

Dépannage automatique du point de terminaison TelePresence ajouté au TMS et passant à l'état Derrière le pare-feu

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composant utilisé](#)

[Problème](#)

[Dépannage](#)

[Solution](#)

Introduction

Ce document décrit comment isoler l'adresse IP qui envoie des paquets au serveur de gestion de téléprésence (TMS) pour le compte du terminal, causant le problème. Lorsqu'un périphérique géré est ajouté au TMS, son état indique Reachable on LAN par défaut pour un certain temps, mais après un certain temps, l'état peut changer pour Derrière le pare-feu. Cela se produit généralement lorsque les paquets reçus du périphérique ont une adresse IP source différente de l'adresse IP du système qui est reçue du xstatus du périphérique par le TMS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Terminal Cisco TelePresence exécutant le logiciel TC (Telepresence Codec) ou MXP
- TMS

Composant utilisé

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. If your network is live, make sure that you understand the potential impact of any command.

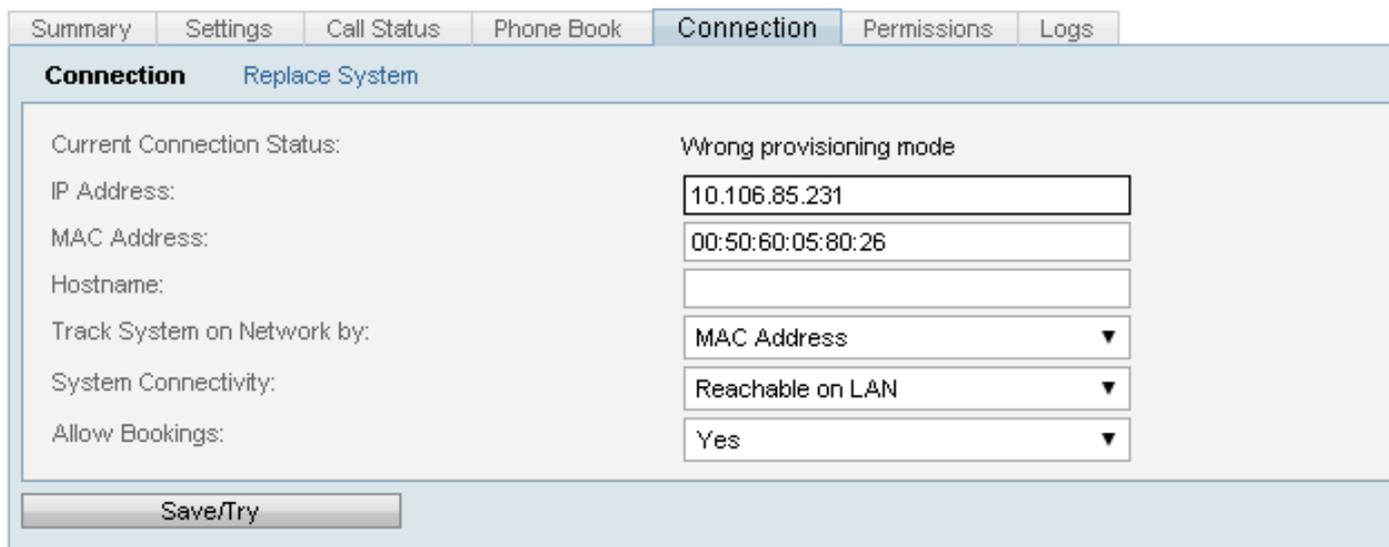
Problème

Les terminaux gérés par le TMS passent automatiquement de l'état Accessible sur le LAN à l'état Derrière le pare-feu, ce qui entraîne l'arrêt de la gestion du périphérique par le TMS. Il est considéré que pour effectuer le dépannage, vous devez disposer d'une communication HTTP autorisée sur le réseau entre le périphérique géré et le TMS.

Dépannage

Afin de vérifier qu'une capture de paquet à partir du TMS est nécessaire :

1. Se connecter au serveur TMS via le protocole RDP (Remote Desktop Protocol).
2. Assurez-vous que la communication HTTP est activée pour TMS et le point d'extrémité et que HTTPS est désactivé.
3. Installez/exécutez Wireshark et sélectionnez l'interface réseau par défaut.
4. N'appliquez aucun filtre et démarrez la capture.
5. Accédez à l'onglet Connexion du point de terminaison avec lequel vous êtes confronté à un problème, cliquez sur le bouton Enregistrer/Essayer comme illustré dans cette image.

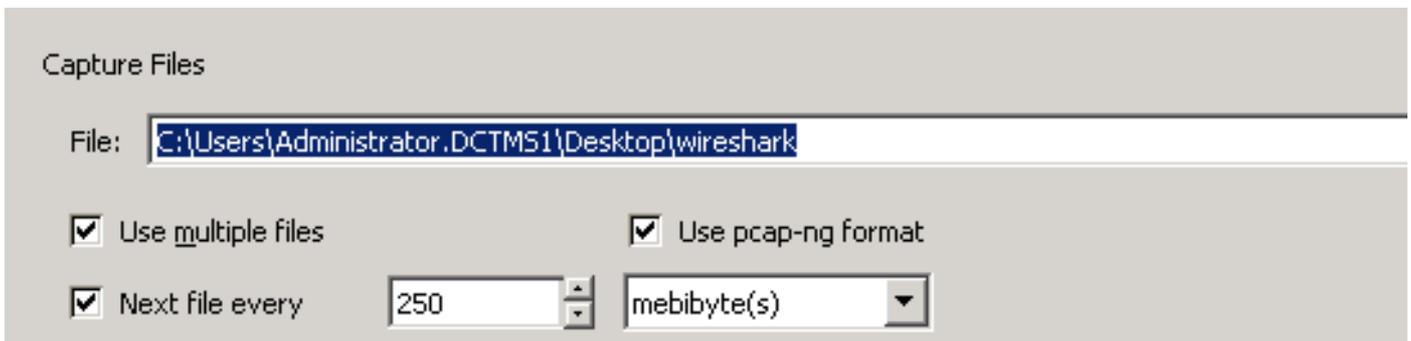


Summary	Settings	Call Status	Phone Book	Connection	Permissions	Logs
Connection Replace System						
Current Connection Status:		Wrong provisioning mode				
IP Address:	<input type="text" value="10.106.85.231"/>					
MAC Address:	<input type="text" value="00:50:60:05:80:26"/>					
Hostname:	<input type="text"/>					
Track System on Network by:	MAC Address ▼					
System Connectivity:	Reachable on LAN ▼					
Allow Bookings:	Yes ▼					
<input type="button" value="Save/Try"/>						

6. Lorsque le point d'extrémité revient derrière le pare-feu, arrêtez la capture Wireshark.

 Remarque : parfois, le problème peut prendre plus de temps que prévu. Pour recréer par conséquent lors du démarrage de la capture Wireshark, assurez-vous d'enregistrer dans plusieurs fichiers.

7. Allez à Capture File option et activez la case à cocher Utiliser plusieurs fichiers.



Ouvrez Wireshark

- Appliquez un filtre tel que `xml.cdata == IP_ADDRESS_OF_DEVICE`
- Après avoir appliqué ce filtre, vous verrez peut-être que la réponse passe de l'adresse IP réelle du périphérique à une autre adresse IP.

Comme l'illustre cette image, l'adresse IP réelle du périphérique est x.x.x.174 ; toutefois, cette adresse IP devient plus tard x.x.x.145

No.	Time	Source	Destination	Protocol	Length	Info
5001	45.112269	174	10.61.71.4	HTTP/1.1	1042	POST /tms/public/external/management/systemmanagementservice.asr
5302	45.759734	174	10.61.71.4	HTTP/1.1	104	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
5410	45.938035	174	10.61.71.4	HTTP/1.1	446	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
8025	50.725647	174	10.61.71.4	HTTP/1.1	1038	POST /tms/public/external/management/systemmanagementservice.asr
8419	51.353143	174	10.61.71.4	HTTP/1.1	148	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
9205	52.664311	174	10.61.71.4	HTTP/1.1	914	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
12154	75.116110	145	10.61.71.4	HTTP/1.1	1364	HTTP/1.1 200 OK
12221	75.754949	145	10.61.71.4	HTTP/1.1	155	HTTP/1.1 200 OK
12334	76.496791	145	10.61.71.4	HTTP/1.1	1364	HTTP/1.1 200 OK

En raison de la modification de cette adresse IP, le TMS vérifie que l'adresse IP du périphérique envoyée dans `xstatus` n'est pas la même que l'adresse IP dans l'en-tête IP et par conséquent il change le périphérique en Derrière l'état du pare-feu.

Solution

Pour résoudre ce problème, vous devez vous assurer qu'aucun périphérique du réseau entre le terminal et le TMS ne modifie l'adresse IP source dans l'en-tête IP, ce qui entraîne une différence entre l'adresse IP source dans l'en-tête IP et l'adresse IP réelle du terminal.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.