

Risoluzione dei problemi relativi all'avviso di errore 802.1X recente nel dispositivo Meraki

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Cos'è il test RADIUS nei dispositivi Meraki?](#)

[Configurazione](#)

[Esempio di rete](#)

[Verifica E Risoluzione Dei Problemi](#)

[Configurazione 802.1X](#)

[Test di verifica della configurazione 802.1X](#)

[Informazioni correlate](#)

[Nota](#)

Introduzione

Questo documento descrive come risolvere il recente avviso di errore 802.1X nel dispositivo Meraki.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comprendere le soluzioni base SDWAN (Wide Area Network) definite dal software Meraki
- Informazioni sulle regole di accesso di base e sull'autenticazione Radius

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

I dispositivi Meraki usano la configurazione delle policy del server AAA Radius per autenticare l'utente finale.

Cos'è il test RADIUS nei dispositivi Meraki?

Il recente avviso di errore 802.1X ha indicato che, se i messaggi periodici di richiesta di accesso inviati ai server RADIUS configurati non sono raggiungibili, è necessario utilizzare un periodo di timeout di 10 secondi.

I dispositivi Meraki inviano periodicamente messaggi di richiesta di accesso ai server RADIUS configurati che utilizzano l'identità **meraki_8021x_test** per garantire che i server RADIUS siano raggiungibili. Queste richieste di accesso hanno un timeout di 10 secondi e se il server RADIUS non risponde, considera i server RADIUS irraggiungibili e richiede il messaggio di avviso "Errore recente 802.1X". Fare riferimento allo screenshot dell'avviso visualizzato sul dispositivo:



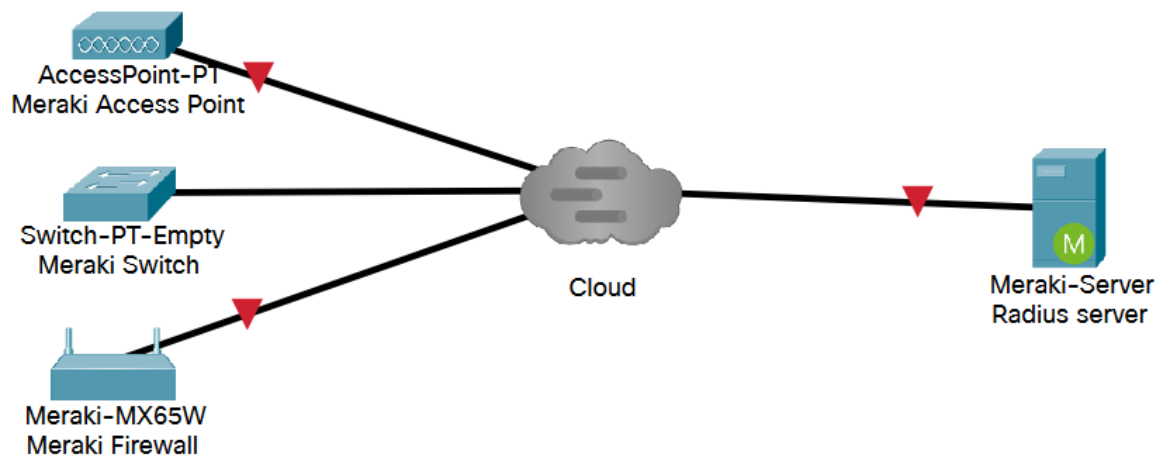
Un test è considerato riuscito se il dispositivo Meraki riceve una risposta RADIUS legittima (Access-Accept/Reject/Challenge) dal server.

Se il test RADIUS è abilitato, tutti i server RADIUS vengono mantenuti in esecuzione su ogni nodo almeno una volta ogni 24 ore, indipendentemente dal risultato del test. Se un test RADIUS non riesce per un determinato nodo, viene eseguito di nuovo ogni ora finché non si verifica un risultato positivo. Un passaggio successivo indica che il server è raggiungibile, cancella l'avviso e torna al ciclo di test di 24 ore.

Configurazione

Esempio di rete

Di seguito è riportato un semplice diagramma della topologia che descrive l'installazione:



Verifica E Risoluzione Dei Problemi

Configurazione 802.1X

La configurazione RADIUS 802.1X è disponibile nel percorso indicato, che dipende dal modello del prodotto Meraki.

1. Appliance MX-Security (configurata per porte di accesso o wireless)

- Per porte di accesso
Sicurezza e SD-WAN > Indirizzamento e VLAN
- Per wireless
Sicurezza e SD-WAN > Impostazioni wireless

2. Punti di accesso MR (abilitati in base agli SSID (Service Set Identifier)): **Wireless > Controllo degli accessi**

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 support **enabled**

RADIUS attribute **Filter-Id**

RADIUS accounting is enabled

3. Switch MS Cambia > Criteri di accesso

Access policies

Name: Forescout MAB

Authentication method: my RADIUS server

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

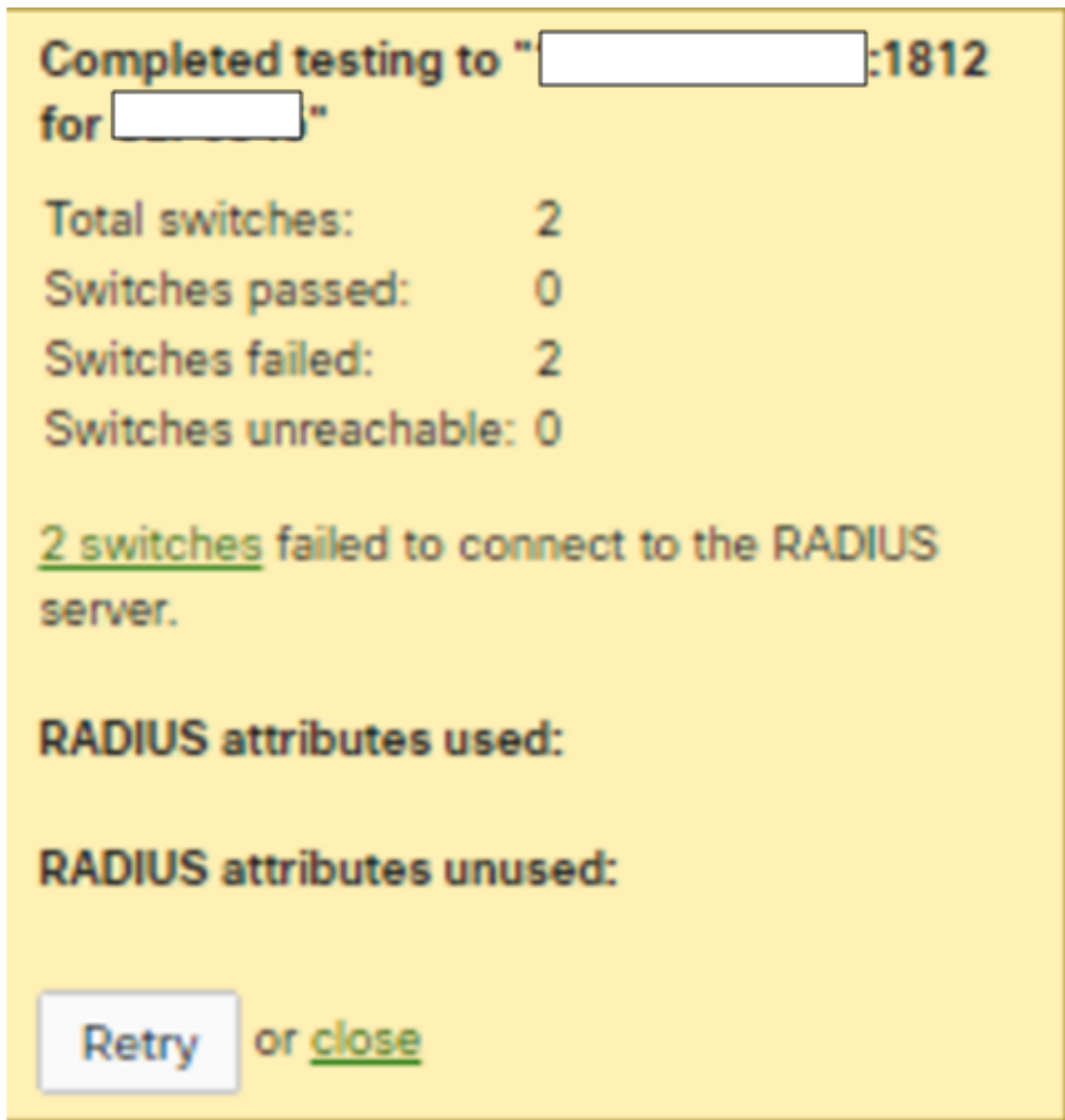
RADIUS accounting enabled

Test di verifica della configurazione 802.1X

- Dashboard Meraki > Modello Di Rete > Switch > Policy Di Accesso > Server Radius > Test
- Dashboard Meraki > Modello di rete > Wireless > Controllo dell'accesso > Server Radius > Test

1. Se il risultato del test viene rilevato come **tutti gli access point non siano riusciti a connettere il**

server radius, è necessario controllare dove la richiesta di accesso è stata eliminata.



2. Eseguire l'acquisizione dei pacchetti sulla porta uplink e verificare il flusso di richiesta di accesso. Fare riferimento alla schermata di packet capture access - La richiesta non riceve alcuna risposta.

Time	Source	Destination	Length	Protocol	Info
0.000000000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0
1.000321800	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 il risultato del test viene segnalato come credenziali di accettazione/rifiuto/negazione/risposta/errate, significa che il server RADIUS è attivo.

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. Eseguire l'acquisizione dei pacchetti sulla porta uplink e verificare il flusso di richiesta di accesso. Fare riferimento allo screenshot dell'accesso all'acquisizione del pacchetto - La richiesta ha ricevuto una risposta.

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) l=19 val=meraki_8021x_test
        > Type: 1
        > Length: 19
        > User-Name: meraki_8021x_test
      > AVP: t=NAS-IP-Address(4) l=6 val=6.254.243.86
      > AVP: t=Calling-Station-Id(31) l=19 val=02-00-00-00-00-01
      > AVP: t=Framed-MTU(12) l=6 val=1400
      > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
      > AVP: t=Service-Type(6) l=6 val=Framed(2)
      > AVP: t=Connect-Info(77) l=24 val=CONNECT 11Mbps 802.11b
      > AVP: t=EAP-Message(79) l=24 Last Segment[1]
  
```

Verifica configurazione criteri di accesso

1. È necessario verificare che il parametro indicato nei criteri di accesso sia corretto e includa l'indirizzo IP dell'host, il numero di porta e la chiave privata.

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	<input type="text"/>	1812	⬇️ × Test
2	<input type="text"/>	1812	⬇️ × Test

[Add a server](#)

2. Gli indirizzi IP dei server RADIUS configurati sono fittizi o non vengono utilizzati nella produzione oppure i criteri di accesso non sono in uso. È consigliabile rimuovere i criteri di accesso. Se si desidera mantenerla, è possibile disattivare l'impostazione del test del raggio.

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 testing disabled

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](#)

Informazioni correlate

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- [Documentazione e supporto tecnico – Cisco Systems](#)

Nota

- Quando i server radius eseguono il polling dei dispositivi Meraki usando l'IP LAN e il nome utente predefinito "meraki_8021x_test", il dashboard Meraki ha usato l'indirizzo MAC Meraki come origine.
- Meraki ha dato visibilità a questi allarmi da ottobre 2021.