La page Web de Reprise sur sinistre est insensible

Contenu

Introduction

Ce document décrit que quand la page Web de Reprise sur sinistre est utilisée pour établir un Unity Connection de sauvegarde et de restauration, là peut être des problèmes. Cet article couvre une telle situation.

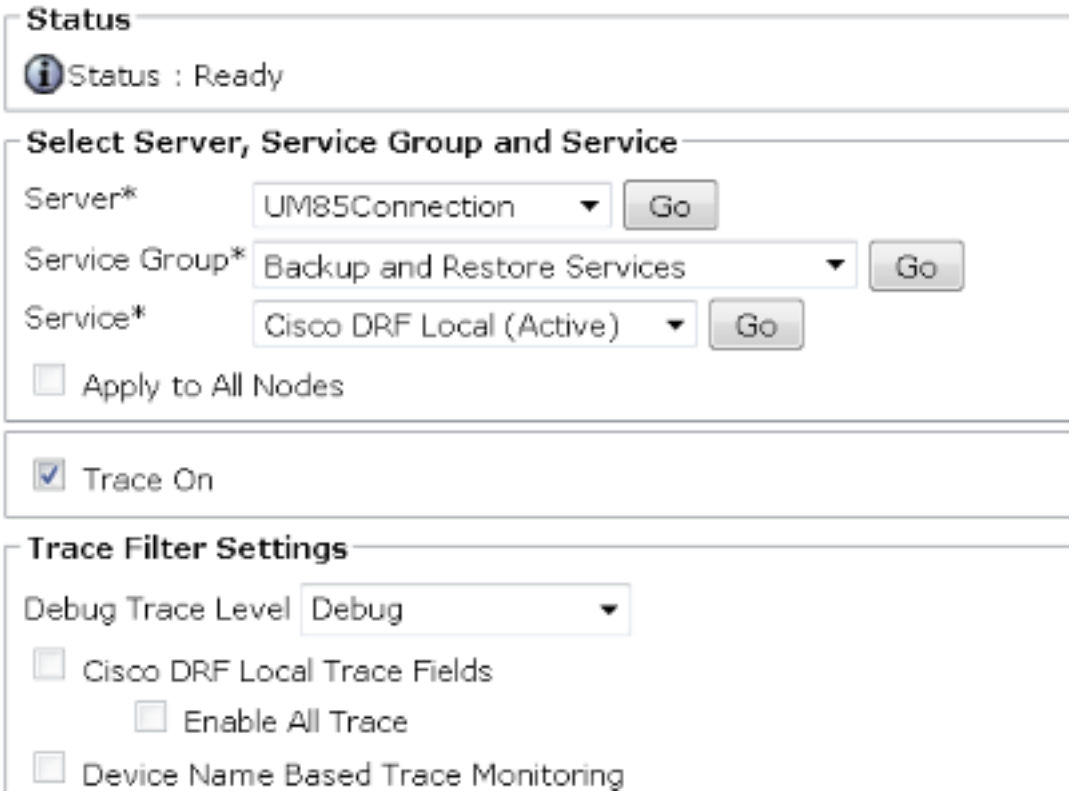
Problème

Quand vous vous connectez dans la page Web de Reprise sur sinistre et cliquez sur n'importe quelle option, page ne charge pas.

Dépannez

Assurez-vous que se connecter de Reprise sur sinistre est activé et tourné débugger.

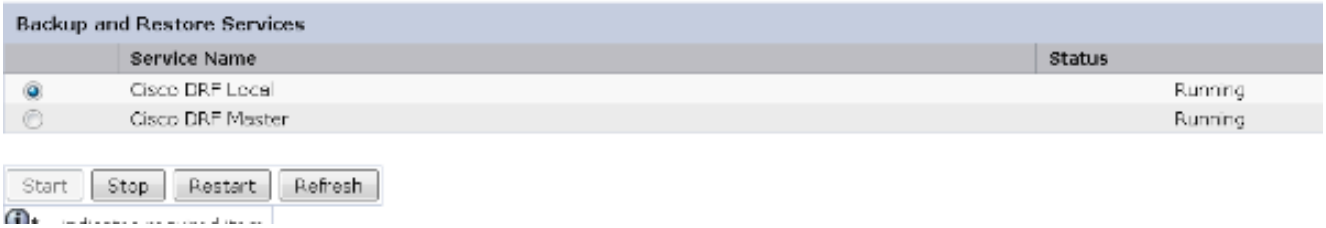
1. Allez à la page Web d'utilité de Cisco Unified.
2. Choisissez le **suivi > la configuration**.
3. De la liste déroulante de Server*, choisissez le serveur.
4. De la liste déroulante de Group* de service, choisissez les **services de sauvegarde et de restauration**.
5. De la liste déroulante de Service*, choisissez les **gens du pays de Cisco DRF (actifs)**.
6. Assurez-vous que le **suivi sur la** case est coché.
7. De la liste déroulante de niveau de suivi de debug, choisissez le



debug.

Ensuite, reproduisez la question. Vous pourriez devoir redémarrer le maître DRF et les services locaux afin d'effectuer un test frais.

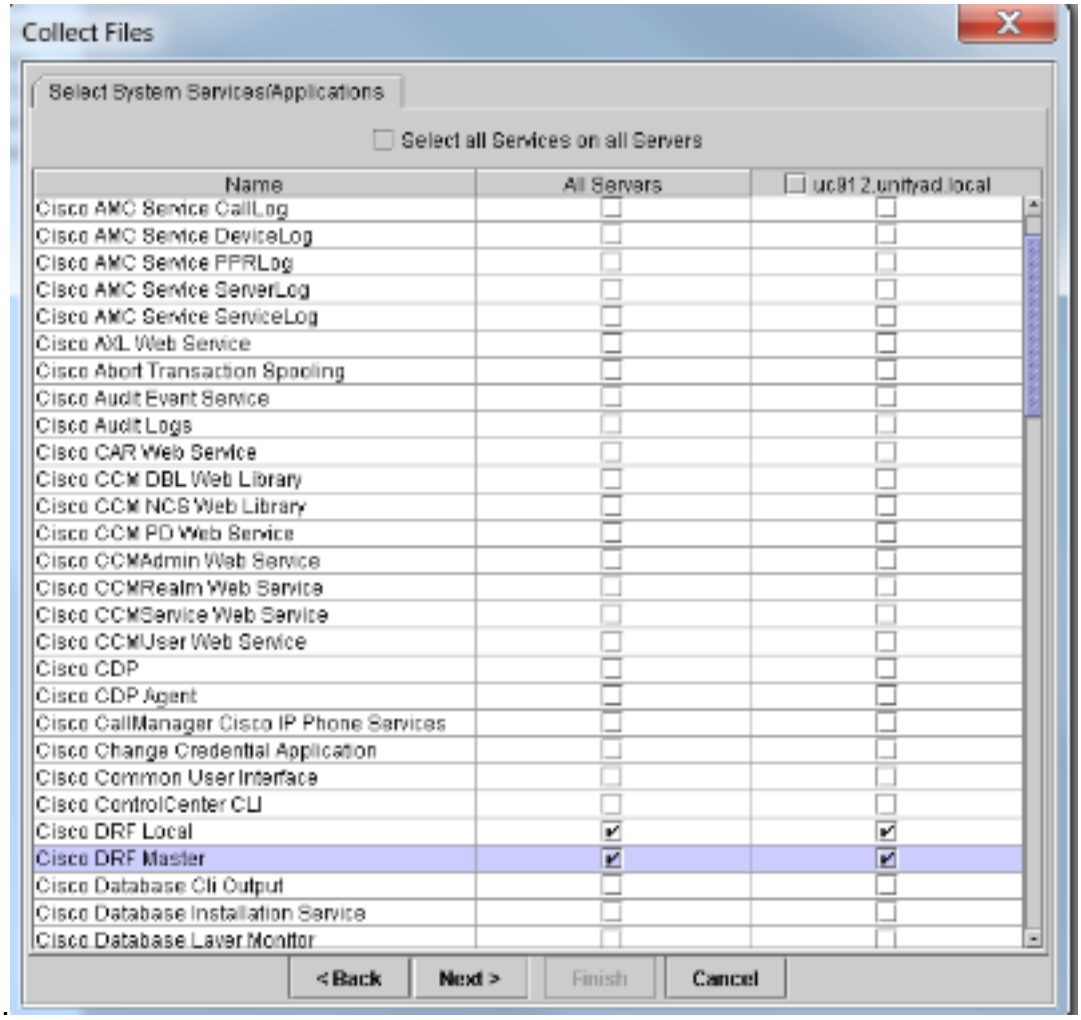
1. Choisissez l'utilité de Cisco Unified.
2. Choisissez le **Tools > Control Center - Services réseau**.
3. Services de sauvegarde de découverte et de restauration et **gens du pays de Cisco DRF d'**arrêt et de début et **maître de Cisco DRF**.



Utilisez alors l'outil de suivi en temps réel afin de collecter les suivis :

1. Allez tracer et se connecter le central.
2. Choisissez **collectent des fichiers**.
3. Cliquez sur Next afin de sélectionner des services système/applications.
4. Vérifiez les cases près des gens du pays de Cisco DRF et du maître de Cisco

DRF.



5. Cliquez sur **Next** (Suivant).
6. Placez la plage de temps de votre test et sélectionnez un site de téléchargement.
7. Cliquez sur **Finish** (Terminer). Ceci commence la collecte de logs à l'emplacement que vous avez spécifié.

Sont ci-dessous les extraits des logs soient sûrs de noter sur le log de maître DRF est afficher *incapable de créer le flot d'entrée/sortie à l'alerte mortelle de client reçue : Mauvais certificat*.

L'exposition locale de logs 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.
```

L'exposition principale de logs :

```
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

Il y a dans ce cas un problème avec le certificat d'IPSec sur le serveur et vous devez le régénérer, supprimez le certificat d'ipsec-confiance, et chargez un neuf. Terminez-vous ces étapes afin d'aborder la question :

1. Connectez-vous la page de gestion de SYSTÈME D'EXPLOITATION.
2. Choisissez la **Sécurité > la Gestion > la découverte de certificat**.
3. **Le fichier du** clic **ipsec.pem et** cliquent sur alors le régénéré**.**
4. Après que la génération réussie du fichier ipsec.pem, téléchargent le fichier.
5. Retournez à la page de Gestion de certificat.
6. Supprimez l'entrée d'ipsec-confiance corrompue par courant.
7. Téléchargez le fichier téléchargé ipsec.pem comme ipsec-confiance.
8. Maître de la reprise DRF et gens du pays DRF.