

# Conexión del Unity incapaz de agregar un dispositivo de backup DRS

## Contenido

[Introducción](#)

[Problema](#)

[Solución 1](#)

[Solución 2](#)

## Introducción

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

Otro síntoma pudo ser cuando ocurre una salvaguardia DRS, usted considera la salvaguardia de los items en el suscriptor fallar.

## Problema

La conexión del Unity no puede agregar un dispositivo de backup DRS.

### [Solución 1](#)

Para resolver problemas este problema, realice estos pasos:

1. En el editor de la conexión del Unity, navegue al **> Security (Seguridad) OS Admin > al mgmt > al hallazgo > a ipsec.pem > a la transferencia directa del certificado a la PC.**
2. Navegue al **suscriptor a la página de la Administración de certificado.**
3. Suprima el certificado de confianza de IPsec para el editor en el servidor del suscriptor.
4. Cargue por teletratamiento el certificado descargado del editor como confianza de 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 de IPsec en el editor. Si es así usted necesita regenerar el certificado en el editor, y después suprime la confianza que existe del suscriptor. Para copiar el nuevo certificado de IPsec

del editor como confianza de IPsec, realice estos pasos:

1. Ábrase una sesión a la página de administración OS del encargado 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 **fichero ipsec.pem**, y haga clic el regenerado.
5. Después de la regeneración acertada del fichero ipsec.pem, descargue el fichero ipsec.pem a su ordenador.
6. Vuelva a la página de la Administración de certificado.
7. Encuentre la entrada de archivo corrompida existente de la confianza de 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 por teletratamiento el **fichero** 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 CSCts01090 de Cisco.