Konfiguration von Mechanismen für die Fehlerbehandlung und Serverunerreichbarkeit für die OCS-Fehlerbehebung auf dem ASR5K

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Mechanismen FH (Failure-Handling) und SU (Server-Unreachable) auf der Gy-Schnittstelle konfiguriert werden, um Probleme im Online Charging System (OCS) zu beheben oder die Verbindung zwischen der Policy and Charging Enforcement Function (PCEF) und dem OCS herzustellen. Die in diesem Dokument beschriebenen Informationen gelten für die Funktionen Home Agent (HA), Gateway General Packet Radio Service (GPRS) Support Node (GGSN) und Packet Data Network Gateway (PGW), die auf dem Cisco Aggregated Services Router der Serie 500 (ASR5K) ausgeführt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Ihr System diese Anforderungen erfüllt, um die FH- und SU-Mechanismen zu verwenden:

- Der Enhanced Charging Service (ECS) ist verfügbar
- Das PCEF ist innerhalb von HA, GGSN oder PGW vorhanden.
- Es gibt einen passenden Durchmesser für die Anbindung über die Datenbank.
- Die Diameter Credit Control Application (DCCA) ist verfügbar.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen des ASR5K.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das PCEF ist über die Gy-Schnittstelle mit dem OCS verbunden, die Diameter als Basisprotokoll und DCCA verwendet. Dies ist der Nachrichtenfluss zwischen PCEF und OCS:

- **Credit Control Request (CCR)** âÂ Â Diese Nachricht wird vom PCEF an das OCS gesendet. Es gibt drei Arten von CCR-Meldungen: Anfänglich, aktualisieren und beenden
- **Credit Control Answer (CCA)** âÂ Â Diese Nachricht wird vom OCS als Antwort auf den CCR an das PCEF gesendet. Es gibt auch drei Arten von CCA-Meldungen: Anfänglich, aktualisieren und beenden
- **Re-Authorization Request (RAR)** âÂ Â Diese Nachricht wird vom OCS an das PCEF gesendet, wenn eine erneute Autorisierung der Sitzung erforderlich ist.
- **Re-Authorization Answer (RAA)** âÂ Â Dies ist die Antwort auf die RAR vom PCEF zum OCS.

Um den Nachrichtenfluss zu ermöglichen, wird zwischen dem PCEF und dem OCS eine Durchmesserverbindung hergestellt. Es besteht die Möglichkeit, dass das OCS negative Nachrichten sendet, die Transportverbindung zwischen dem PCEF und dem OCS fehlschlägt oder die Nachricht ausfällt, was zu einem Ausfall in der Teilnehmersitzungseinrichtung führen kann. Dies kann den Teilnehmer an der Nutzung von Diensten hindern.

Diese beiden Mechanismen können zur Lösung dieses Problems verwendet werden:

- Der FH-Mechanismus

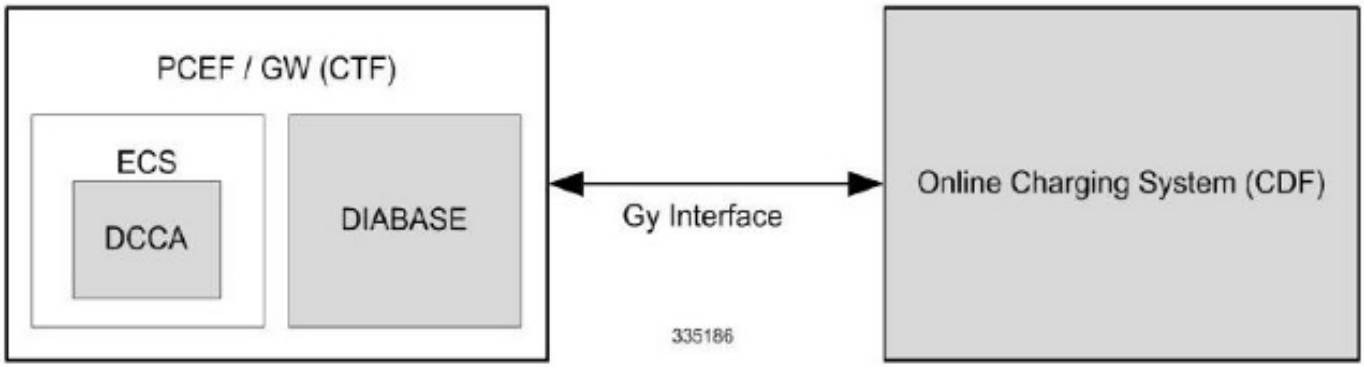
- Der SU-Mechanismus

Konfigurieren

In diesem Abschnitt werden die Konfigurationen beschrieben, die zur Unterstützung der FH- und SU-Mechanismen erforderlich sind.

Netzwerkdiagramm

Die Informationen in diesem Dokument verwenden die folgende Topologie:



X-Ablaufdatum

Dies ist ein Timer auf Anwendungsebene für das DCCA, der in den Einstellungen für *die* Kreditsteuerung des *Durchmessers* konfiguriert werden kann. Der Wert kann zwischen 1 und 300 Sekunden liegen.

Hier ein Beispiel:

```
[local]host_name(config-dcca)# diameter pending-timeout
```

Antwort-Timeout

Dies ist ein Datenbank-Timeout und kann in den *Diameter-Endpunkteeinstellungen* konfiguriert werden. Der Wert kann zwischen 1 und 300 Sekunden liegen.

> **Hinweis**: Der für diesen Timer konfigurierte Wert sollte größer sein als der für den Tx-Expiry-Timer verwendete Wert.

Hier ein Beispiel:

```
[context_name]host_name(config-ctx-diameter)# response-timeout
```

Durchmesser: Sitzungs-Failover

Diese Funktion wird verwendet, um die Ausfallsicherung für Kreditsteuerungssitzungen mit einem Durchmesser zu aktivieren oder zu deaktivieren. Dadurch kann das System einen Sekundärserver verwenden, wenn der Primärserver nicht erreichbar ist. Dies ist in den Einstellungen für *die Kreditsteuerung* des *Durchmessers* konfigurierbar.

Hier ein Beispiel:

```
local]host_name(config-dcca)# diameter session failover
```

FH-Mechanismus

Der FH-Mechanismus funktioniert nur, wenn Sitzungsausfallsicherung mit Durchmesser vorhanden ist. Das FH ermöglicht dem System zu entscheiden, ob die Sitzung fortgesetzt und in Offline konvertiert oder die Sitzung beendet werden soll, wenn ein Verbindungs- oder Nachrichtenfehler auftritt.

> **Hinweis**: Der FH ist standardmäßig aktiviert und konfiguriert.

Konfiguration des FH-Mechanismus

Der FH-Mechanismus kann in den Einstellungen für die *Kreditsteuerung* des *Durchmessers* konfiguriert werden. Die folgende Syntax wird in der FH-Konfiguration verwendet:

```
failure-handling { initial-request | terminate-request | update-request } { continue
[ go-offline-after-tx-expiry | retry-after-tx-expiry ] | retry-and-terminate,
[ retry-after-tx-expiry ] | terminate }
```

Der erste Abschnitt gibt den *Anforderungstyp an*: Initial (CCR-I), Update (CCR-U) und Terminate (CCR-T).

Im zweiten Abschnitt wird die *Aktion* angegeben, die bei Aktivierung des FH-Mechanismus durchgeführt werden soll. Diese drei Aktionen sind mit dem FH-Mechanismus möglich:

- **Continue** â Â Dies ermöglicht die Sitzung fortzufahren und konvertiert sie in offline. Diese Funktion verwendet zwei Optionen, die sich auf Tx-Ablauf beziehen:

  Go-offline-after-tx-exponent âÂ Â Diese startet das Offline-Aufladen nach dem Tx-Ablauf tritt.

  Nach-tx-Verfallsdatum âÂ Â Diese erneuert den sekundären Server nach dem Tx-

Verfallsdatum.

- **Retry-and-terminate** âÂ Â Diese beendet die Sitzung, nachdem das System den sekundären Server erneut versucht, wenn der sekundäre Server ebenfalls nicht verfügbar ist. Dabei wird auch die Option **Retry-after-tx-Expending** verwendet, die den sekundären Server nach dem Tx-Ablaufdatum erneut versucht.

- **Terminate** â Â Diese beendet die Sitzung ohne Versuche, den sekundären Server zu kontaktieren.

Standardverhalten des FH-Mechanismus

In diesem Abschnitt wird das FH-Standardverhalten beschrieben, wenn keine Konfiguration vorhanden ist. Standardmäßig wird der FH-Mechanismus während eines Response Timeout (RT) aktiviert, außer wenn die Aktion *Terminate* konfiguriert ist.

Wenn ein AVP (*Credit-Control-Failure-Handling* Attribute Value Pair) vom Server empfangen wird, werden die empfangenen Einstellungen angewendet.

Hier einige Beispiele:

- **Anfängliche Anfrage > Kündigen**

- **Update-Request > Retry-and-Terminate**

- **Abschlussanforderung > Wiederholen und Beenden**

FH-Mechanismus - Detaillierter Anruffluss

In diesem Abschnitt wird der detaillierte Anrufablauf des FH-Mechanismus mit allen möglichen Optionen beschrieben.

Anfängliche Anforderung

CCFH-Einstellung	CLI-Befehl	Verhalten bei Tx	Verhalten bei RT	Sekundär ist aktiv	Sekundäres Gerät is
Weiter	Erstantrag fortfahren	K/A	Weiter	Sekundär übernimmt RT	Offline nach einem a Es werden keine Qu mehr durchgeführt. für beliebige Ratingg Sitzung nach DCCA-Ausfall Verbindung zum DC wiederhergestellt)
	Erstantrag weiter offline gehen TX-Ablaufdatum	Offline	K/A	Offline bei Tx	Offline bei Tx
	Erstantrag Wiederholung des Wiederholungsversuchs	Weiter	K/A	Sekundär übernimmt Tx	Offline nach einem a

	TX-Ablaufdatum Erstantrag wiederholen und beenden	K/A	Wiederholen	Sekundär übernimmt RT	Nach einem anderen kündigen
Wiederholen und beenden	Erstantrag wiederholen und beenden	Wiederholen	K/A	Sekundär übernimmt Tx	Nach einer anderen
	Nach-tx-Ablauf erneut versuchen				
Beenden	Erstantrag beenden	Beenden	K/A	Nach Tx beenden	Nach Tx beenden

Aktualisierungsanforderung

CCFH-Einstellung	CLI-Befehl	Verhalten bei Tx	Verhalten bei RT	Sekundär ist aktiv	Sekundäres Gerät ist ausgefa
	Aktualisierungsanfrage fortfahren	K/A	Weiter	Sekundär übernimmt RT	Offline nach einem anderen R
	Aktualisierungsanfrage weiter offline gehen	Offline	K/A	Offline bei Tx	Offline bei Tx
Weiter	TX-Ablaufdatum Aktualisierungsanfrage Wiederholung des Wiederholungsversuchs	Weiter	K/A	Sekundär übernimmt Tx	Offline nach einem anderen T
	TX-Ablaufdatum Aktualisierungsanfrage wiederholen und beenden	K/A	Wiederholen	Sekundär übernimmt RT	Sendet CCR-T nach einem anderen RT
Wiederholen und beenden	Aktualisierungsanfrage wiederholen und beenden	Wiederholen	K/A	Sekundär übernimmt Tx	Sendet CCR-T nach einer anderen Tx
	Nach-tx-Ablauf erneut versuchen				
Beenden	Aktualisierungsanfrage beenden	Beenden	K/A	Sendet CCR-T nach Tx	Sendet CCR-T nach Tx

Anfrage beenden

CCFH-Einstellung	CLI-Befehl	Verhalten bei Tx	Verhalten bei RT	Sekundär ist aktiv	Sekundäres Gerät ist ausgefa
Weiter	Abschlussanforderung fortfahren	K/A	Wiederholen	CCR-T wird gesendet sekundär nach RT	Nach einem anderen RT kündigen

	Abschlussanforderung weiter offline gehen TX-Ablaufdatum	Wiederholen	K/A	CCR-T wird gesendet sekundär nach Tx	Nach einer anderen Tx beend
	Abschlussanforderung Wiederholung des Wiederholungsversuchs TX-Ablaufdatum	Wiederholen	K/A	CCR-T wird gesendet sekundär nach Tx	Nach einer anderen Tx beend
	Abschlussanforderung wiederholen und beenden	K/A	Wiederholen	CCR-T wird gesendet sekundär nach RT	Nach einem anderen RT kündigen
Wiederholen und beenden	Abschlussanforderung wiederholen und beenden Nach-tx-Ablauf erneut versuchen	Wiederholen	K/A	CCR-T wird gesendet sekundär nach Tx	Nach einer anderen Tx beend
Beenden	Abschlussanforderung beenden	Beenden	K/A	Kündigen nach Tx	Nach Tx beenden

SU-Mechanismus

Der SU-Mechanismus ähnelt dem FH-Mechanismus, bietet jedoch eine präzisere Kontrolle über Fehlerverfahren. Zusätzlich zur Fortsetzung der Sitzung nach Ausfällen auf Nachrichten- und Verbindungsebene (Transport) kann dieser Mechanismus verwendet werden, wenn die Antworten aus dem OCS langsam sind. Sie bietet außerdem die Möglichkeit, die Sitzung entweder für eine bestimmte Zeit/Ausschöpfung des Kontingents vor Beendigung fortzusetzen oder ein konfigurierbares vorläufiges Kontingent (Volumen und Zeit) sowie konfigurierbare Server-Wiederholungen zu verwenden, bevor eine Sitzung in offline umgewandelt oder beendet wird.

Konfiguration des SU-Mechanismus

Der SU-Mechanismus kann in den Einstellungen für die *Kreditsteuerung* des *Durchmessers* konfiguriert werden. Die in der SU-Konfiguration verwendete Syntax variiert je nach verwendeter Version.

Für die Versionen 12.1 und früher ist dies die Syntax, die für die Konfiguration des SU-Mechanismus verwendet wird:

```
servers-unreachable { initial-request { continue | terminate [ after-timer-expiry
<timeout_period> ] } | update-request { continue | terminate [ after-quota-expiry
| aftertimer-expiry <timeout_period> ] } }
```

Für die Versionen 12.2 und höher ist dies die Syntax, die für die Konfiguration des SU-Mechanismus verwendet wird:

```
servers-unreachable { behavior-triggers { initial-request | update-request }
result-code { any-error | <result-code> [ to <end-result-code> ] }
| transport-failure [ response-timeout | tx-expiry ] | initial-request
{ continue [ { [ after-interim-time <timeout_period> ] [ after-interim-volume
<quota_value> ] } server-retries <retry_count> ] | terminate [ {
[ after-interim-time <timeout_period> ] [ after-interim-volume <quota_value> ]
} server-retries <retry_count> | after-timer-expiry <timeout_period> ] }
| update-request { continue [ { [ after-interim-time <timeout_period> ]
[ after-interim-volume <quota_value> ] } server-retries <retry_count> ]
| terminate [ { [ after-interim-time <timeout_period> ] [ after-interim-volume
<quota_value> ] } server-retries <retry_count> ] | after-quota-expiry |
after-timer-expiry <timeout_period> ] } }
```

> **Hinweis**: In Versionen vor Version 12.2 gab es Flexibilität, die FH- und SU-Mechanismen unabhängig zu konfigurieren. In Version 12.2 und höher hat der SU-Mechanismus jedoch bei der Konfiguration Vorrang vor dem FH-Mechanismus.

Wenn der Server den CC-FH AVP zurückgibt und der SU-Mechanismus für eine Reihe von Verhaltens-Triggern konfiguriert ist, wird die SU-Konfiguration angewendet. Andernfalls wird der AVP-Wert für CC-FH angewendet. Ergebniscodes wie 3002, 3004 und 3005 fallen standardmäßig unter *Lieferfehler* und werden als RTs behandelt.

Diese Aktionen sind mit dem SU-Mechanismus möglich:

- **Behavior-Trigger** âÂ Â Dieser Wert gibt die Art der Nachrichten an, die Initial-Requests (CCR-I) oder Update-Requests (CCR-U) sein können. Für diese Trigger stehen drei Optionen zur Verfügung:

  Result-Code âÂ Â Dies ermöglicht die Konfiguration von bestimmten Ergebniscodes, Bereich der Ergebniscodes (3000-5999) oder jeder Fehler zusammen mit dem Meldungstyp.

  Transport-Failure âÂ Â Diese Spezifikation löst das Verhalten bei Transportausfall aus, das abwärtskompatibel mit Version 12.0 ist. Für diese Einstellung stehen zwei Optionen zur Verfügung:

  Response-Timeout âÂ Â Diese Option löst das Verhalten bei RT aus und sollte immer bei Transportausfällen verwendet werden.

  Tx-Expiry âÂ Â Diese Option löst das Verhalten bei Tx-Ablauf aus und sollte immer bei Transportausfällen angewendet werden.

  Aktionen â Â Dieser Wert legt die Aktion fest, die ausgeführt wird, wenn ein SU-Trigger für CCR-I oder CCR-U auftritt. Diese Aktion hängt vom Nachrichtentyp und der Softwareversion ab.

- **Continue** â Â Dies ermöglicht, die Sitzung zu offline konvertieren und fortzufahren. Für die Verwendung dieser Aktion in Versionen vor Version 12.2 stehen keine weiteren Optionen zur Verfügung. In Version 12.2 und höher stehen die Optionen für das Zwischenkontingent, Server-Retries und das Ablaufdatum nach dem Timeout für den Timer für diese Aktion zur Verfügung.

- **Terminate** â Â Dies führt zum Ende der Sitzung, wenn der Server nicht erreichbar wird. Diese

Aktion ermöglicht die Optionen für Zwischenkontingent, Server-Wiederholungen und Timeout nach Ablauf des Timers.

Diese Optionen können mit der Aktion *Weiter* oder *Beenden* verwendet werden:

- **Nach der Zwischenzeit** âÂ Â Diese Option ermöglicht die Fortsetzung oder Beendigung des Anrufs nach der Zwischenzeitüberschreitung. Dies entspricht einem Zeitkontingent, bevor die Aktion ausgeführt wird. Der Wert wird in Sekunden formatiert und kann zwischen 1 und 4.294.967.295 liegen.

- **After-Interim-Volume** âÂ Â Diese Option weist das Zwischenkontingent zu und ermöglicht die Fortsetzung oder Beendigung der Sitzung vor Erschöpfung der konfigurierten Menge. Der Wert wird in Byte formatiert und kann zwischen 1 und 4.294.967.295 liegen.

- **Server-Retries** âÂ Â Diese Option ermöglicht es dem PCEF, das OCS vor dem Fortfahren oder Beenden der Sitzung erneut zu testen. Die Wiederholungszahl kann konfiguriert werden, und der Wert liegt zwischen 0 und 65.535. Wenn der Wert 0 (null) lautet, wird der Wiederholungsversuch nicht ausgeführt, und die Aktion wird sofort angewendet.

Hinweis: Die Optionen *für Zwischenvolumen* und *NachZwischenvolumen* werden immer mit der *Option Serverneuerversuche* verwendet, oder alle drei Optionen können gleichzeitig verwendet und sowohl für Fortsetzung als auch für Terminierung angewendet werden. Die Optionen für *Zwischen-* und *Nachbereitungsvolumen* weisen ebenfalls Zeit sowie Mengenkontingent zu, und das ausgeschöpfte Kontingent löst den Serverneustart aus.

- **After-Timer-Expending** âÂ Â Diese Option gibt die Zeitdauer (in Sekunden) an, für die Sitzungen im Offline-Status verbleiben, bevor sie beendet werden. Die Werte können zwischen 1 und 4.294.967.295 liegen. Diese Option gilt nur für Terminierungsaktionen.

- **Nach Ablauf des Kontingents** Â Â Diese Option endet mit Erschöpfung der bereits zugewiesenen Quote.

Hier einige wichtige Informationen, die Sie sich merken sollten:

- Die Optionen *für Nach-Interim-* und *Server-Retries* können einzeln oder in Kombination verwendet werden. Sie gelten sowohl für Fortsetzung als auch für Beendigung von Aktionen.

- Die Option *nach Ablauf des Kontingents* gilt nur für den Auslöser für das Aktualisierungsverhalten.

- Die Option *nach Ablauf des Zeitgebers* gilt nur für die Terminierungsaktion.

- Die Optionen *nach Zwischen-, Nach-Interim-Volume-* und *Server-Retries* gelten nur für die Versionen 12.2 und höher.

- Wenn Sitzungs-Failover mit Durchmesser unterstützt (und konfiguriert) wird, wird immer der sekundäre Server kontaktiert, bevor der SU-Mechanismus ausgelöst wird.

- Der Server, der zuletzt kontaktiert wurde, bevor der SU-Mechanismus ausgelöst wird, wird immer kontaktiert, wenn die Zwischen- oder Zwischenzeit erschöpft ist und die Option *Server retries* mit einem Wert größer als Null konfiguriert ist. Wenn beispielsweise zunächst OCS1 ausprobiert wird und OCS2 nach einem Fehler bei OCS1 ausprobiert wird, löst die Kommunikation mit OCS2 den SU-Mechanismus aus. Während des Serverneuversuchs wird zunächst OCS2 kontaktiert und dann OCS1, wenn eine negative Antwort von OCS2 eingeht.

SU-Mechanismus - Anrufverläufe

Der SU-Mechanismus kann durch einen Ausfall des CCR-I oder des CCR-U ausgelöst werden. Die Ursache kann ein Fehlercode, ein Transportfehler, ein Tx-Limit oder ein RT sein. Dabei kann es sich um eine Zuweisung von Interimskontingenten (Zeit und/oder Volumen), Server-Wiederholungen, Timer-Werten (die dazu führen, dass die Sitzung für eine bestimmte Zeit und nur für eine Beendigung offline geht) oder Quoten-Ablaufdatum (nur für CCR-U und Beendigung) handeln, bevor die Sitzung offline geht oder beendet wird.

Das vorläufige Kontingent wird pro Sitzung und nicht pro Rating-Gruppe (RG) in MSCC-Szenarien (Multiple Services Credit Control) bereitgestellt.

Es besteht die Möglichkeit, dass der primäre Server einen Transportfehler auslöst und der sekundäre Server den Tx-Ablauf oder das Response-Timeout auslöst. In diesem Szenario wird der letzte Fehler als Auslöser des Fehlers angesehen.

Wenn der SU-Mechanismus nicht für einen Auslöser für einen Ausfall konfiguriert ist, wird der FH-Mechanismus ausgelöst.

> **Hinweis**: In den folgenden Abschnitten werden einige Beispiele für den Anrufablauf im Zusammenhang mit dem SU-Mechanismus aufgeführt. Diese Anrufverläufe werden unter der Annahme bereitgestellt, dass ein Cailover-Modus mit Durchmesser und Sitzungen unterstützt wird und der sekundäre Server mit einem Wert mit Ablaufdatum (Tx) konfiguriert ist, der unter dem RT-Wert liegt. Außerdem wird davon ausgegangen, dass der SU-Mechanismus für Transportausfälle, Tx-Limit und RT konfiguriert ist.

Anfängliche Anforderung ohne Sitzungstrennung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet einen CCR-I an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder die vorläufige Uhrzeit konfiguriert werden, wird die vorläufige Quote der Sitzung zugewiesen.

5. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-I erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird der CCR-I an einen anderen Server gesendet.

6. Wenn der Transportfehler oder ein Tx-Timeout erneut erkannt werden, werden die Schritte 2 bis 5 wiederholt, bis der Wert für den *erneuten Versuch des Servers* erschöpft ist oder eine erfolgreiche Antwort nicht vom OCS kommt.

7. Wenn das Problem weiterhin besteht, wird die Sitzung fortgesetzt (in offline konvertiert) oder beendet (entsprechend der Konfiguration).

   Hinweis: Das Zwischenkontingent, das verbraucht wird, während die Sitzung aufgrund von CCR-I in den SU-Modus wechselt, wird im nächsten CCR-I nicht gemeldet. Das gesamte verwendete Zwischenkontingent wird in CCR-U gemeldet, das dem erfolgreichen CCA-I folgt.

Anfängliche Anforderung mit Sitzungstrennung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet einen CCR-I an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder die vorläufige Uhrzeit konfiguriert werden, wird die vorläufige Quote der Sitzung zugewiesen.

5. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-I erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird der CCR-I an einen anderen Server gesendet.

6. Wenn der Transportfehler oder ein Tx-Timeout erneut erkannt werden, werden die Schritte 2 bis 5 wiederholt, bis der Wert für den *erneuten Versuch des Servers* erschöpft ist oder eine erfolgreiche Antwort nicht vom OCS kommt. An diesem Punkt wird die Sitzung unterbrochen, ohne dass die gesamte Interimsquote ausgeschöpft wird.

7. Nach Beendigung der Sitzung sendet das PCEF erneut den CCR-I, um eine neue Sitzung zu starten. Ist dies erfolgreich, sendet die PCEF den CCR-T, der das gesamte verwendete temporäre Kontingent meldet.

Aktualisierungsanforderung ohne Sitzungstrennung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet eine CCR-U an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder die vorläufige Uhrzeit konfiguriert werden, wird die vorläufige Quote der Sitzung zugewiesen.

5. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-U erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird eine CCR-U an einen anderen Server gesendet, der das gesamte verbrauchte, nicht gemeldete Kontingent enthält.

6. Wenn der Transportfehler oder ein Tx-Timeout erneut erkannt werden, werden die Schritte 2 bis 5 wiederholt, bis der Wert für den *erneuten Versuch des Servers* erschöpft ist oder eine erfolgreiche Antwort nicht vom OCS kommt.

7. Das gesamte verbrauchte Kontingent wird dem OCS mit dem erfolgreichen CCR-U gemeldet.

8. Wenn das Problem weiterhin besteht, wird die Sitzung gemäß der Konfiguration fortgesetzt (in offline konvertiert) oder beendet, nachdem der maximale Wiederholungswert ausgeschöpft wurde.

Aktualisierungsanforderung mit Sitzungstrennung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet eine CCR-U an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder die vorläufige Uhrzeit konfiguriert werden, wird die

vorläufige Quote der Sitzung zugewiesen.

5. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-U erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird eine CCR-U an einen anderen Server gesendet, der das gesamte verbrauchte, nicht gemeldete Kontingent enthält.

6. Wenn der Transportfehler oder ein Tx-Timeout erneut erkannt werden, werden die Schritte 2 bis 5 wiederholt, bis der Wert für den *erneuten Versuch des Servers* erschöpft ist oder eine erfolgreiche Antwort nicht vom OCS kommt. An diesem Punkt wird die Sitzung unterbrochen, bevor die gesamte temporäre Quote verbraucht wird.

7. Das PCEF sendet ein CCR-T an das OCS, um das gesamte verbrauchte Kontingent zu melden.

8. Wenn das OCS mit einem Ergebniscode *2002* antwortet, sind die zusätzlichen Berichte nicht erforderlich.

Aktualisierungsanforderung mit unbekannter Sitzung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet eine CCR-U an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder die vorläufige Uhrzeit konfiguriert werden, wird die vorläufige Quote der Sitzung zugewiesen.

5. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-U erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird eine CCR-U an einen anderen Server gesendet, der das gesamte verbrauchte, nicht gemeldete Kontingent enthält.

6. Der OCS antwortet mit einem Ergebniscode *5002* (unbekannte Sitzungs-ID) für den CCR-U, der in dem Szenario möglich ist, in dem der OCS neu gestartet wurde und die Sitzungs-ID-Informationen verloren haben.

7. Das PCEF initiiert eine neue Sitzung mit dem CCR-I und erhält den CCA-I.

8. Das PCEF meldet in nachfolgenden Meldungen das gesamte verbrauchte

Zwischenkontingent über CCR-U.

Aktualisierungsanfrage mit mehreren RGs (MSCC-Szenario)

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet die CCR-U für RG1 an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportausfall oder ein Timeout aufweist, wird der SU-Mechanismus ausgelöst. Dies tritt sofort bei Transportausfällen oder nach Ablauf der Tx-Frist für eine Zeitüberschreitung auf.

4. Wenn die vorläufige Menge und/oder Uhrzeit konfiguriert ist, wird die vorläufige Quote der Sitzung zugewiesen

5. Zu diesem Zeitpunkt erschöpft RG2 auch die gesamte zugewiesene Quote, initiiert aber nicht die CCR-U, da sich die Sitzung bereits im SU-Modus befindet und beginnt, die vorläufige Quote zu nutzen.

6. Nach Erschöpfung des Zwischenkontingents (Zeit oder Volumen) und wenn der *Server den* Wert *erneut versucht*, einen Wert von mehr als 0 zu erreichen, wird der CCR-U erneut an den Server gesendet, der den SU-Mechanismus ausgelöst hat. Bei einem weiteren Ausfall wird eine CCR-U an einen anderen Server gesendet, der das gesamte verbrauchte, nicht gemeldete Kontingent für beide RGs enthält.

7. Wenn der Transportfehler oder ein Tx-Timeout erneut erkannt werden, werden die Schritte 2 bis 6 wiederholt, bis der *Server den* Wert für den *erneuten Versuch* ausgeschöpft hat oder eine erfolgreiche Antwort nicht vom OCS kommt.

8. Das gesamte verbrauchte Kontingent wird dem OCS mit dem erfolgreichen CCR-U gemeldet.

9. Wenn das Problem weiterhin besteht, wird die Sitzung gemäß der Konfiguration fortgesetzt (in offline konvertiert) oder beendet, nachdem der maximale Wiederholungswert ausgeschöpft wurde.

Anfrage beenden

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet ein CCR-T an das OCS.

2. Ein Timeout oder ein Transportfehler wird erkannt. Wenn ein Transportfehler erkannt wird, versucht das PCEF sofort erneut mit dem sekundären Server. Andernfalls wird das Tx-Limit ausgelöst.

3. Wenn der sekundäre Server auch einen Transportfehler oder ein Timeout aufweist, wird die Sitzung entfernt.

CCR-Fehlercodeverwaltung

Der Nachrichtenfluss für dieses Szenario sieht folgendermaßen aus:

1. Das PCEF sendet einen CCR an das OCS, und das OCS antwortet mit einem Fehlercode.

2. Der Fehlercode wird im SU-Mechanismus statisch konfiguriert.

3. Das PCEF stellt das vorläufige Kontingent bereit, ohne dass ein erneuter Versuch zum sekundären Server unternommen wird.

FH- und SU-Beispielkonfigurationen

Dieser Abschnitt enthält ein Konfigurationsbeispiel für die Mechanismen FH und SU. Wenn sowohl die FH- als auch die SU-Mechanismen konfiguriert sind, hat die SU für denselben Verhaltens-Trigger Vorrang vor der FH.

Hier ein Beispiel:

```
credit-control group test

diameter origin endpoint test

diameter peer-select peer test

quota volume-threshold percent 10

diameter pending-timeout 80 deciseconds msg-type any

diameter session failover

trigger type rat lac

apn-name-to-be-included virtual

quota request-trigger exclude-packet-causing-trigger

failure-handling initial-request continue retry-after-tx-expiry

servers-unreachable initial-request terminate after-interim-volume 200
after-interim-time 3600 server-retries 0

servers-unreachable behavior-triggers initial-request transport-failure
tx-expiry

servers-unreachable update-request continue after-interim-volume 200
after-interim-time 3600 server-retries 50

servers-unreachable behavior-triggers update-request transport-failure
tx-expiry
```

Überprüfen

Um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert, geben Sie den Befehl **show active-charge service <service name>** ein:

```
# show active-charging service name test

Service name: test

TCP Flow Idle Timeout : 300 (secs)
UDP Flow Idle Timeout : 300 (secs)
ICMP Flow Idle Timeout : 300 (secs)
ICMP Flow Idle Timeout : 300 (secs)
ALG Media Idle Timeout : 120 (secs)

TCP Flow-Mapping Idle Timeout : 300 (secs)
UDP Flow-Mapping Idle Timeout : Not Configured

Deep Packet Inspection: Enabled
Passive Mode : Disabled
CDR Flow Control : Enabled
CDR Flow Control Unsent Queue Size: 75
Unsent Queue high watermark: 56
Unsent Queue low watermark: 18

Content Filtering: Disabled

Dynamic Content Filtering: Disabled

URL-Blacklisting: Disabled
URL-Blacklisting Match-method: Exact

Content Filtering Match-method: Generic
```

```
Interpretation of Charging-rule-base-name: active-charging-group-of-ruledefs



Selection of Charging-rule-base AVP : Last


Credit Control:

Group : test


Mode : diameter

APN-name-to-be-included: gn

Trigger-Type : N/A


Failure-Handling:

Initial-Request : continue retry-after-tx-expiry

Update-Request : retry-and-terminate

Terminate-Request: retry-and-terminate


Server Unreachable Failure-Handling:

Initial-Request : terminate

Update-Request : continue
```

Fehlerbehebung

Geben Sie den Befehl **show active-Charging Credit-Control Statistics** ein, um die Statistiken anzuzeigen, die sich auf die SU- und FH-Mechanismen beziehen. Hier eine Beispielausgabe:

```
#show active-charging credit-control statistics
...

OCS Unreachable Stats:

Tx-Expiry: 2291985 Response-TimeOut: 615

Connection-Failure: 2 Action-Continue: 0

Action-Terminated: 0 Server Retries: 2023700


Assumed-Positive Sessions:
```

```
Current: 2 Cumulative: 2196851
```

Hier einige wichtige Hinweise zu dieser Beispielausgabe:

- **Tx-Expiry** âÂ Â Dies weist auf eine SU-Erkrankung aufgrund eines Tx-Verfalles hin.
- **Response-Timeout** âÂ Â Dies zeigt eine SU-Bedingung aufgrund einer RT.
- **Connection-Failure** âÂ Â Dies weist auf einen SU-Zustand aufgrund eines Transportausfalls hin.
- **Action-Continue** âÂ Â Dieses Feld gibt die Anzahl der Sitzungen an, die offline gegangen sind.
- **Action-Terminate** âÂ Â Dieses Feld gibt die Anzahl der Sitzungen an, die beendet wurden.
- **Server Retries** âÂ Â Dieses Feld gibt an, wie oft das OCS erneut versucht wurde.
- **Angenommene positive Sitzungen**:

  Current â Â Dieses Feld gibt die Anzahl der Sitzungen an, die sich derzeit in der SU-Zustand.

  Kumulative â Â Dieses Feld gibt die Gesamtzahl der Sitzungen an, die in den SU-Status versetzt wurden.

Geben Sie den Befehl **show active-charge sessions full** command ein, um Informationen zum SU-Status der Sitzung anzuzeigen. Hier eine Beispielausgabe:

```
#show active-charging sessions full all
..
..

Current Server Unreachable State: CCR-I

Interim Volume in Bytes (used / allotted): 84/ 200

Interim Time in Seconds (used / allotted): 80/ 3600

Server Retries (attempted / configured): 1/ 50
```

Hier einige wichtige Hinweise zu dieser Beispielausgabe:

- **Aktueller Server Unreachable State** âÂ Â Dieser Wert gibt an, ob der aktuelle SU-Status auf den CCR-I oder CCR-U zurückzuführen ist.
- **Zwischenvolumen in Byte (verwendet/zugeteilt)** âÂ Â Dies zeigt das Zwischenvolumen in Byte verwendet verwendet im Vergleich zu Byte zugewiesen.
- **Interim Time in Seconds (used/Allotted)** âÂ Â Diese zeigt das Zwischenvolumen in Sekunden verwendet, verglichen mit Sekunden zugeteilt.
- **Server Retries (versuchte/konfigurierte)** âÂ Â Dies ist die Anzahl der versuchten Server-

Wiederholungen versus, gegenüber der konfigurierten.

Zugehörige Informationen

- Befehlszeilenschnittstellenreferenz, StarOS, Version 16
- Technischer Support und Dokumentation - Â Â Cisco Systems