La pagina Web di Disaster Recovery non risponde

Sommario

Introduzione

In questo documento viene descritto che quando si utilizza la pagina Web Disaster Recovery per creare una connessione Unity di backup e ripristino, possono verificarsi dei problemi. Questo articolo riguarda una di tali situazioni.

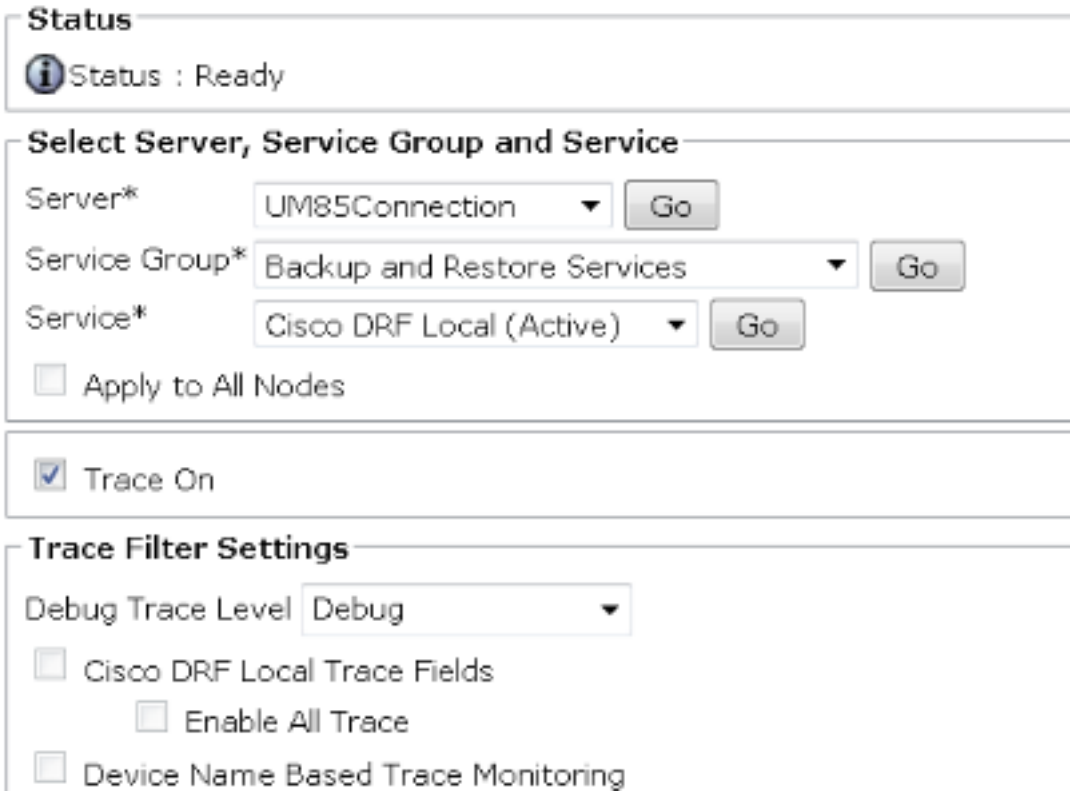
Problema

Quando si accede alla pagina Web di Disaster Recovery e si fa clic su un'opzione qualsiasi, non viene caricata alcuna pagina.

Risoluzione dei problemi

Verificare che la registrazione del ripristino di emergenza sia abilitata e impostata su Debug.

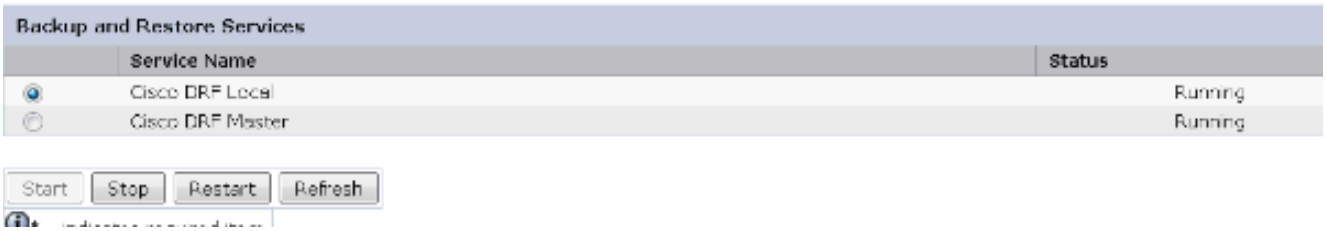
1. Andare alla pagina Web di Cisco Unified Serviceability.
2. Scegliete **Traccia > Configurazione**.
3. Dall'elenco a discesa Server*, scegliere il server.
4. Dall'elenco a discesa Service Group* (Gruppo di servizi*), scegliere **Backup and Restore Services** (Servizi di backup e ripristino).
5. Dall'elenco a discesa Service* (Servizio*), scegliere **Cisco DRF Local (Active) (Locale Cisco DRF (attivo)**.
6. Assicurarsi che la casella di controllo **Traccia su** sia selezionata.
7. Dall'elenco a discesa Livello di traccia debug, scegliere



Debug.

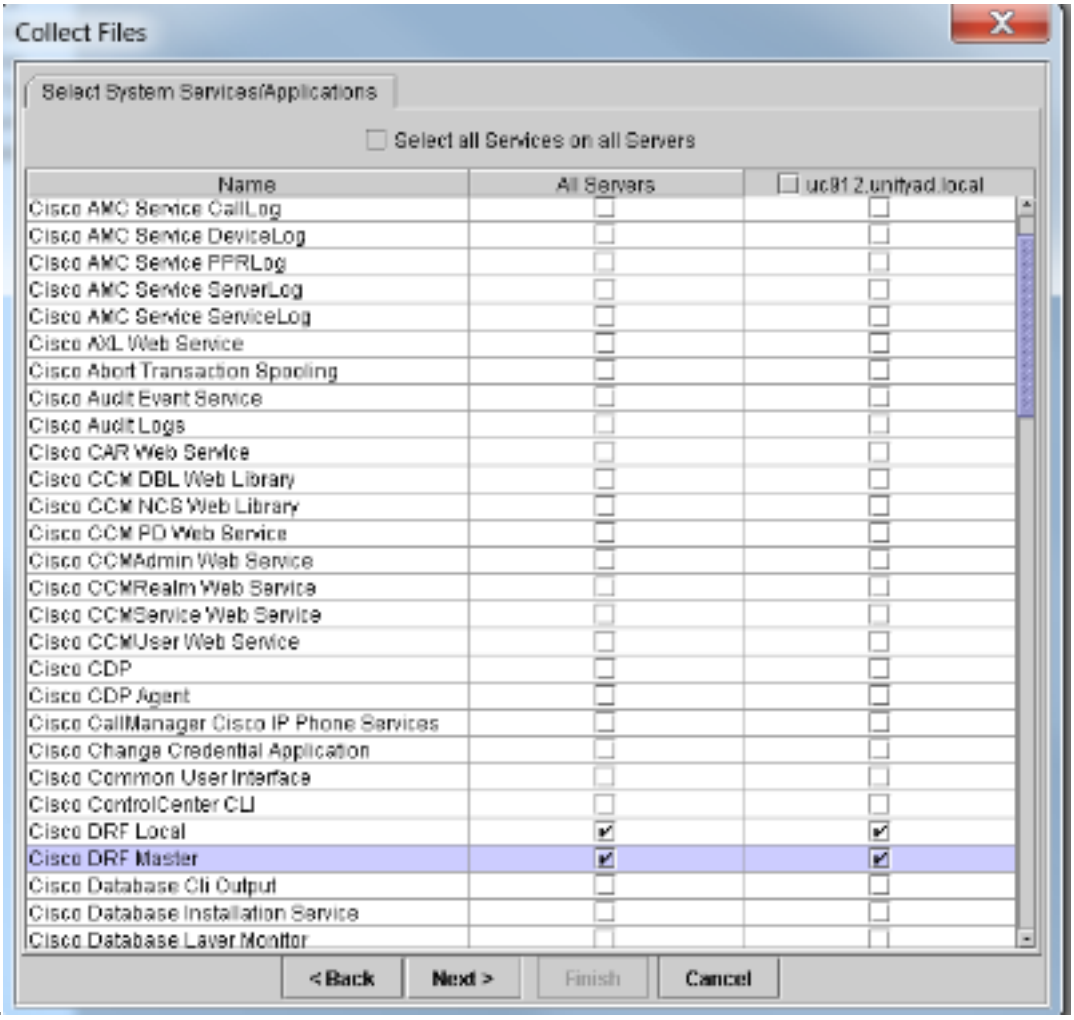
Riprodurre quindi il problema. Per eseguire un nuovo test, potrebbe essere necessario riavviare il master DRF e i servizi locali.

1. Scegli Cisco Unified Serviceability.
2. Scegliere **Strumenti > Control Center - Servizi di rete**.
3. Trovare i servizi di backup e ripristino e arrestare e avviare **Cisco DRF Local** e **Cisco DRF Master**.



Quindi, usare lo strumento di monitoraggio in tempo reale per raccogliere le tracce:

1. Passare a Trace & Log Central.
2. Scegliere **Raccogli file**.
3. Per selezionare i servizi/le applicazioni di sistema, fare clic su **Next** (Avanti).
4. Selezionare entrambe le caselle di controllo accanto a Cisco DRF Local e Cisco DRF

Master. 

5. Fare clic su **Next** (Avanti).
6. Impostare l'intervallo di tempo del test e selezionare un percorso di download.
7. Fare clic su **Finish (Fine).** Verrà avviata la raccolta dei log nel percorso specificato.

Di seguito sono riportati alcuni estratti dei log. Assicurarsi di notare che sul registro master DRF viene visualizzato il messaggio *Impossibile creare il flusso di input/output per il client Alert irreversibile ricevuto: Certificato non valido*.

I log locali DRF mostrano:

```
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.
```

I registri master mostrano:

```
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
```

Soluzione

In questo caso si è verificato un problema con il certificato IPSec nel server ed è necessario rigenerarlo, eliminare il certificato di attendibilità IPSec e caricarne uno nuovo. Per risolvere il problema, completare i seguenti passaggi:

1. Accedere alla pagina Amministrazione del sistema operativo.
2. Scegliere **Protezione > Gestione certificati > trova**.
3. Fare clic su **ipsec.pem file** e quindi su **rigenera**.
4. Dopo la generazione corretta del file ipsec.pem, scaricare il file.
5. Torna alla pagina di gestione dei certificati.
6. Elimina la voce IPSec-trust danneggiata corrente.
7. Caricare il file ipsec.pem scaricato come attendibilità ipsec.
8. Riavviate DRF Master e DRF Local.