La página web de la Recuperación tras desastres es insensible

Contenido

Introducción

Este documento describe que cuando la página web de la Recuperación tras desastres se utiliza para hacer un Unity Connection de reserva y del Restore, allí puede ser problemas. Este artículo cubre una tal situación.

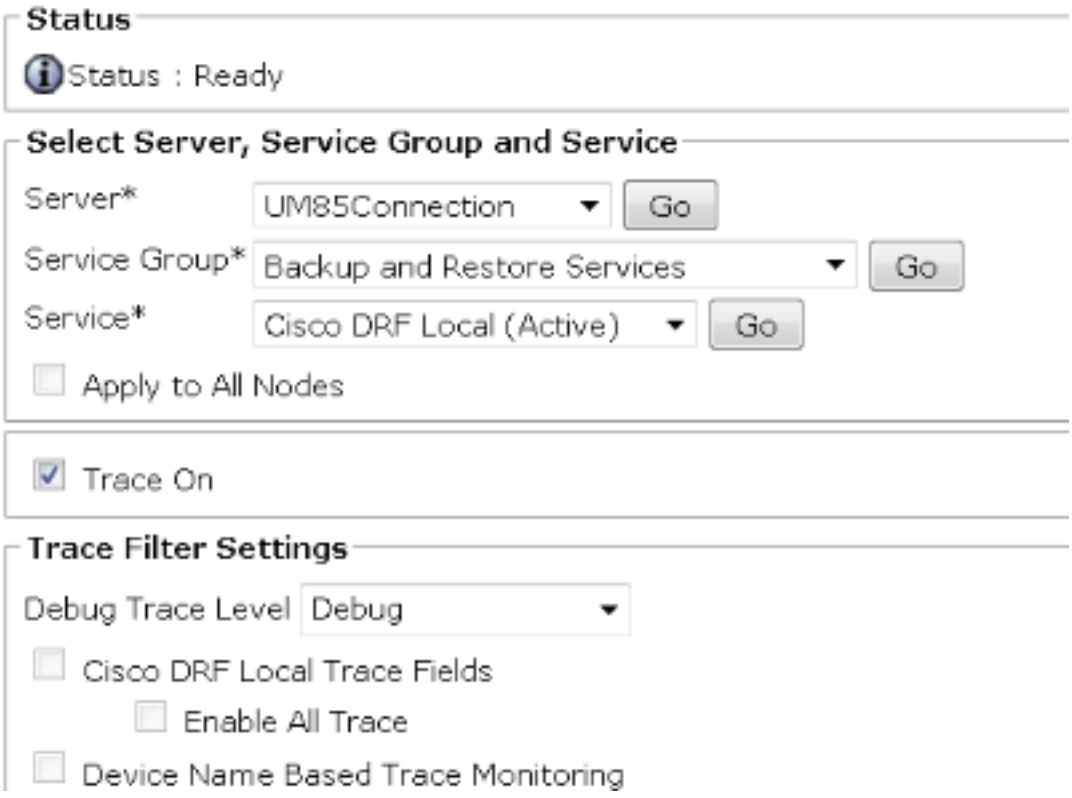
Problema

Cuando usted registra en la página web de la Recuperación tras desastres y hace clic cualquier opción, ningunas páginas cargan.

Troubleshooting

Asegúrese de que el registro de la Recuperación tras desastres esté habilitado y dado vuelta para hacer el debug de.

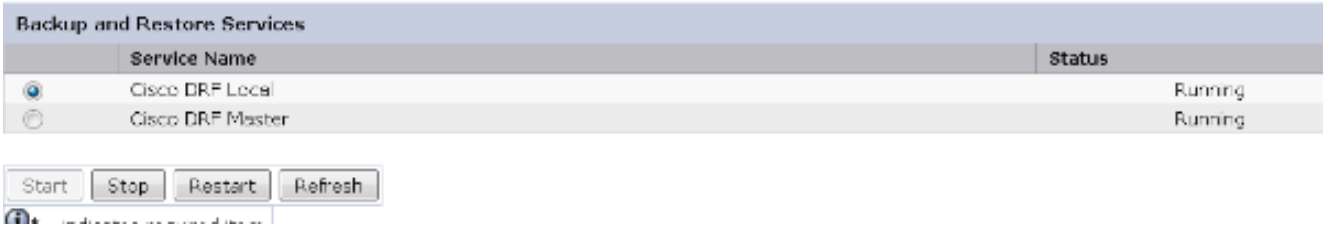
1. Vaya a la página web unificada Cisco de la utilidad.
2. Elija el **Trace > Configuration**.
3. De la lista desplegable de Server*, elija el servidor.
4. De la lista desplegable de Group* del servicio, elija los **servicios de reserva y del Restore**.
5. De la lista desplegable de Service*, elija el **Local de Cisco DRF (activo)**.
6. Asegúrese de que la **traza en la** casilla de verificación esté marcada.
7. De la lista desplegable del nivel de traza del debug, elija el



debug.

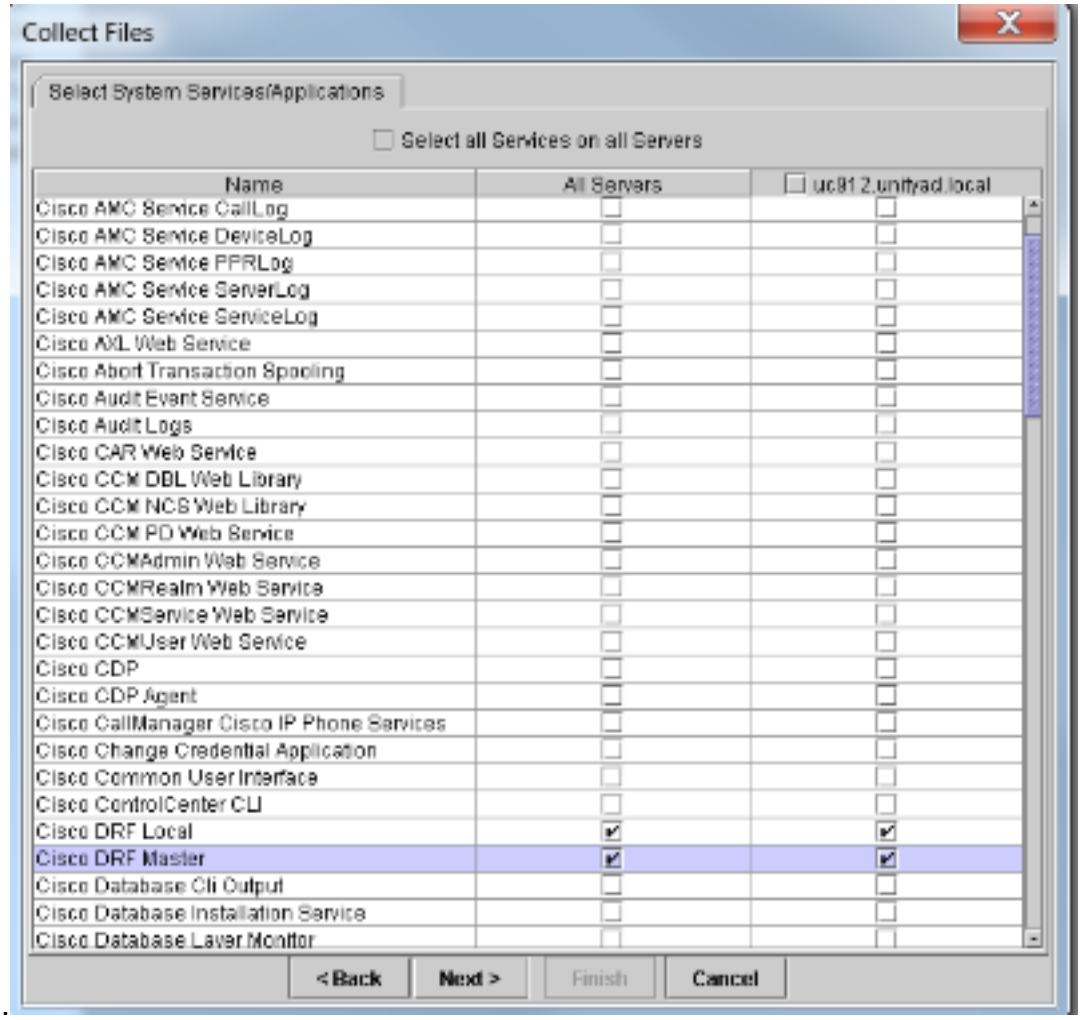
Después, reproduzca el problema. Usted puede ser que necesite recomenzar el master y los servicios locales DRF para conducir una prueba fresca.

1. Elija la utilidad unificada Cisco.
2. Elija el **Tools (Herramientas) > Control Center (Centro de control) - Servicios de red**.
3. Servicios de reserva del hallazgo y del Restore y **Local de Cisco DRF de la** parada y del comienzo y **master de Cisco DRF**.



Entonces utilice la herramienta del monitoreo en tiempo real para recoger las trazas:

1. Vaya a localizar y a registrar la central.
2. Elija **recogen los archivos**.
3. Haga clic **después** para seleccionar los servicios del sistema/las aplicaciones.
4. Marque las casillas de verificación al lado del Local de Cisco DRF y del master de Cisco

DRF. 

5. Haga clic en Next (Siguiente).
6. Fije el rango de tiempo de su prueba y seleccione una ubicación de la descarga.
7. Haga clic en Finish (Finalizar). Esto comienza la colección de registros a la ubicación que usted especificó.

Abajo están los extractos de los registros estén seguros de notar en el master DRF que el registro es el mostrar *incapaz de crear la secuencia de la entrada-salida a la alerta fatal del cliente recibida: Mún certificado*.

La demostración local de los registros DRF:

```
2014-02-10 11:08:15,342 DEBUG [main] - drfNetServerClient.
Reconnect: Sending version id: 9.1.1.10000-11
2014-02-10 11:08:15,382 ERROR [main] - NetworkServerClient::Send failure;
2014-02-10 11:08:15,384 FATAL [NetMessageDispatch] - drfLocalAgent.drfLocal
Worker: Unable to send 'Local Agent' client identifier message to Master Agent.
This may be due to Master or Local Agent being down.
```

La demostración principal de los registros:

```
2014-02-10 11:19:37,844 DEBUG [NetServerWorker] - Validated Client. IP =
10.1.1.1 Hostname = labtest.cisco.com. Request is from a Node within the
Cluster
2014-02-10 11:19:37,844 DEBUG [NetServerWorker] - drfNetServerWorker.drfNet
ServerWorker: Socket Object InpuputStream to be created
2014-02-10 11:19:37,850 ERROR [NetServerWorker] - drfNetServerWorker.drfNet
ServerWorker: Unable to create input/output stream to client Fatal Alert
received: Bad Certificate
```

Solución

En este caso hay un problema con el certificado del IPSec en el servidor y usted necesidad de regenerarla, de borrar el certificado de la IPSec-confianza, y de cargar un nuevo. Complete estos pasos para abordar el problema:

1. Registro sobre la página de administración OS.
2. Elija el **Certificate Management (Administración de certificados) > el hallazgo de la Seguridad**.
3. **El archivo del** tecleo **ipsec.pem y** entonces hace clic el regenerado**.**
4. Después de que la generación acertada del archivo ipsec.pem, descargue el archivo.
5. Vuelva a la página de la administración de certificados.
6. Borre la entrada corrompida corriente de la IPSec-confianza.
7. Cargue el archivo descargado ipsec.pem como IPSec-confianza.
8. Master del reinicio DRF y Local DRF.