Porte di prova in Windows e MAC

Sommario

troduzione	
erequisiti	
Requisiti	
Componenti usati	
emesse	
orte di test	
Per Windows	
formazioni correlate	

Introduzione

In questo documento viene descritto come testare le porte del traffico TCP SIP per risolvere i problemi relativi alla presenza di <u>dispositivi supportati per Webex Calling</u>.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comprensione dell'ambiente e dell'architettura Webex Calling
- · Aver letto le informazioni di riferimento sulla porta per Webex Calling
- Risoluzione dei problemi di base relativi al registro dispositivi.
- Esecuzione dello strumento CSCAN Webex Calling offre <u>Utilizzo di CScan per verificare la</u> <u>qualità della rete Webex Calling</u>

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.

Premesse

In questo documento viene descritto un modo di base per risolvere i problemi e verificare se si ha accesso alle porte SIP (Signaling Session Initiation Protocol) di Webex.

In alcuni casi, i dispositivi non vengono registrati e viene visualizzato lo stato offline o dei problemi in Control Hub.

È necessaria un'acquisizione di pacchetti per poter verificare se il dispositivo deve registrare il flusso SIP previsto:



In un'acquisizione pacchetto, se riuscita, appare simile all'immagine successiva:

No	Time	< Storme	Destination	Pentocol	Inda
	310 2023-03-08 17:46:43.063779	10.21.144.144	199.59.66.120		56059 - 8034 (51N) Seque Win+65535 Lenve M55+1350 W5+64 T5val+2164988443 TSecr+0 SACK_PERM+1
	312 2023-03-08 17:46:43.203038	199.59.66.120	10.21.144.144	TCP	8934 - 56959 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1260 SACK_PERM=1 TSval=3981094889 TSecr=2164900443 WS=4
	313 2023-03-08 17:46:43.203115	10.21.144.144	199.59.66.120	TCP	56959 - 8934 [ACK] Seg-1 Ack=1 Win=132288 Len=0 TSval=2164980583 TSecr=3981894889
	314 2023-03-08 17:46:43.205513	10.21.144.144	199.59.66.120	TLSv1.2	Client Hello
	316 2023-03-08 17:46:43.329379	199.59.66.120	10.21.144.144	TCP	8934 - 56959 [ACK] Seq=1 Ack=518 Win=30032 Len=0 TSval=3901094950 TSecr=2164900505
	318 2023-03-08 17:46:43.331761	199.59.66.120	10.21.144.144	TLSv1.2	Server Hello

La casella rossa indica che la connessione TCP è stata stabilita.

Nell'immagine seguente viene mostrato un esempio di connessione TCP non stabilita:

•••				extendedlogging.pcap					
🖪 🔳 🔏 🔘 🖿 🗎 🕅 🔀 🦉 ୍	🔄 🔿 🔤 🐻 🕹 🔲	🔲 ବ୍ର୍ର୍ 🛄		Mail Password Regimed					
				🥌 internet Accounts.					
tcp.portime#34									
eo. Time	Source	Destnation	Protocol Inf						
- 103 2023-03-07 10130122,763274	10.03.207.223	199.39.00.124	TCP	3333 - 8934 (31%) Segre Win-27486 Letter P03-1466 3AUL/PDM-1 T548(-3346538/8 T3467-8 KS-128					
	10.03.247.223	199.39.00.110	10	[ICP RETRASKISSION] [ICP PUTE NUMBERS REUSED] 33233 + 0034 [STRI] SEGRE REMERSSHARE SACK_PERMIT ISVALISSHBALIR ISECT					
518 2025-03-07 10150125-029730	10.03.207.223	199.39.00.120	TCP	(TCP Netrationission) (TCP Pert tembers result) 33233 + 8934 (SNR) Seq.4 Mil-29248 Lenve RSS-1446 SAC, PENPA TSVL-SS46464 ESEC+4					
	10.03.247.223	199.39.00.110	107	[ICP RETRASKISSION] [ICP Part NUMBERS reused] 33233 * 0334 [STRI] Septe NUM-SY200 Lenve PSS=1400 SACK_PENNAL (Systems)44050400044 [Sterre					
009 2023-03-07 10130130.11/740	14.63.247.223	199.39.00.124	107	(TCP Retrainmission) (TCP Pert Numbers Febred) 33233 - 8034 (STN) Sed-# Min-2228 Len-# PSS-1488 SAC_PERM+1 TSV81-SS4867712 TSECF					
874 2023-03-07 10130142-149311	10.03.247.223	199.59.00.110	10	33421 = 0334 [378] Segre Kin-Syde Lene RSS-1000 SxX, (12941 [3481-354000713 [360148 KS-120					
922 2023-03-07 10130143-173771	10.03.207.223	199.39.00.120	TCP	(TCP Retrainings100) (TCP Pert numbers result) 3542 + 8034 (SNR) See-4 Min-2228 Lenve RSS-1446 SAC, PERH-1 TSVL-SS408076 TSEC-4					
970 2023-03-07 10:30:43.109/04	10.03.247.223	199.39.00.110	107	[TCP RETRASKISSION] [TCP PUT NUMBERS reused] 35421 + 0004 [STM] Septe Min-Syze Lenve PSS-1440 SACK_PENH1 (SVA1+5)-4809440 [SECTH					
1131 2023-03-07 10130149-301710	10.03.207.223	199.39.00.120	TCP	(TCP Retrainings100) (TCP Pert numbers result) 3542 + 4034 (SNR) See-4 Min-2228 Lenve RSS-1446 SAC, PERH-1 TSV1-SS407028 TSEC+4					
	10.03.247.223	199.39.00.110	107	[TCP RETransmission] [TCP Port numbers reused] 33233 + 0004 [STM] Septe Min-Syze Lenve PSS-1448 SACK_PENH1 (SVA1+354871744 [Sect-					
1332 2023-03-07 10130137-373740	10.03.207.223	199.39.00.120	107	[TCP Retrainsission] [TCP Fort numbers reside) 35421 + 8934 [SIN] Seg-# Min-2228 Lenve RSS-1488 SACK_FERM+1 TSV81-954872576 TSECF					
1414 2023-03-07 10:59102.140100	10.03.247.223	199.59.00.110	10	-6139 - 6334 [318] Segre Kin-Stee Level RS-1466 SKX, (200-1 [3val-3548/3713 [3et/re K5-128					
1487 2023-03-07 10139103.173731	10.03.207.223	199.39.00.120	TCP	(TCP Retraininission) (TCP Port numbers reused) 40199 + 4034 (SNR) Seq-4 Min-2220 Lenve RSS-1446 SAC, PERMA TSVA1-SS403976 TSEC-4					
1531 2023-03-07 10:59:05.109733	10.63.247.223	199.59.60.120	TUP	[TCP Retraismission] [TCP Part numbers reused] 40199 - 8934 [SNN] See-8 Min-29208 Lenve MSS-1468 SACK_PINH-1 TSv1-554874488 TSecre					
1632 2023-03-07 16159109-349720	10.03.247.223	199.39.00.120	TUP	[TCP Retransmission] [TCP Port numbers reused] 40199 + 8934 [STN] Seq+8 Min-29288 Len+8 MSS=1448 SACK_PER+1 TSys1+354875528 TSecr+					
1777 2023-03-07 10:59:13.701733	10.63.247.223	199.59.00.120	102	[TCP Retransmission] [TCP Port numbers reused] 35421 + 8934 [STN] Seq-8 Min-29288 Lenve RSs-1448 SACK_PERH-1 Tsva1-55487688 Tsecre-					
1830 2023-03-07 10139117-341733	10.03.247.223	199.39.00.120	107	[TCP Retransmission] [TCP Port numbers reused] 40199 + 8934 [STN] Seq+8 Min+29288 Len+8 MSS=1488 SACK_PENH+1 TSys1+354877588 TSecre					
1835 2023-03-07 10:59:22.630363	10.63.247.223	199.59.65.120	100	36213 - 8934 (SYN) Seque Win-29288 Lenve RSS=1468 SACK PIRM=1 TSval=S54878848 TSecree WS=128					
2099 2023-03-07 10159123-053727	10.03.247.223	199.39.63.120	TUP	[TCP Retransmission] [TCP Port numbers reused] 36213 + 8934 [STN] Seq+8 Min-29288 Len+8 MSS=1468 SACK_PER+1 TSys1+354879896 [Secre					
2994 2023-03-07 16:59:25.669770	10.63.247.223	199.59.65.120	TOP	[TCP Retransmission] TCP Fort numbers reused] 3623 - 8034 [StN] Sep-0 Win-20200 Lenve MSS-1468 SACK_PERH-1 TSval-654479600 TSecre					
- 3016 2023-03-07 16159127.269726	10.63.247.223	199.59.60.120	TCP	[TCP Retransmission] [TCP Port numbers reused] 33253 + 8934 [SIN] Seq=0 Min=29200 Len+0 MSS=1448 SACK_PERM+1 TSval=S54800000 TSecr=					
3119 2023-03-07 16:59:29.829718	10.63.247.223	199.59.65.120	10	[TCP Retransmission] [TCP Port numbers reused] 36213 - 8934 [STN] Seq=8 Win-29288 Len=8 MSS-1468 SACK_PERM-1 TSval-SS4888648 TSecr=					
3212 2023-03-07 16159133.669739	10.63.247.223	199.59.60.120	TCP	(TCP Retransmission) (TCP Port numbers reused) 46199 - 8934 (SYN) Sequé Win-29208 Lenvé MSS-1468 SACK_PERM+1 TSval-SS4881688 TSecr-					
7 Frame 165: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)									
Ethernet II, Src: Cisco_9b:3e:ff (4c:e1:76:9	bi3eiff), Dsti IETF-WRRP-VR	ID_bc (00:00:5e:00:01:bc)							

In questo caso, sull'acquisizione viene visualizzata solo la sintassi TCP SYN, quindi il dispositivo non è in grado di aprire la connessione TCP.

Nota: quando si incontra questo tipo di problema, è necessario indagare perché questo è bloccato. In alcuni casi, è bloccato sul lato firewall, tuttavia è necessario eseguire ulteriori indagini.

È possibile eseguire alcune operazioni per convalidare le connessioni TCP da Windows/MAC.

Porte di test

Per Windows

Aprire Power Shell e utilizzare i seguenti comandi:

tnc 10.119.57.136 -p 8934 tnc 10.119.56.136 -p 8934

Inoltre, utilizzare ipconfig per controllare l'origine:

```
Windows PowerShell

Vindows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\^''- ''> tnc 85.119.57.136 -p 8934

ComputerName : 85.119.57.136

RemoteAddress : 85.119.57.136

RemotePort : 8934

InterfaceAlias : Wi-Fi

SourceAddress : 10.152.200.59

TcpTestSucceeded : True

PS C:\Users\''' tnc 85.119.56.136 -p 8934

ComputerName : 85.119.56.136

RemoteAddress : 85.119.56.136

RemoteAddress : 85.119.56.136

RemoteAddress : 85.119.56.136

RemoteAddress : 10.152.200.59

InterfaceAlias : Wi-Fi

SourceAddress : 10.152.200.59

InterfaceAlias : Wi-Fi

SourceAddress : 10.152.200.59

TcpTestSucceeded : True
```

Nota: gli indirizzi IP mostrati qui sono Webex Calling Session Border Controller (SBC).

Andare al terminale e usare i comandi successivi:

nmap -sV -p 8934 10.119.57.136 nmap -sV -p 8934 10.119.56.136

Inoltre, utilizzare ipconfig per controllare l'origine:

10

Informazioni correlate

- Usa CScan per verificare la qualità della rete di chiamate Webex
- Supporto tecnico Cisco e download

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).