Solução de problemas "5440 Endpoint Abandonou sessão EAP e iniciou New" Devido a Tempo Limite do Requerente ou Configuração Incorreta

Contents

Problema

O ISE envia um Desafio de Acesso RADIUS ao endpoint. Em vez de responder ao desafio de acesso, o endpoint reinicia repetidamente o processo de autenticação. A autenticação do ponto final com o Cisco Identity Services Engine (ISE) finalmente falha com erro.

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

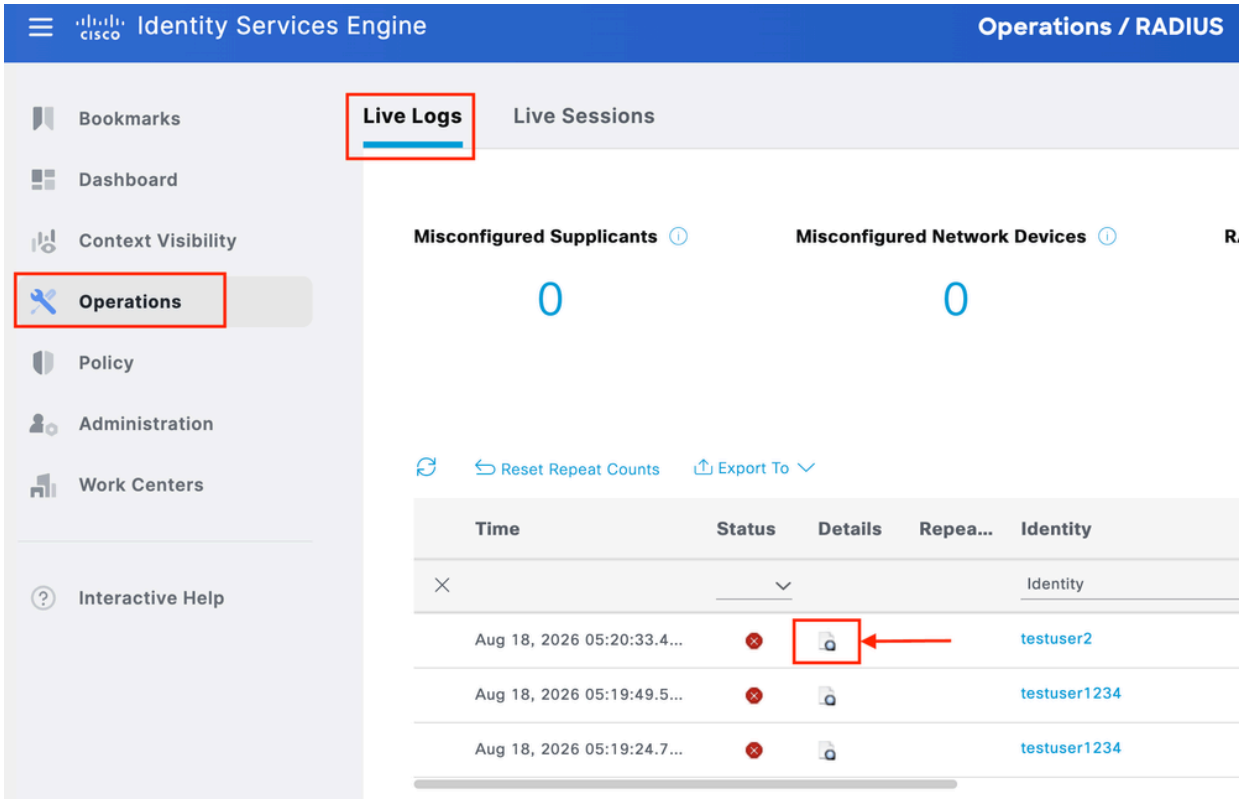
Ambiente

- Cisco ISE
- Autenticação 802.1X
- Rede com ou sem fio
- Autenticação baseada em EAP (Extensible Authentication Protocol)
- Solicitante do ponto final

Resolução

Siga estas etapas para solucionar problemas:

1. Verifique os detalhes de autenticação do ISE
    1. Navegue até Operations > RADIUS > Live Logs.
    2. Abra a autenticação com falha.



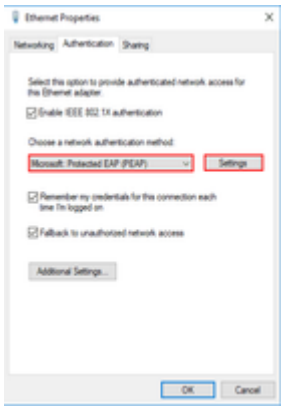
    3. Verifique se o ISE envia um "Access-Challenge".
    4. Confirme se o endpoint envia uma nova "Solicitação de Acesso" em vez de responder ao desafio.
    5. Observe o tempo entre o desafio de acesso e a nova solicitação de acesso.
    6. Nessa imagem, podemos ver o ISE enviando "Access-Challenge", mas o ISE não recebeu nenhuma resposta.

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. Verificar a configuração do solicitante do ponto final

- Confirme se o método EAP correto está configurado.
- Verifique o modo de autenticação, como máquina, usuário ou máquina + autenticação de usuário.



- Verifique o tempo limite do solicitante e tente novamente as configurações.
- Verifique se o ponto final usa o perfil 802.1X esperado.
- Compare a configuração com um endpoint em funcionamento.

3. Verificar os logs de ponto de extremidade

- Revisar os registros do sistema operacional e da autenticação do solicitante.
- Verifique se o requerente recebe a solicitação EAP.
- Identifique todos os erros relacionados a timeout, reinicialização de autenticação ou EAP.
- Se o Cisco Secure Client for usado, colete um pacote DART para análise adicional.
    - Coletar pacote DART para cliente seguro

4. Verificar o caminho da rede

- Faça capturas de pacotes simultâneas no endpoint (Wireshark), NAD (captura de SPAN) e ISE (TCPDump)
- Verifique se o tráfego EAPOL chega ao NAD.

- Verifique se as respostas RADIUS do ISE alcançam o NAD.
- Verifique se há perda ou atraso de pacote entre o endpoint, NAD e ISE.
- Use uma captura de pacote quando os logs de endpoint não identificarem o motivo da reinicialização.

5. Compare com um endpoint em funcionamento

- Use o mesmo NAD, ISE PSN e política de autenticação sempre que possível.
- Compare o método EAP, a configuração do solicitante, os valores de tempo limite e a sequência de autenticação.
- Se apenas endpoints específicos falharem, concentre a investigação na configuração do endpoint ou no solicitante.

Para validar se o problema foi resolvido, execute uma nova autenticação e verifique se o endpoint responde ao desafio de acesso do ISE e conclui a autenticação com êxito sem gerar o 5440.

Causa

O solicitante do ponto final não conclui a autenticação EAP dentro do tempo limite configurado ou usa uma configuração 802.1X incorreta. Um tempo limite curto do solicitante, configurações EAP incorretas ou um problema do solicitante podem fazer com que o ponto de extremidade reinicie a autenticação antes que a sessão anterior seja concluída.

Conteúdo relacionado

- Entender e configurar EAP-TLS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.