

Solucione problemas de alerta de falha recente do 802.1X no dispositivo Meraki

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Qual é o teste RADIUS em dispositivos Meraki?](#)

[Configurar](#)

[Diagrama de Rede](#)

[Verificar e solucionar problemas](#)

[Configuração 802.1X](#)

[Teste de verificação de configuração 802.1X](#)

[Informações Relacionadas](#)

[Nota](#)

Introduction

Este documento descreve como resolver o recente alerta de falha 802.1X no dispositivo Meraki.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entender a solução básica de rede de longa distância definida por software (SDWAN) da Meraki
- Entender a política de acesso básica e a autenticação Radius

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

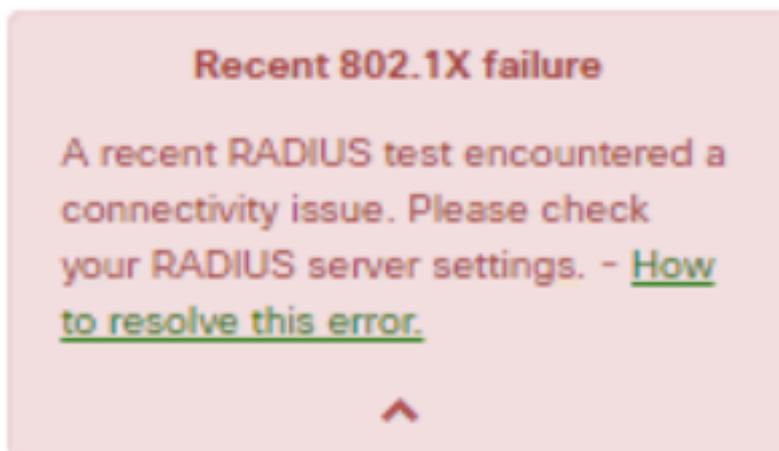
Problema

Os dispositivos Meraki usam a configuração de política do servidor AAA radius para autenticar o usuário final.

Qual é o teste RADIUS em dispositivos Meraki?

O alerta de falha recente do 802.1X exibiu que, se as mensagens periódicas de solicitação de acesso enviadas aos servidores RADIUS configurados estiverem inacessíveis, você deverá usar um período de tempo limite de 10 segundos.

Os dispositivos Meraki enviam periodicamente mensagens de solicitação de acesso aos servidores RADIUS configurados que usam a identidade **meraki_8021x_test** para garantir que os servidores RADIUS estejam acessíveis. Essas solicitações de acesso têm um tempo limite de 10 segundos e, se o servidor RADIUS não responder, ele considera que os servidores radius estão inalcançáveis e solicita a mensagem de alerta "Falha recente 802.1X". Consulte a captura de tela do alerta visto no dispositivo:



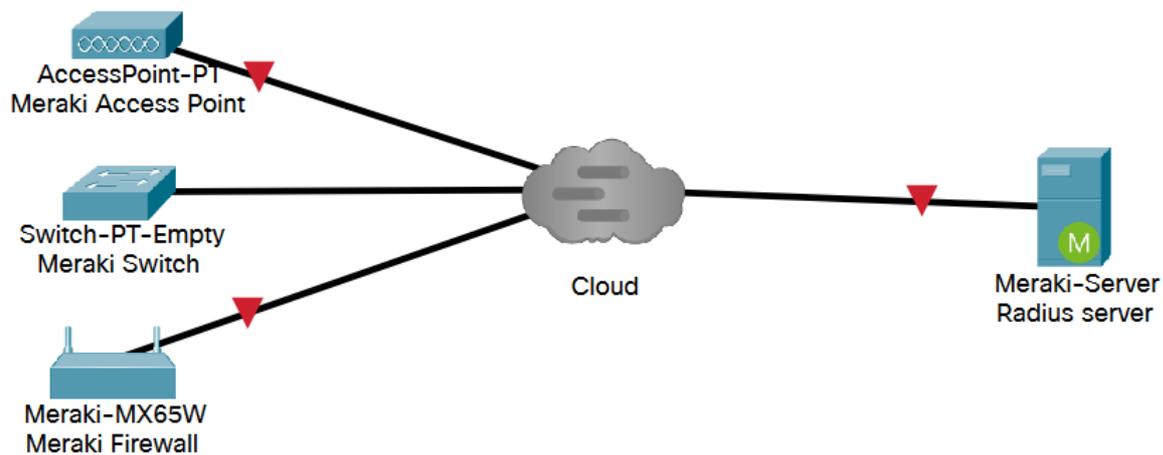
Um teste é considerado bem-sucedido se o dispositivo Meraki receber qualquer resposta RADIUS legítima (Access-Accept/Reject/Challenge) do servidor.

Com o teste RADIUS ativado, todos os servidores RADIUS são mantidos em execução de teste em cada nó pelo menos uma vez por 24 horas, independentemente do resultado do teste. Se um teste RADIUS falhar para um determinado nó, ele testa novamente a cada hora até que ocorra um resultado que passe. Uma aprovação subsequente marca o servidor alcançável, limpa o alerta e retorna ao ciclo de teste de 24 horas.

Configurar

Diagrama de Rede

Este é um diagrama simples de topologia que descreve a configuração:



Verificar e solucionar problemas

Configuração 802.1X

A configuração RADIUS 802.1X pode ser encontrada no caminho mostrado, dependendo do modelo do produto Meraki.

1. Dispositivo de segurança MX (configurado para portas de acesso ou sem fio)

- Para portas de acesso
Segurança e SD-WAN > Endereçamento e VLANs

- Para redes sem fio
Segurança e SD-WAN > Configurações sem fio

2. Pontos de acesso MR (habilitado por SSID (Service Set Identifier): **Sem fio > Controle de acesso**

RADIUS servers

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	⇄ X Test
2	<input type="text"/>	1812	⇄ X Test

[Add a server](#)

RADIUS testing:

RADIUS CoA support:

RADIUS attribute:

RADIUS accounting is enabled

3. Switches MS

Switch > Políticas de acesso

Access policies

Name:

Authentication method:

RADIUS servers

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	⇄ X Test
2	<input type="text"/>	1812	⇄ X Test

[Add a server](#)

RADIUS testing enabled

RADIUS CoA enabled

RADIUS accounting enabled

Teste de verificação de configuração 802.1X

- Painel Meraki > Modelo de rede > Switch > Políticas de acesso > Servidores Radius > Teste
- Painel Meraki > Modelo de Rede > Tecnologia Wireless > Controle de acesso > Servidores Radius > Teste

1. Se o resultado do teste for notado como **All AP failed to connect radius server**, você precisará

verificar onde a solicitação de acesso foi removida.

Completed testing to "[redacted]:1812
for [redacted]"

Total switches: 2
Switches passed: 0
Switches failed: 2
Switches unreachable: 0

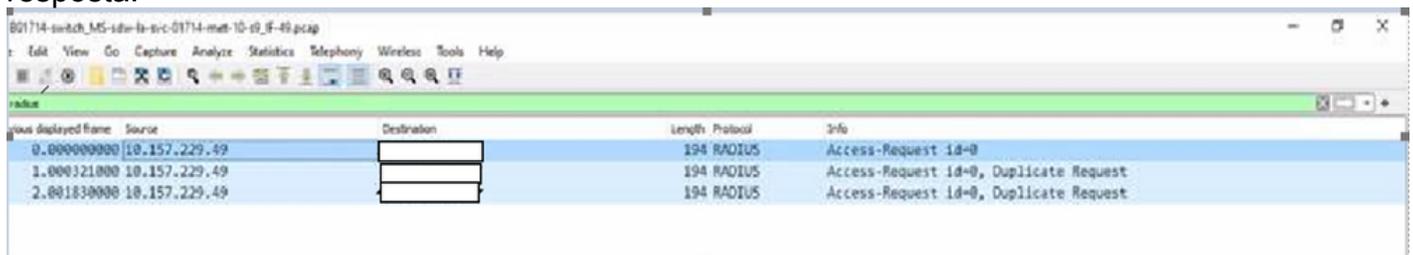
2 switches failed to connect to the RADIUS server.

RADIUS attributes used:

RADIUS attributes unused:

or close

2. Execute a captura de pacotes na porta de uplink e verifique o fluxo de solicitação de acesso. Consulte a captura de tela do acesso à captura de pacotes - A solicitação não recebe nenhuma resposta.



The screenshot shows a Wireshark interface with a packet capture of RADIUS traffic. The packet list pane shows three frames:

Time	Source	Destination	Length	Protocol	Info
0.000000000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0
1.000321000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0, Duplicate Request
2.001830000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0, Duplicate Request

3. Se o resultado do teste observado for retornado como credenciais de aceitação/rejeição/negação/resposta/incorreta, significa que o servidor radius está ativo.

Completed testing to "[redacted]:1812 for

[redacted]"

Total APs: 1
APs passed: 0
APs failed: 1
APs unreachable: 0

Authentication failed while testing on one of your APs. This means the RADIUS server was reached but your credentials were incorrect. The test was stopped to prevent this account from being locked out due to multiple failed attempts. Please try again with different username and/or password.

RADIUS attributes used:

RADIUS attributes unused:

or [close](#)

4. Execute a capture of packets on the uplink port and verify the flow of the access request. Consult the packet capture screenshot of the access request - The request received a response.

Time delta from previous displayed frame	Source	Destination	Length	Protocol	Info
0.000000000	10.157.26.113		194	RADIUS	Access-Request id=0
0.046784000		10.157.26.113	204	RADIUS	Access-Challenge id=0
0.000473000	10.157.26.113		290	RADIUS	Access-Request id=1
0.004286000		10.157.26.113	84	RADIUS	Access-Reject id=1


```

> Frame 3853: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
> Ethernet II, Src: CiscoMer_fe:f3:56 (98:18:88:fe:f3:56), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1010
> Internet Protocol Version 4, Src: 10.157.26.113, Dst: 
> User Datagram Protocol, Src Port: 35585, Dst Port: 1812
> RADIUS Protocol
  Code: Access-Request (1)
  Packet Identifier: 0x0 (0)
  Length: 148
  Authenticator: 77ac6e9af7c3b6112fd5c3b38d193aaf
  [The response to this request is in frame 3863]
  Attribute Value Pairs
    AVP: t=User-Name(1) 1=19 val=meraki_8021x_test
      Type: 1
      Length: 19
      User-Name: meraki_8021x_test
    > AVP: t=NAS-IP-Address(4) 1=6 val=6.254.243.86
    > AVP: t=Calling-Station-Id(31) 1=19 val=02-00-00-00-00-00-01
    > AVP: t=Framed-MTU(12) 1=6 val=1400
    > AVP: t=NAS-Port-Type(61) 1=6 val=Wireless-802.11(19)
    > AVP: t=Service-Type(6) 1=6 val=Framed(2)
    > AVP: t=Connect-Info(77) 1=24 val=CONNECT 11Mbps 802.11b
    > AVP: t=EAP-Message(79) 1=24 Last Segment[1]
  
```

Verificação da configuração da política de acesso

1. É necessário verificar se o parâmetro mencionado na política de acesso está correto e inclui o IP do host, o número da porta e a chave secreta.

Search Dashboard Announ

This network is acting as the configuration template for [231 networks](#).

Access policies

Name: Forescout MAB

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions
1		1812	*****	⊕ × Test
2		1812	*****	⊕ × Test

[Add a server](#)

2. Os IPs do servidor radius configurados são fictícios ou não são usados na produção ou a política de acesso não está em uso. Recomenda-se remover a política de acesso. Se quiser mantê-lo, você pode desativar a **configuração de teste de RADIUS**.

Search Dashboard Announcer

This network is acting as the configuration template for [231 networks](#).

Access policies

Name: Forescout MAB

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	*****	⊕ × Test
2	<input type="text"/>	1812	*****	⊕ × Test

[Add a server](#)

RADIUS testing: RADIUS testing enabled

RADIUS CoA support

RADIUS accounting: RADIUS accounting enabled

RADIUS accounting servers

#	Host	Port	Secret	Actions
1	<input type="text"/>	1813	*****	⊕ × Test
2	<input type="text"/>	1813	*****	⊕ × Test

[Add a server](#)

Informações Relacionadas

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- [Suporte Técnico e Documentação - Cisco Systems](#)

Nota

- Quando os servidores radius pesquisam os dispositivos Meraki usam o IP da LAN e o nome de usuário padrão "meraki_8021x_test", o painel da Meraki usou o endereço MAC da Meraki como origem.
- A Meraki disponibilizou visibilidade para esses alertas desde outubro de 2021.