Dépannage de " ; 5440 - Session EAP abandonnée et démarrage de New" ; Expiration du délai du demandeur ou configuration incorrecte

Table des matières

Problème

L'ISE envoie une demande d'accès RADIUS au terminal. Au lieu de répondre à la demande d'accès, le point d'extrémité redémarre à plusieurs reprises le processus d'authentification. L'authentification des terminaux avec Cisco Identity Services Engine (ISE) échoue finalement avec une erreur.

```
"5440 – Endpoint abandoned EAP session and started new"
```

Environnement

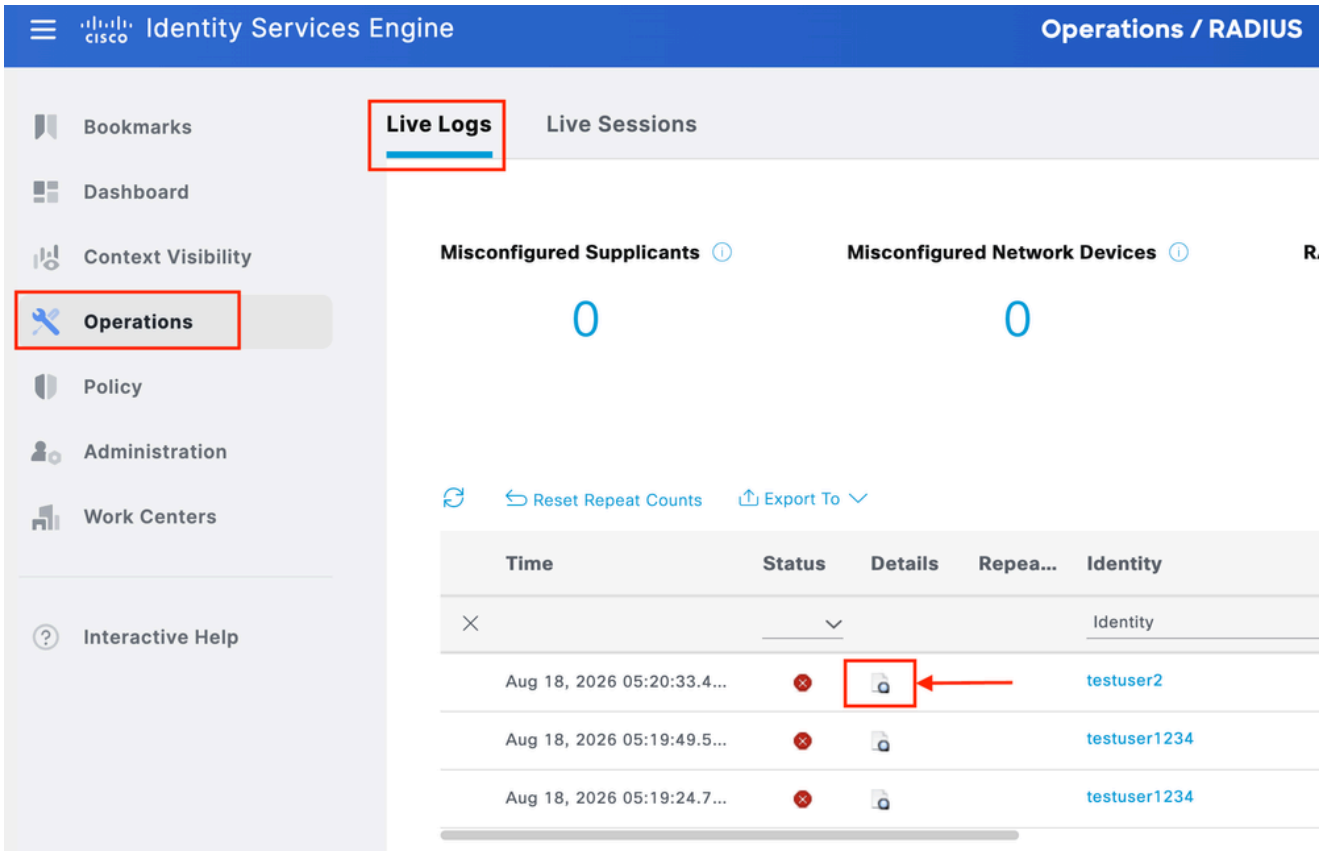
- Cisco Identity Services Engine (ISE)
- Authentification 802.1X
- Réseau filaire ou sans fil
- Authentification basée sur le protocole d'authentification extensible (EAP-TLS, PEAP, TEAP, etc.)
- Demandeur de point de terminaison configuré pour l'authentification 802.1X
- Périphérique d'accès réseau (NAD), tel qu'un commutateur Cisco ou un contrôleur LAN sans fil (WLC)

Résolution

Procédez comme suit pour résoudre les problèmes :

Vérifiez les détails de l'authentification ISE

1. Accédez à Operations > RADIUS > Live Logs.
2. Ouvrez l'authentification Échec.



3. Vérifiez que l'ISE envoie un « Access-Challenge ».
4. Confirmez que le terminal envoie une nouvelle « demande d'accès » au lieu de répondre au défi.
5. Notez le temps qui s'écoule entre le « Access-Challenge » et la nouvelle « Access-Request ».
6. Dans cette image, nous pouvons voir qu'ISE envoie un « défi d'accès », mais qu'ISE n'a reçu aucune réponse.

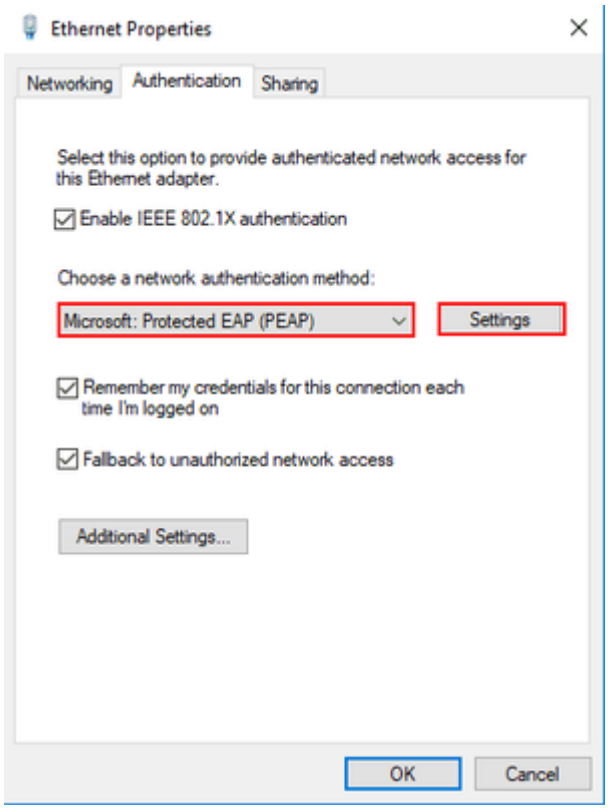
Cisco Identity Services Engine

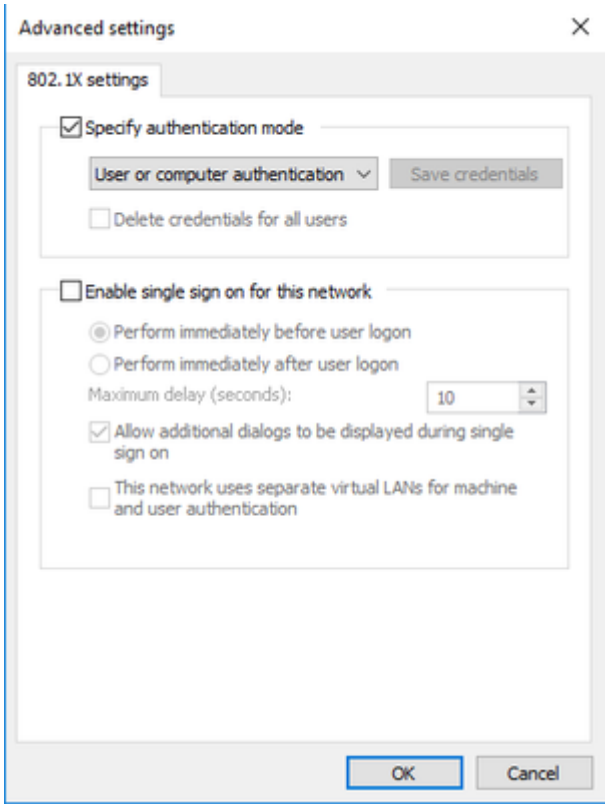
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	0
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	140
11018	RADIUS is re-using an existing session	0
12504	Extracted EAP-Response containing EAP-TLS challenge-response	1
12505	Prepared EAP-Request with another EAP-TLS challenge	0
11006	Returned RADIUS Access-Challenge	0
5440	Endpoint abandoned EAP session and started new	58134

Vérifier la configuration du demandeur de point de terminaison

- Vérifiez que la méthode EAP correcte est configurée.
- Vérifiez le mode d'authentification, tel que l'authentification Ordinateur, Utilisateur ou

Ordinateur + Utilisateur.





- Vérifiez le délai d'attente du demandeur et réessayez.
- Vérifiez que le point de terminaison utilise le profil 802.1X attendu.
- Comparez la configuration avec un terminal opérationnel.

Vérifier les journaux des terminaux

- Vérifiez le système d'exploitation et les journaux d'authentification du demandeur.
- Vérifiez si le demandeur reçoit la demande EAP.
- Identifiez tout délai d'attente, redémarrage de l'authentification ou erreurs liées à EAP.
- Si le client sécurisé Cisco est utilisé, collectez une offre groupée DART pour une analyse plus approfondie.
    - Collecter l'offre groupée DART pour client sécurisé

Vérifier le chemin réseau

- Effectuer des captures simultanées de paquets sur les terminaux (Wireshark) , NAD (SPAN-Switched Port Analyzer capture) et ISE (TCPDump)
- Vérifiez que le trafic EAPOL atteint le NAD.
- Vérifiez que les réponses RADIUS d'ISE atteignent le NAD.
- Vérifiez la perte ou le délai de paquets entre le point d'extrémité, NAD et ISE.
- Utilisez une capture de paquets lorsque les journaux des points d'extrémité n'identifient pas la raison du redémarrage.

Comparer avec un terminal opérationnel

- Utilisez la même NAD, le même PSN ISE et la même stratégie d'authentification lorsque cela est possible.
- Comparez la méthode EAP, la configuration du demandeur, les valeurs de délai d’attente et la séquence d’authentification.
- Si seuls des points d'extrémité spécifiques échouent, concentrez l'enquête sur la configuration du point d'extrémité ou le demandeur.

Pour vérifier si le problème est résolu, exécutez une nouvelle authentification et vérifiez que le point d'extrémité répond à la demande d'accès ISE et termine l'authentification sans générer de

5440.

Motif

Le demandeur de point d'extrémité ne termine pas l'authentification EAP dans le délai d'attente configuré ou utilise une configuration 802.1X incorrecte. Un délai d'attente court du demandeur, des paramètres EAP incorrects ou un problème du demandeur peuvent entraîner le redémarrage de l'authentification du point d'extrémité avant la fin de la session précédente.

Autres informations utiles

- Comprendre et configurer EAP-TLS

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.