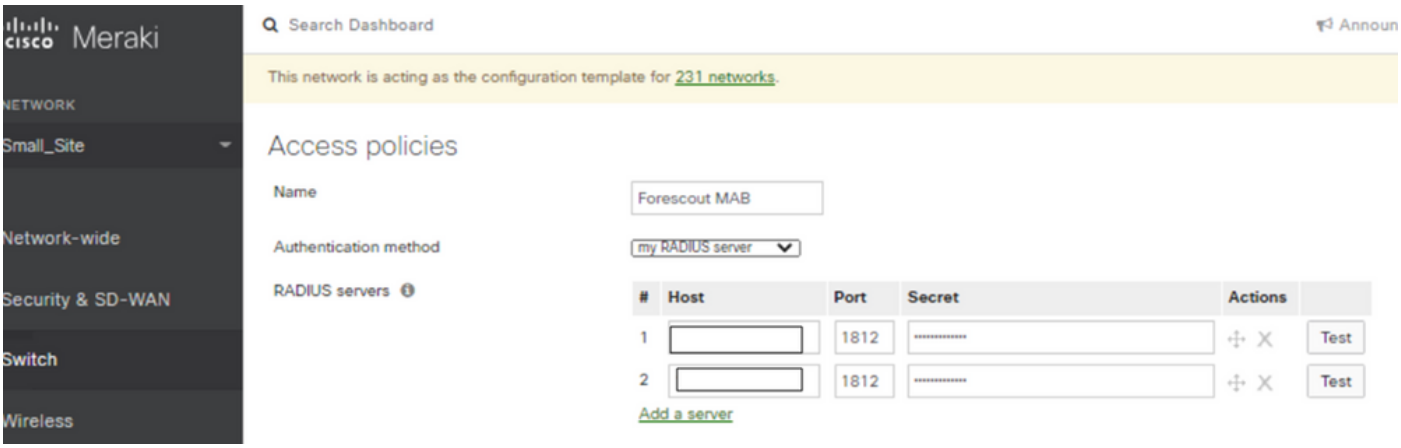


4. Exécutez la capture de paquets sur le port de liaison ascendante et vérifiez le flux de demande d'accès. Reportez-vous à la capture d'écran de l'accès à la capture de paquets - La demande a reçu une réponse.

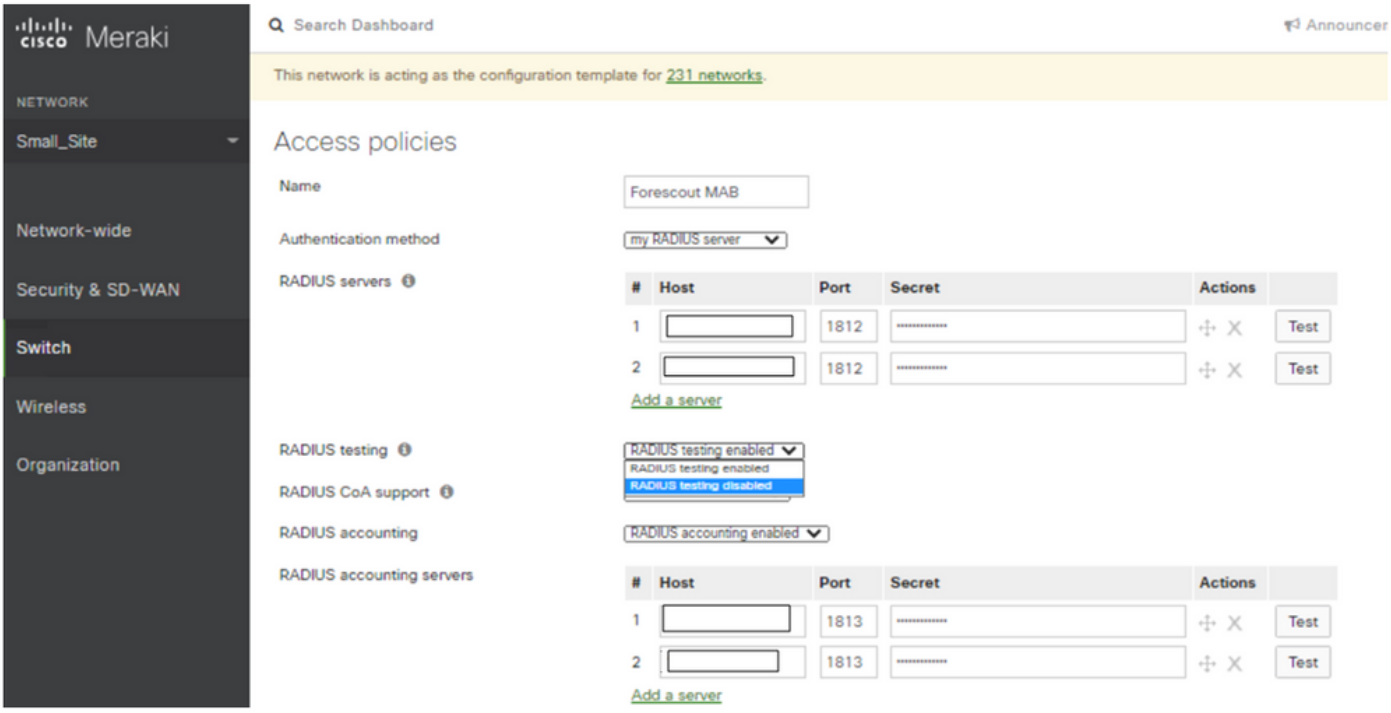


Vérification de la configuration de la stratégie d'accès

1. Vous devez vérifier que le paramètre mentionné dans la stratégie d'accès est correct et inclut l'adresse IP de l'hôte, le numéro de port et la clé secrète.



2. Les adresses IP de serveur RADIUS configurées sont factices ou ne sont pas utilisées dans la production ou la stratégie d'accès n'est pas utilisée. Il est recommandé de supprimer la stratégie d'accès. Si vous voulez le conserver, vous pouvez désactiver le **paramètre de test Radius.**



Informations connexes

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Support et documentation techniques - Cisco Systems

Remarque

- Lorsque les serveurs radius interrogent les périphériques Meraki à l'aide de l'adresse IP LAN et du nom d'utilisateur par défaut “ meraki_8021x_test ”, le tableau de bord Meraki utilise l'adresse MAC Meraki comme source.
- Meraki a fourni une visibilité sur ces alertes depuis octobre 2021.