

# Contenido

[Introducción](#)

[Problema](#)

[Solución 1](#)

[Solución 2](#)

## Introducción

Este documento describe una situación que pudo ocurrir donde está incapaz el Unity Connection de agregar un dispositivo de backup del sistema de la Recuperación tras desastres (DR) porque la opción es grayed hacia fuera. Esto puede también ocurrir en el suscriptor del cluster del Unity Connection también.

Otro síntoma pudo ser cuando ocurre un respaldo DR, usted considera el respaldo de los elementos en el suscriptor fallar.

## Problema

El Unity Connection no puede agregar un dispositivo de backup DR.

### [Solución 1](#)

Para resolver problemas este problema, realice estos pasos:

1. En el Unity Connection Publisher, navegue al **> Security (Seguridad) OS Admin > al mgmt > al hallazgo > a ipsec.pem > a la descarga del certificado al PC.**
2. Navegue al **suscriptor a la página de la administración de certificados.**
3. Borre el certificado de confianza del IPsec para Publisher en el servidor del suscriptor.
4. Cargue el certificado descargado de Publisher como confianza del IPsec.
5. Recomience el agente principal (MA) y al agente local (LA).

### **Solución 2**

Si la solución 1 no soluciona el problema, usted puede ser que tenga un problema con el certificado del IPsec en Publisher. Si es así usted necesita regenerar el certificado en Publisher, y después borra la confianza que existe del suscriptor. Para copiar el nuevo certificado del IPsec de Publisher como confianza del IPsec, realice estos pasos:

1. Inicie sesión a la página de administración del administrador OS de las Comunicaciones unificadas de Cisco.
2. Elija el **Certificate Management (Administración de certificados) de la Seguridad.** Las visualizaciones de la ventana de la lista del certificado.

3. Utilice el hallazgo controla para filtrar la lista del certificado.
  4. Elija el **archivo ipsec.pem**, y haga clic el regenerado.
  5. Después de que la regeneración acertada del archivo ipsec.pem, descargue el archivo ipsec.pem a su ordenador.
  6. Vuelva a la página de la administración de certificados.
  7. Encuentre la entrada de archivo corrompida existente de la confianza del IPSec. Elija el nombre del archivo del certificado (CTL), y haga clic la **cancelación**. Refiera a la **cancelación un certificado** para más información.
  8. Cargue el **archivo** descargado **ipsec.pem** con el título "IPSec-confianza".
  9. Recomience el MA y el LA.
- Este problema se pudo relacionar con el Id. de bug Cisco CSCts01090.