La página web de recuperación ante desastres no responde

Contenido

Introducción

Este documento describe que cuando la página web Recuperación ante Desastres se utiliza para realizar una Conexión de Copia de Seguridad y Restauración de Unity, puede haber problemas. Este artículo trata una de esas situaciones.

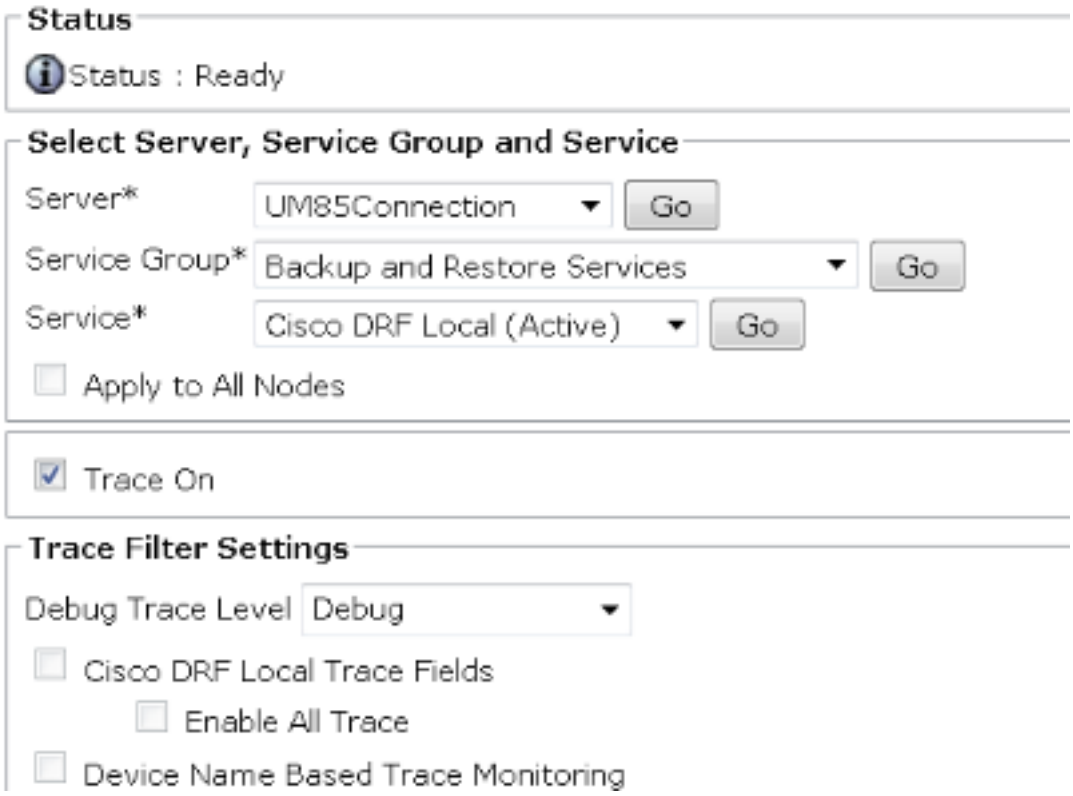
Problema

Cuando inicia sesión en la página web Recuperación ante desastres y hace clic en cualquier opción, no se carga ninguna página.

Troubleshoot

Asegúrese de que el registro de recuperación ante desastres esté habilitado y convertido en Debug.

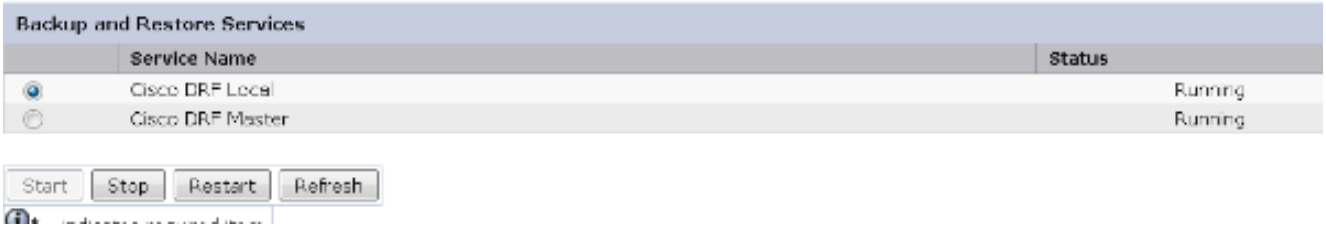
1. Vaya a la página web de Cisco Unified Serviceability.
2. Elija Rastreo > Configuración.
3. En la lista desplegable Servidor*, elija el servidor.
4. En la lista desplegable Service Group*, elija **Backup and Restore Services**.
5. En la lista desplegable Service*, elija **Cisco DRF Local (Activo)**.
6. Asegúrese de que la casilla de verificación **Trace On** esté marcada.
7. En la lista desplegable Debug Trace Level, elija



Debug.

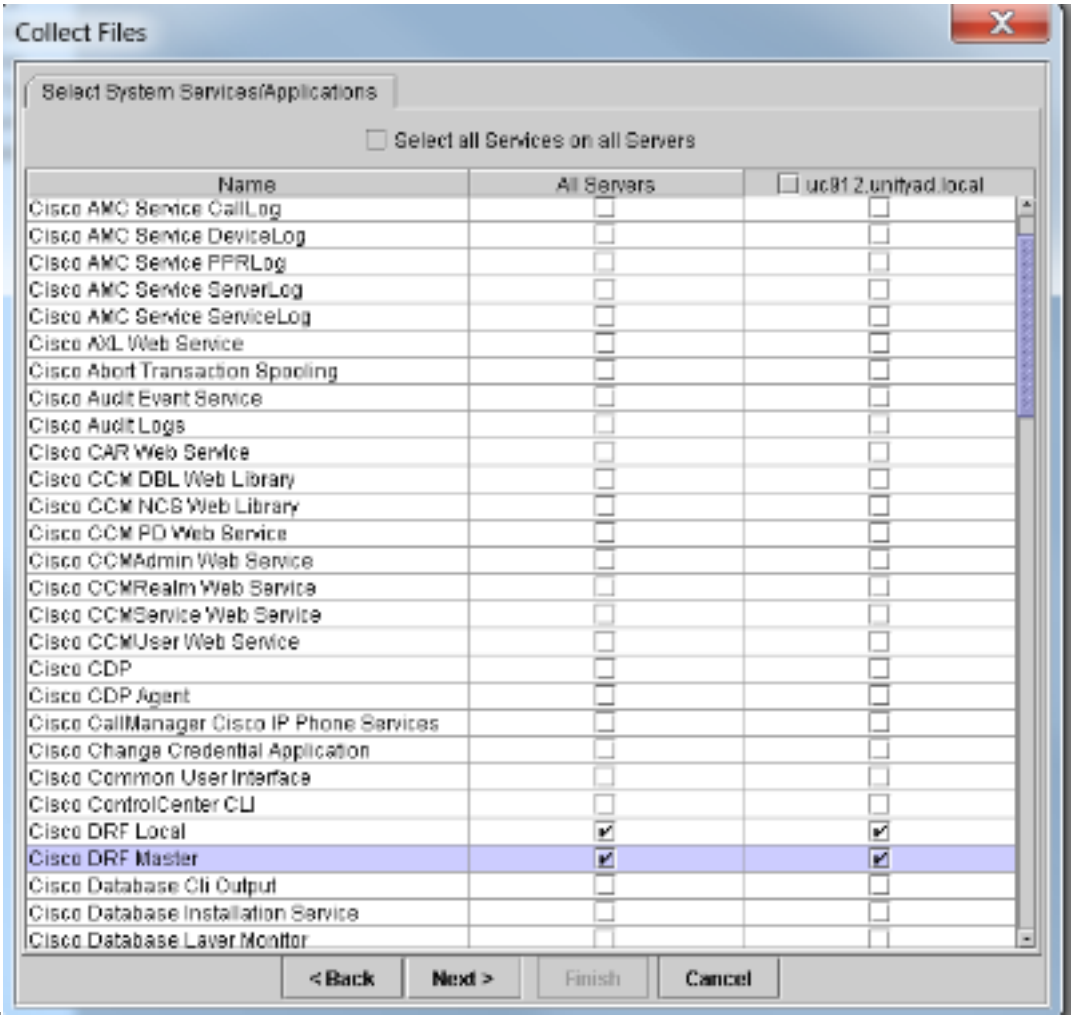
A continuación, reproduzca el problema. Es posible que deba reiniciar el DRF master y los Servicios locales para realizar una nueva prueba.

1. Seleccione Serviciabilidad de Cisco Unified.
2. Elija **Tools > Control Center - Network Services**.
3. Encuentre Servicios de Copia de Seguridad y Restauración y Detenga e Inicie **Cisco DRF Local** y **Cisco DRF Master**.



A continuación, utilice la Herramienta de supervisión en tiempo real para recopilar los seguimientos:

1. Vaya a Trace & Log Central.
2. Elija **Collect Files**.
3. Haga clic en **Next** para seleccionar System Services/Applications.
4. Active ambas casillas de verificación junto a Cisco DRF Local y Cisco DRF

Master. 

5. Haga clic en Next (Siguiente).
6. Establezca el intervalo de tiempo de la prueba y seleccione una ubicación de descarga.
7. Haga clic en Finish (Finalizar). Esto inicia la colección de registros en la ubicación especificada.

A continuación se muestran extractos de los registros asegúrese de que el registro maestro de DRF muestra *No se puede crear el flujo de entrada/salida para la alerta de error del cliente recibida: Certificado incorrecto*.

Los Registros Locales de DRF muestran:

```
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.
```

Los registros maestros muestran:

```
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 IPSec en el servidor y debe regenerarlo, eliminar el certificado ipsec-trust y cargar uno nuevo. Complete estos pasos para abordar el problema:

1. Inicie sesión en la página OS Administration (Administración del sistema operativo).
2. Elija **Security > Certificate Management > find**.
3. Haga clic en **archivo ipsec.pem** y luego haga clic en **regenerar**.
4. Después de la generación correcta del archivo ipsec.pem, descargue el archivo.
5. Vuelva a la página de administración de certificados.
6. Elimine la entrada de ipsec-trust dañada actualmente.
7. Cargue el archivo ipsec.pem descargado como un ipsec-trust.
8. Reinicie DRF Master y DRF Local.