Problemen oplossen TelePresence Endpoint dat aan TMS wordt toegevoegd door automatisch de firewallstatus te wijzigen

Inhoud

Inleiding

Dit document beschrijft hoe u het IP-adres kunt isoleren dat pakketten naar de TelePresence Management Server (TMS) uit naam van het endpointgebeurtenissen verstopt waardoor het probleem wordt veroorzaakt. Wanneer een beheerd apparaat aan TMS wordt toegevoegd, toont de status ervan in de standaardinstelling Reachable op LAN iets echter na een tijdje dat de status kan veranderen in Achter de Firewall. Dit gebeurt over het algemeen wanneer pakketten die van apparaat worden ontvangen een bron IP adres anders hebben dan het systeem IP adres dat van de status van het apparaat door TMS wordt ontvangen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco TelePresence Endpoint runk TC-software (TelePresence Codec) voor MXP
- TMS

Gebruikte component

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

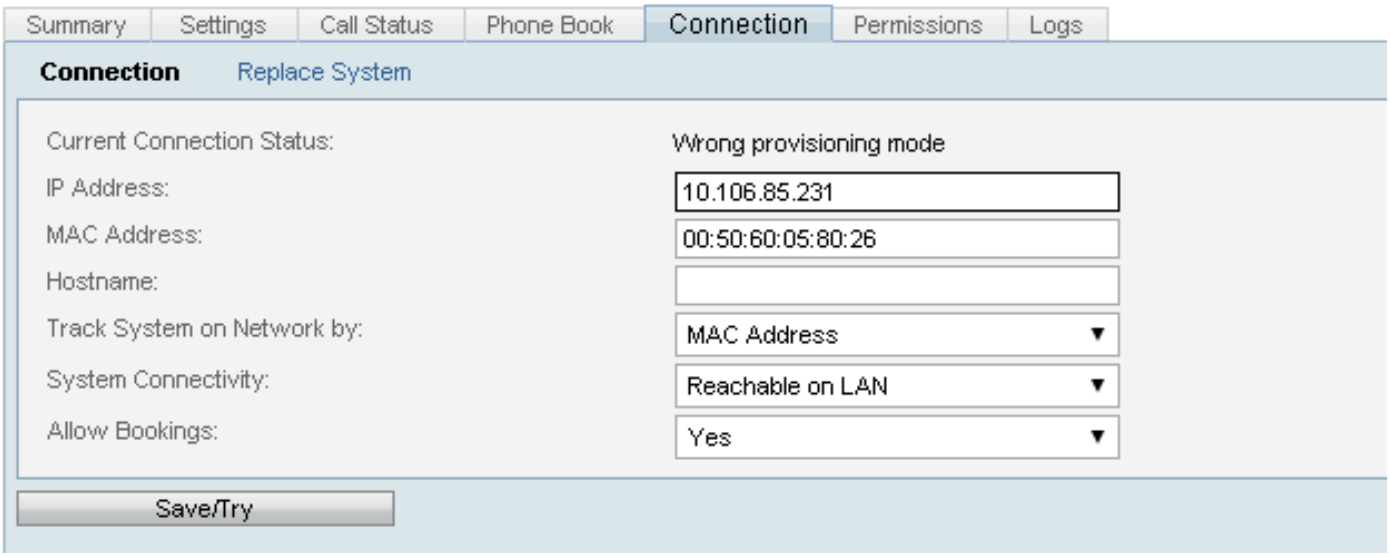
Probleem

Endpoints die worden beheerd door TMS veranderen van Reachable on LAN status automatisch in Behind de firewallstatus, waardoor de TMS het beheer van het apparaat moet stoppen. Er wordt vanuit gegaan dat u om een probleemoplossing te kunnen oplossen een HTTP-communicatie moet hebben die in het netwerk tussen het beheerde apparaat en de TMS is toegestaan.

Problemen oplossen

Om een pakketvastlegging van de TMS te kunnen controleren is het volgende vereist:

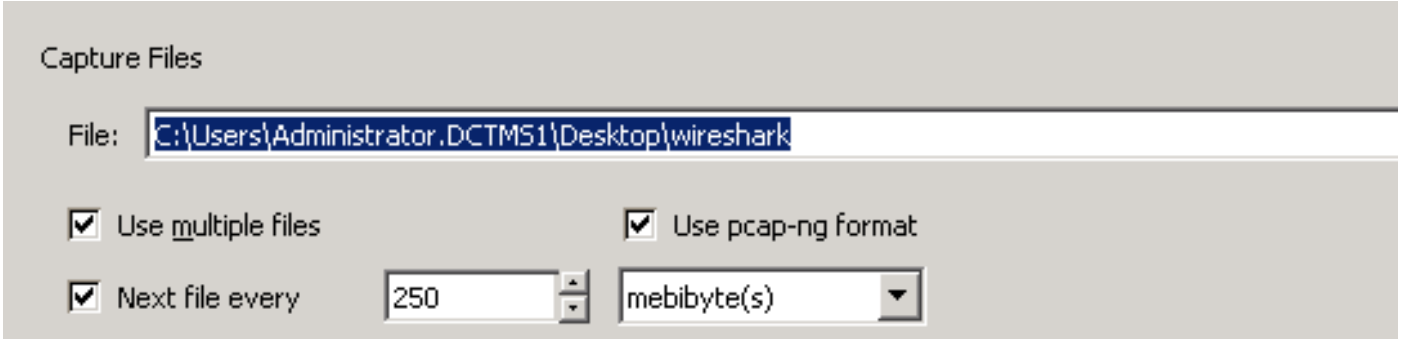
1. Connect met TMS-server via Remote Desktop Protocol (RDP).
2. Zorg ervoor dat TMS en endpointgebeurtenissen HTTP-communicatie ingeschakeld zijn en dat HTTPS uitgeschakeld is.
3. Installeer/voer Wireless-haai en selecteer de standaardnetwerkinterface.
4. Gebruik geen filter en start de opname.
5. Navigeer naar het tabblad Connection van het eindpunt waarmee u een probleem hebt, klikt u op de knop **Opslaan/proberen** zoals in deze afbeelding.



6. Wanneer het eindpunt terugvalt naar achter de firewall, stop de vangst van haaien.

> **Opmerking:** Soms duurt het langer dan verwacht. Om vandaar opnieuw te creëren terwijl u de Wireless-shark opname start, moet u ervoor zorgen dat u in meerdere bestanden opslaat.

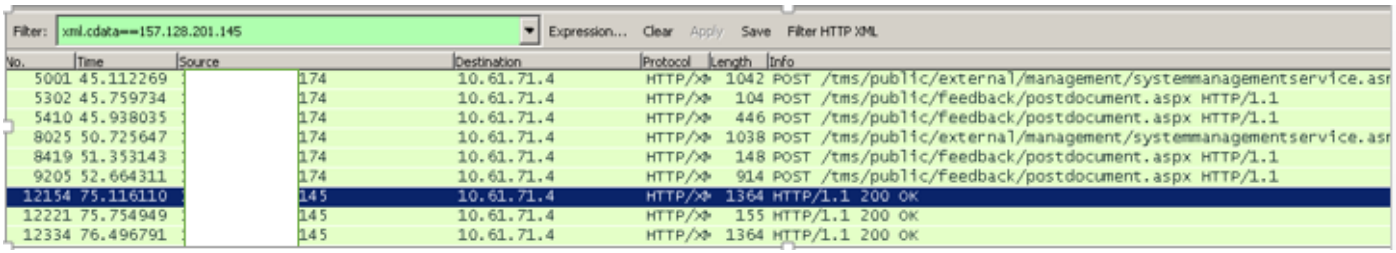
7. Ga naar **Opname bestand** en selecteer de optie **Meerdere bestanden gebruiken**.



Open Wireshark

- Filter toepassen zoals xml.cdata ==IP_ADDRESS_OF_DEVICE
- Na het toepassen van dit filter zou je kunnen zien dat de respons zal veranderen van het feitelijke ip-adres van het apparaat in een ander verschillend ip-adres.

Zoals in deze afbeelding wordt getoond, is het werkelijke IP-adres van het apparaat x.x.x.174; later verandert dit IP echter in x.x.x.145



Vanwege verandering van dit IP-adres verifieert TMS dat het IP-adres van het apparaat dat in xstatus wordt verzonden niet hetzelfde is als het IP-adres in de IP-header en verandert het apparaat dus in Achter de firewallstatus.

Oplossing

Om dit probleem op te lossen moet u ervoor zorgen dat er geen apparaat in het netwerk tussen het Endpoint en TMS is dat het bron IP-adres in de IP-header verandert. Daardoor zal de bron IP in de IP-header anders zijn dan de huidige IP-telefoon met dit eindpunt.