La page Web de reprise après sinistre ne répond pas

Contenu

Introduction

Ce document décrit que lorsque la page Web de récupération d'urgence est utilisée pour créer une connexion Unity de sauvegarde et de restauration, il peut y avoir des problèmes. Cet article traite d'une telle situation.

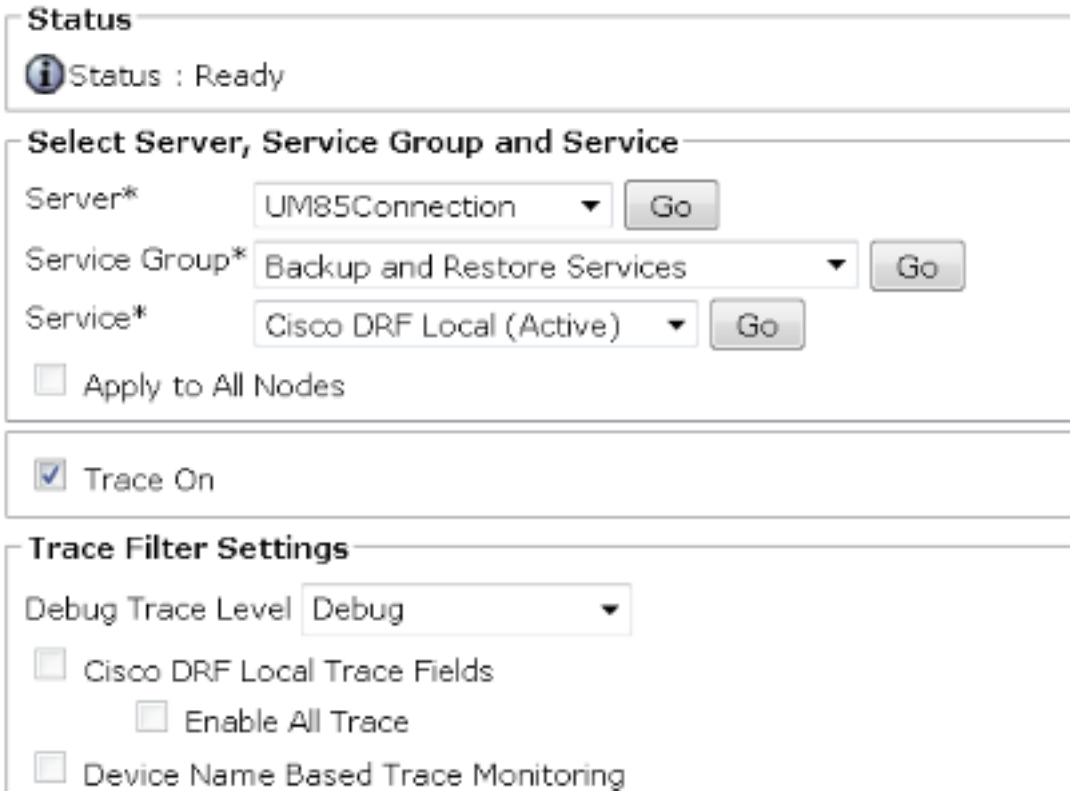
Problème

Lorsque vous vous connectez à la page Web de reprise après sinistre et que vous cliquez sur une option, aucune page ne se charge.

Dépannage

Assurez-vous que la journalisation de la récupération d'urgence est activée et activée sur Débogage.

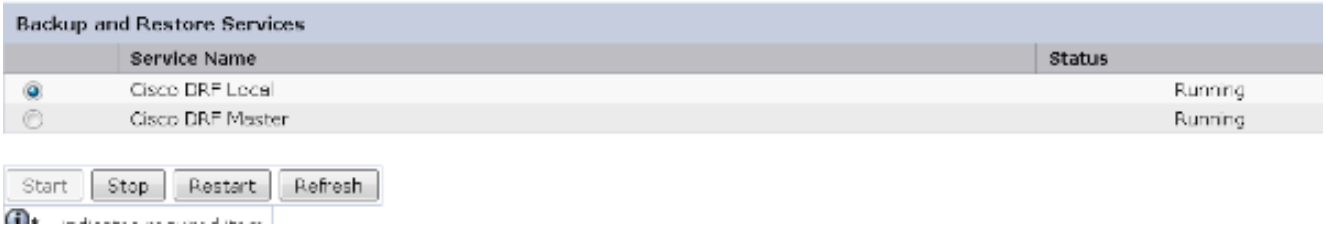
1. Accédez à la page Web Cisco Unified Serviceability.
2. Choisissez Trace > Configuration.
3. Dans la liste déroulante Serveur*, sélectionnez le serveur.
4. Dans la liste déroulante Groupe de services*, sélectionnez **Services de sauvegarde et de restauration**.
5. Dans la liste déroulante Service*, sélectionnez **Cisco DRF Local (Active)**.
6. Assurez-vous que la case **Trace On** est cochée.
7. Dans la liste déroulante Debug Trace Level, sélectionnez



Debug.

Ensuite, reproduisez le problème. Vous devrez peut-être redémarrer le maître DRF et les services locaux pour effectuer un nouveau test.

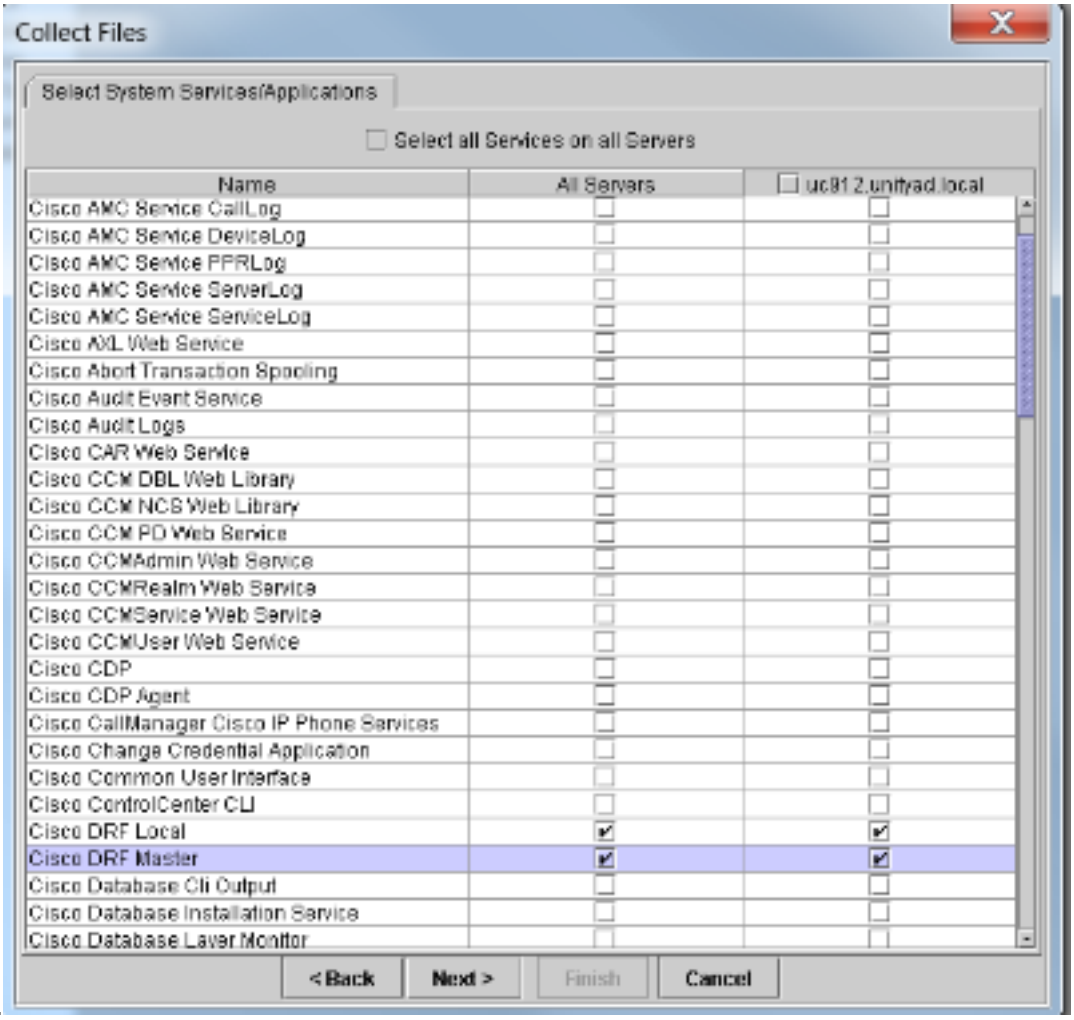
1. Choisissez Cisco Unified Serviceability.
2. Choisissez **Outils > Centre de contrôle - Services réseau**.
3. Rechercher des services de sauvegarde et de restauration et arrêter et démarrer **Cisco DRF Local** et **Cisco DRF Master**.



Utilisez ensuite l'outil de surveillance en temps réel afin de collecter les traces :

1. Accédez à Trace & Log Central.
2. Choisissez **Collecter les fichiers**.
3. Cliquez sur **Suivant** afin de sélectionner Services/applications système.
4. Cochez les deux cases en regard de Cisco DRF Local et Cisco DRF

Master.



5. Cliquez sur **Next** (Suivant).
6. Définissez la plage horaire de votre test et sélectionnez un emplacement de téléchargement.
7. **Cliquez sur Finish.** Cette opération démarre la collecte des journaux à l'emplacement spécifié.

Ci-dessous, des extraits de journaux doivent être notés sur le journal principal DRF indiquant *Impossible de créer un flux d'entrée/sortie vers l'alerte fatale du client reçue : Certificat incorrect*.

Les journaux locaux DRF affichent :

```
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.
```

Les journaux maîtres affichent :

```
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
```

Solution

Dans ce cas, il y a un problème avec le certificat IPSec sur le serveur et vous devez le régénérer, supprimer le certificat ipsec-trust et en charger un nouveau. Complétez ces étapes afin de résoudre le problème :

1. Connectez-vous à la page Administration du système d'exploitation.
2. Choisissez **Security > Certificate Management > find**.
3. Cliquez sur **fichier ipsec.pem**, puis sur **régénération**.
4. Après la génération réussie du fichier ipsec.pem, téléchargez le fichier.
5. Revenir à la page de gestion des certificats.
6. Supprimez l'entrée ipsec-trust actuellement endommagée.
7. Téléchargez le fichier ipsec.pem téléchargé en tant qu'ipsec-trust.
8. Redémarrez DRF Master et DRF Local.