Fehlerbehebung "5440-Endpunkt hat EAP-Sitzung abgebrochen und New" gestartet Aufgrund von Supplicant-Timeout oder falscher Konfiguration

Inhalt

Problem

Die ISE sendet eine RADIUS Access-Challenge an das Endgerät. Anstatt auf die Access-Challenge zu reagieren, startet das Endgerät den Authentifizierungsprozess wiederholt neu. Die Endgeräteauthentifizierung mit der Cisco Identity Services Engine (ISE) schlägt schließlich mit einem Fehler fehl.

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

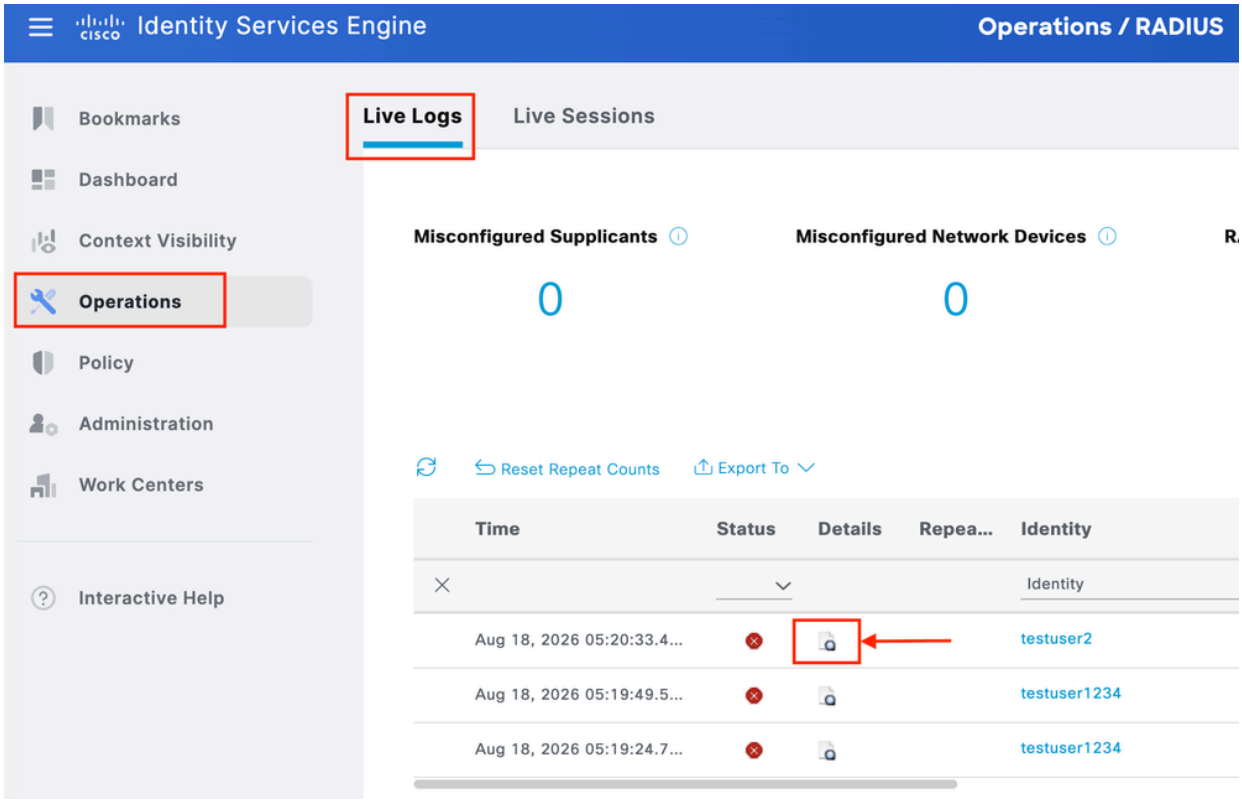
Umwelt

- Cisco ISE
- 802.1X-Authentifizierung
- Kabelgebundenes oder Wireless-Netzwerk
- EAP-basierte (Extensible Authentication Protocol) Authentifizierung
- Endgerätekomponente

Auflösung

Gehen Sie zur Fehlerbehebung wie folgt vor:

1. Überprüfen der ISE-Authentifizierungsdetails
    1. Navigieren Sie zu Operations > RADIUS > Live Logs.
    2. Öffnen Sie die fehlgeschlagene Authentifizierung.



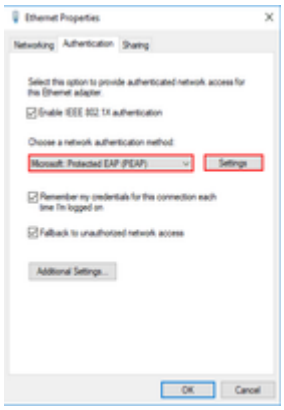
    3. Vergewissern Sie sich, dass die ISE eine "Access-Challenge" sendet.
    4. Vergewissern Sie sich, dass das Endgerät eine neue "Access-Request" sendet, anstatt auf die Herausforderung zu antworten.
    5. Notieren Sie sich die Zeit zwischen der Access-Challenge und dem neuen Access-Request.
    6. In diesem Bild sieht man, wie die ISE eine "Access-Challenge" sendet, aber keine Antwort erhielt.

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

2. Überprüfen der Endgerätekonfiguration

- Bestätigen Sie, dass die richtige EAP-Methode konfiguriert ist.
- Überprüfen Sie den Authentifizierungsmodus, z. B. Computer-, Benutzer- oder Computer + Benutzerauthentifizierung.



- Überprüfen Sie die Timeout- und Wiederholungseinstellungen der Komponente.
- Überprüfen Sie, ob der Endpunkt das erwartete 802.1X-Profil verwendet.
- Vergleichen Sie die Konfiguration mit einem funktionierenden Endgerät.

3. Überprüfen der Endgeräteprotokolle

- Überprüfen Sie die Protokolle für das Betriebssystem und die Supplicant-Authentifizierung.
- Überprüft, ob der Supplicant die EAP-Anfrage empfängt.
- Ermitteln Sie Zeitüberschreitungen, Authentifizierungsneustarts oder EAP-bezogene Fehler.
- Wenn Cisco Secure Client verwendet wird, sammeln Sie ein DART-Paket zur weiteren Analyse.
    - Sammeln Sie DART-Pakete für sichere Clients

4. Netzwerkpfad überprüfen

- Gleichzeitige Paketerfassung auf Endgeräten (Wireshark), NAD (SPAN-Erfassung) und ISE (TCPDump)
- Überprüfen, ob der EAPOL-Datenverkehr den NAD erreicht

- Überprüfen Sie, ob die RADIUS-Antworten der ISE die NAD erreichen.
- Überprüfen Sie, ob zwischen dem Endpunkt, NAD und der ISE Paketverluste oder Verzögerungen auftreten.
- Verwenden Sie eine Paketerfassung, wenn die Endpunktprotokolle den Grund für den Neustart nicht identifizieren.

5. Vergleich mit einem funktionierenden Endgerät

- Verwenden Sie so weit wie möglich dieselbe NAD, dasselbe ISE-PSN und dieselbe Authentifizierungsrichtlinie.
- Vergleichen Sie die EAP-Methode, die Supplicant-Konfiguration, die Timeout-Werte und die Authentifizierungssequenz.
- Wenn nur bestimmte Endgeräte ausfallen, konzentrieren Sie die Untersuchung auf die Endgerätekonfiguration oder Komponente.

Um zu überprüfen, ob das Problem behoben wurde, führen Sie eine neue Authentifizierung durch, und überprüfen Sie, ob das Endgerät auf die ISE Access-Challenge antwortet und die Authentifizierung erfolgreich abschließt, ohne 5440 zu generieren.

Ursache

Die Endgerätekomponente schließt die EAP-Authentifizierung nicht innerhalb des konfigurierten Timeouts ab oder verwendet eine falsche 802.1X-Konfiguration. Ein kurzer Zeitüberschreitungswert für die Komponente, falsche EAP-Einstellungen oder ein Problem mit der Komponente können dazu führen, dass der Endpunkt die Authentifizierung neu startet, bevor die vorherige Sitzung beendet wird.

Verwandte Inhalte

- Verständnis und Konfiguration von EAP-TLS

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.