

Die Website zur Notfallwiederherstellung reagiert nicht.

Inhalt

[Einleitung](#)

[Problem](#)

[Fehlerbehebung](#)

[Lösung](#)

Einleitung

Dieses Dokument beschreibt, dass es Probleme geben kann, wenn die Disaster Recovery-Webseite verwendet wird, um eine Backup and Restore Unity Connection herzustellen. Dieser Artikel behandelt eine solche Situation.

Problem

Wenn Sie sich auf der Webseite zur Notfallwiederherstellung anmelden und auf eine Option klicken, werden keine Seiten geladen.

Fehlerbehebung

Stellen Sie sicher, dass die Disaster Recovery-Protokollierung aktiviert ist und in Debug umgewandelt wird.

1. Rufen Sie die Cisco Unified Serviceability-Webseite auf.
2. Wählen Sie **Trace > Configuration aus**.
3. Wählen Sie aus der Server*-Dropdown-Liste den Server aus.
4. Wählen Sie aus der Dropdown-Liste "Service Group*" die Option **Backup und Restore Services**.
5. Wählen Sie in der Service*-Dropdown-Liste die Option **Cisco DRF Local (Active)**.
6. Stellen Sie sicher, dass das Kontrollkästchen **Trace On** aktiviert ist.
7. Wählen Sie in der Dropdown-Liste Debug Trace Level (Nachverfolgungsebene debuggen) die Option **Debug**

Status
i Status : Ready

Select Server, Service Group and Service

Server*

Service Group*

Service*

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level



Cisco DRF Local Trace Fields
 Enable All Trace

Device Name Based Trace Monitoring

aus.

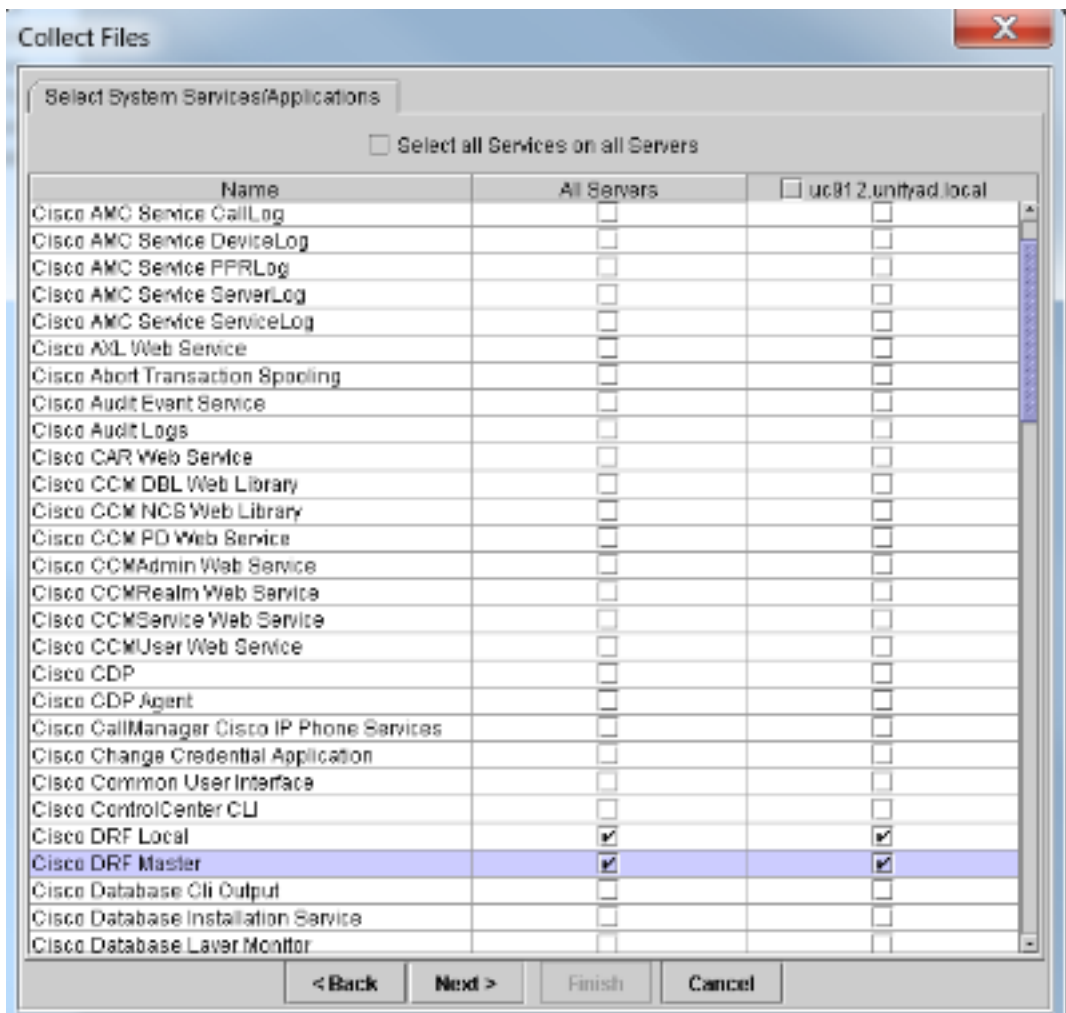
Reproduzieren Sie anschließend das Problem. Möglicherweise müssen Sie den DRF-Master und die lokalen Dienste neu starten, um einen neuen Test durchführen zu können.

1. Wählen Sie Cisco Unified Serviceability.
2. Wählen Sie **Tools > Control Center - Network Services aus.**
3. Suchen Sie nach Backup- und Wiederherstellungsdiensten, und beenden und starten Sie **Cisco DRF Local** und **Cisco DRF Master.**

Backup and Restore Services	
Service Name	Status
 Cisco DRF Local	Running
 Cisco DRF Master	Running

Verwenden Sie dann das Real-Time Monitoring Tool, um die Ablaufverfolgungen zu erfassen:

1. Gehen Sie zu Trace & Log Central.
2. Wählen Sie **Dateien sammeln aus.**
3. Klicken Sie auf **Weiter**, um Systemdienste/Anwendungen auszuwählen.
4. Aktivieren Sie beide Kontrollkästchen neben Cisco DRF Local (Lokale DRF) und Cisco DRF Master (Cisco DRF-



Master).

5. Klicken Sie auf **Weiter**.
6. Legen Sie den Zeitraum für Ihren Test fest, und wählen Sie einen Download-Speicherort aus.
7. Klicken Sie auf **Fertig stellen**. Dadurch wird die Protokollsammlung an dem von Ihnen angegebenen Speicherort gestartet.

Nachfolgend sind Auszüge aus Protokollen aufgeführt. Beachten Sie, dass im DRF-Masterprotokoll die Meldung angezeigt wird, dass *kein Eingabe-/Ausgabestrom für den Client* erstellt werden kann. *Ungültiges Zertifikat*.

Die lokalen DRF-Protokolle zeigen Folgendes an:

```
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.
```

Die Master-Protokolle werden angezeigt:

```
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

Lösung

In diesem Fall liegt ein Problem mit dem IPSec-Zertifikat auf dem Server vor, und Sie müssen es neu generieren, das ipsec-trust-Zertifikat löschen und ein neues Zertifikat laden. Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Melden Sie sich auf der Seite für die Betriebssystemverwaltung an.
2. Wählen Sie **Security > Certificate Management > Find aus**.
3. Klicken Sie auf die **Datei ipsec.pem** und anschließend auf **regenerieren**.
4. Nach der erfolgreichen Generierung der Datei ipsec.pem laden Sie die Datei herunter.
5. Kehren Sie zur Seite Zertifikatsverwaltung zurück.
6. Löschen Sie den aktuellen beschädigten ipsec-trust-Eintrag.
7. Laden Sie die heruntergeladene Datei ipsec.pem als ipsec-trust hoch.
8. Starten Sie DRF Master und DRF Local neu.