Risoluzione dei problemi "5440 Endpoint Abandonato Sessione EAP E Avviato Nuovo" A causa di timeout del richiedente o configurazione errata

Sommario

Problema

L'ISE invia un messaggio di richiesta di verifica di accesso RADIUS all'endpoint. Anziché rispondere alla richiesta di verifica dell'accesso, l'endpoint riavvia ripetutamente il processo di autenticazione. L'autenticazione dell'endpoint con Cisco Identity Services Engine (ISE) ha infine esito negativo con un errore.

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

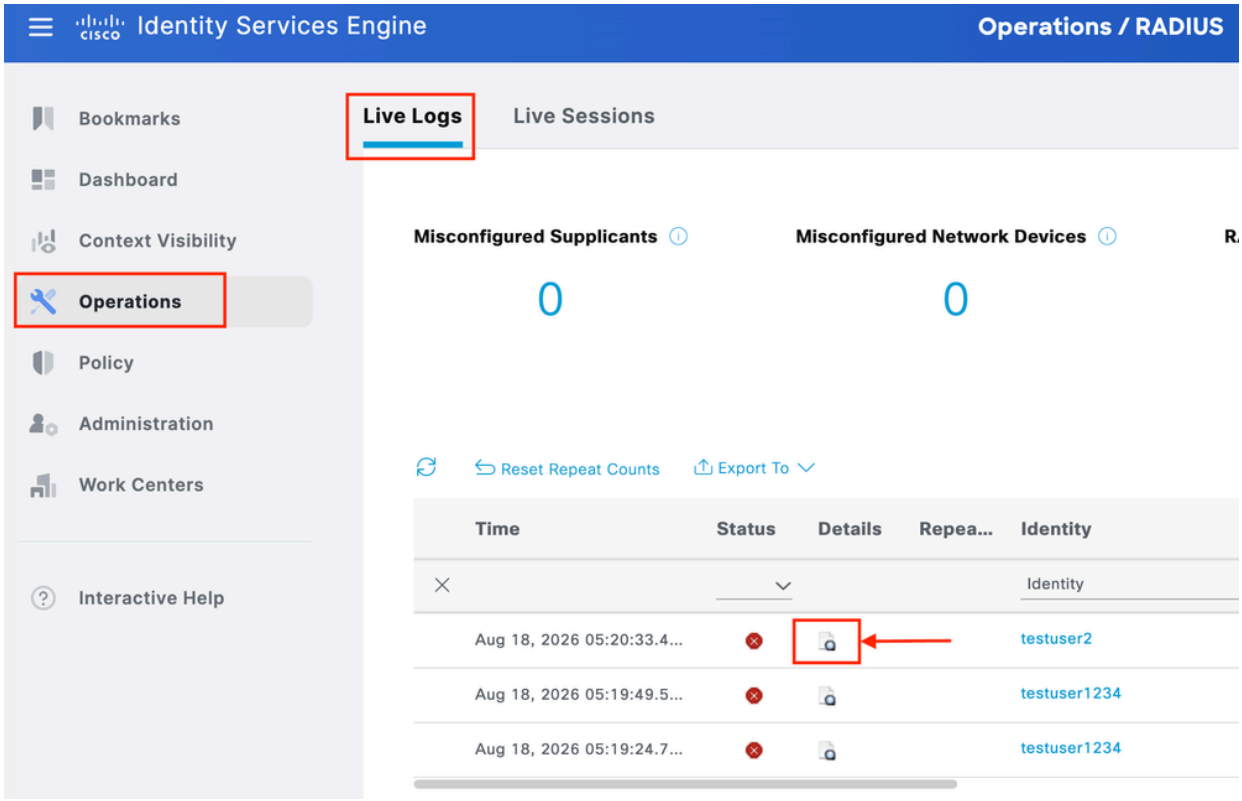
Ambiente

- Cisco ISE
- Autenticazione 802.1X
- Rete cablata o wireless
- Autenticazione basata su EAP (Extensible Authentication Protocol)
- Supplicant endpoint

Risoluzione

Per risolvere il problema, procedere come segue:

1. Controlla i dettagli dell'autenticazione ISE
    1. Passare a Operazioni > RADIUS > Live Log.
    2. Aprire l'autenticazione non riuscita.



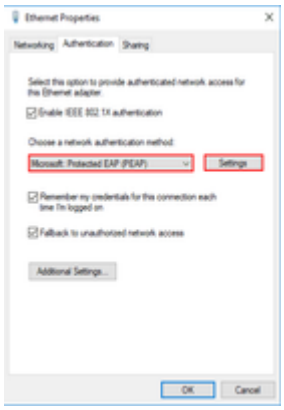
    3. Verificare che ISE invii una "Access-Challenge".
    4. Confermare che l'endpoint invii una nuova "Access-Request" anziché rispondere alla richiesta.
    5. Prendere nota del tempo che intercorre tra l'esecuzione di Access-Challenge e la nuova esecuzione di Access-Request.
    6. In questa immagine, vediamo ISE inviare "Access-Challenge", ma ISE non ha ricevuto risposta.

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. Verificare la configurazione del supplicant dell'endpoint

- Verificare che sia configurato il metodo EAP corretto.
- Verificare la modalità di autenticazione, ad esempio Autenticazione computer, utente o computer + utente.



- Verificare le impostazioni di timeout e riprovare.
- Verificare che l'endpoint utilizzi il profilo 802.1X previsto.
- Confrontare la configurazione con un endpoint funzionante.

3. Controllare i registri degli endpoint

- Esaminare i registri di autenticazione del sistema operativo e dei supplicant.
- Controllare se il supplicant riceve la richiesta EAP.
- Identificare eventuali timeout, riavvii dell'autenticazione o errori correlati a EAP.
- Se si utilizza Cisco Secure Client, raccogliere un bundle DART per ulteriori analisi.
    - Raccogli bundle DART per Secure Client

4. Controllare il percorso di rete

- Acquisizione simultanea di pacchetti sull'endpoint (Wireshark), NAD (SPAN capture) e ISE (TCP/IPump)
- Verificare che il traffico EAPOL raggiunga NAD.

- Verificare che le risposte RADIUS da ISE raggiungano il server NAD.
- Verificare la perdita o il ritardo del pacchetto tra l'endpoint, NAD e ISE.
- Utilizzare l'acquisizione di un pacchetto quando i registri dell'endpoint non identificano il motivo del riavvio.

5. Confrontare con un endpoint funzionante

- Ove possibile, utilizzare lo stesso NAD, ISE PSN e il criterio di autenticazione.
- Confrontare il metodo EAP, la configurazione supplicant, i valori di timeout e la sequenza di autenticazione.
- Se solo determinati endpoint hanno esito negativo, focalizzare l'analisi sulla configurazione dell'endpoint o sul supplicant.

Per verificare se il problema è stato risolto, eseguire una nuova autenticazione e verificare che l'endpoint risponda alla richiesta di verifica di accesso ISE e completi l'autenticazione senza generare il modello 5440.

Causa

Il supplicant dell'endpoint non completa l'autenticazione EAP entro il timeout configurato o utilizza una configurazione 802.1X non corretta. Un breve timeout del supplicant, impostazioni EAP non corrette o un problema del supplicant possono determinare il riavvio dell'autenticazione dell'endpoint prima del completamento della sessione precedente.

Contenuto correlato

- Comprendere e configurare EAP-TLS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).