TLS-handdrukfout op VCS-webinterface

Inhoud

Inleiding

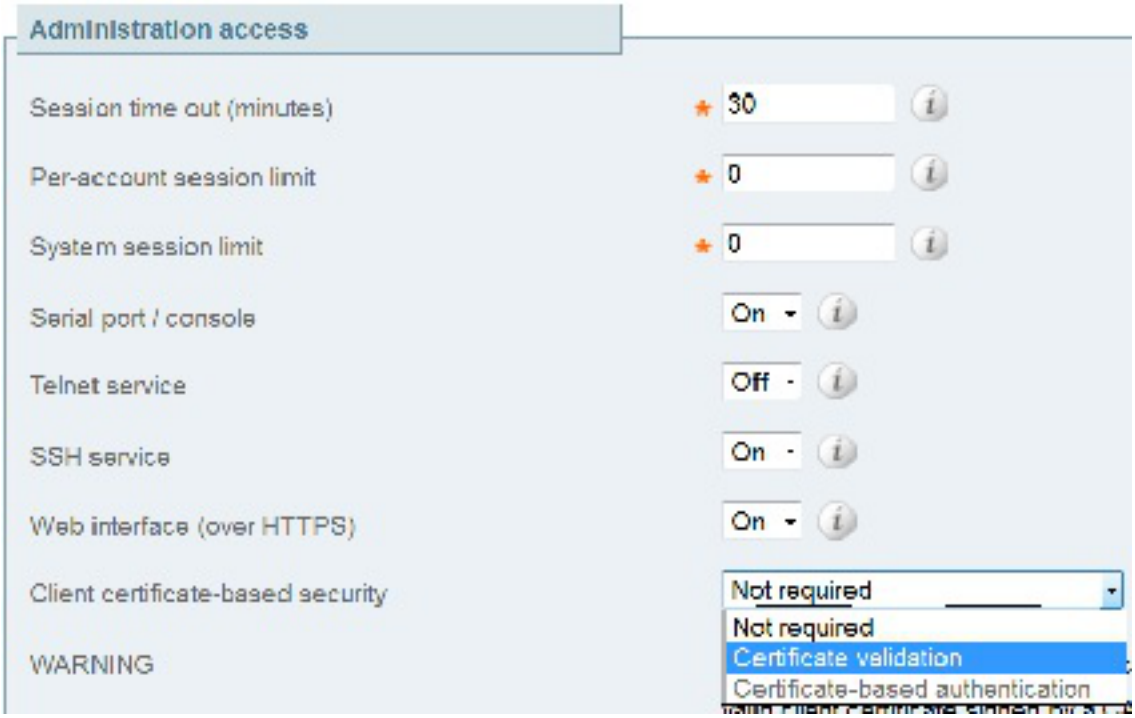
Cisco Video Communication Server (VCS) gebruikt clientcertificaten voor de verificatie en autorisatie. Deze optie is zeer nuttig voor bepaalde omgevingen, omdat het een extra veiligheidslaag toestaat en kan worden gebruikt voor enkel teken op doeleinden. Indien echter niet correct geconfigureerd, kan dit beheerders uit de VCS-webinterface uitsluiten.

De stappen in dit document worden gebruikt om de op client gebaseerde beveiliging van Cisco VCS uit te schakelen.

Probleem

Als de op het clientcertificaat gebaseerde beveiliging op een VCS is ingeschakeld en onjuist is geconfigureerd, kunnen gebruikers mogelijk geen toegang krijgen tot de VCS-webinterface. Pogingen om toegang te krijgen tot de webinterface worden gedaan met een fout in de TLS-handdruk (Transport Layer Security).

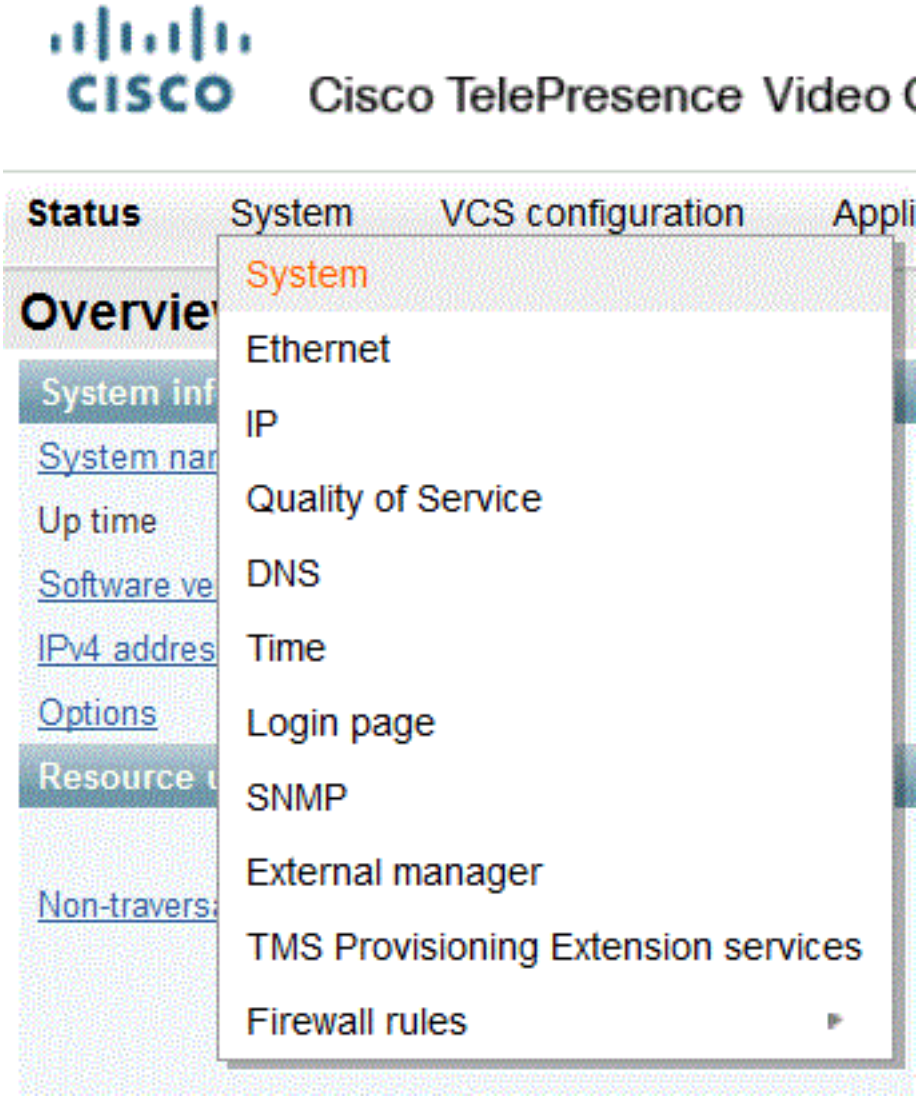
Dit is de configuratie verandering die de kwestie veroorzaakt:



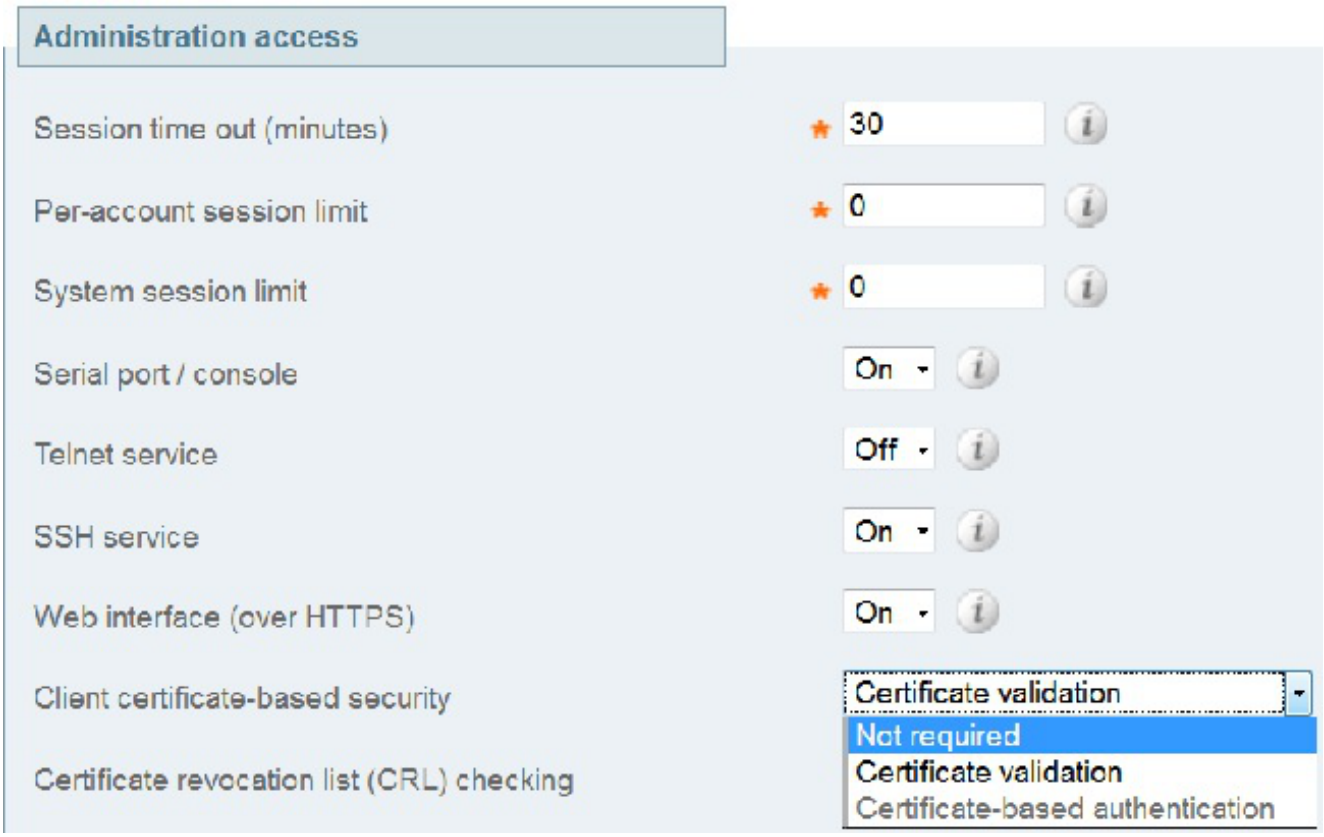
Oplossing

Voltooi deze stappen om de beveiliging van clientcertificaten uit te schakelen en het systeem terug te sturen naar een staat waar beheerders toegang hebben tot de web interface van de VCS:

1. Connect met het VCS als wortel via Secure Shell (SSH).
2. Typ deze opdracht als wortel in om Apache met harde code te coderen zodat u nooit op client gebaseerde beveiliging kunt gebruiken:
   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   Opmerking: Nadat deze opdracht is ingevoerd, kan de VCS niet opnieuw worden geconfigureerd voor clientbeveiliging totdat het bestand **removecba.conf** is verwijderd en de VCS opnieuw is gestart.
3. U moet de VCS opnieuw opstarten om deze configuratie te kunnen wijzigen. Wanneer u klaar bent om de VCS opnieuw te starten, voert u deze opdrachten in:
   ```
   tshell
   xcommand restart
   ```
   Opmerking: Hiermee start u de VCS opnieuw en laat u alle oproepen/registraties vallen.
4. Zodra de VCS opnieuw is geladen, is de op het certificaat van de client gebaseerde beveiliging uitgeschakeld. Het wordt echter niet op een gewenste manier gehandicapt. Meld u aan bij de VCS met een admin-account voor het lezen. Navigeer naar **System > System pagina** op de VCS.



Zorg er op de systeembeheerpagina van de VCS voor dat de beveiliging van het clientcertificaat is ingesteld op "Not Requirements":



Nadat deze wijziging is aangebracht, slaat u de wijzigingen op.

5. Voer deze opdracht na voltooiing in als wortel in SSH om Apache weer normaal te maken:
   `rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf`
   Waarschuwing: Als u deze stap overslaat, kunt u de beveiliging van het clientcertificaat nooit meer inschakelen.
6. Start de VCS nogmaals om na te gaan of de procedure heeft gewerkt. Nu u toegang tot het web hebt, kunt u de VCS vanaf de webinterface opnieuw opstarten onder **Onderhoud > Start**.

Gefeliciteerd! Uw VCS werkt nu met op client gebaseerde security uitgeschakeld.