

# Fehlerbehebung RCMC-Gehäuse Wird aufgrund von RCM initiiertem Neuladen neu geladen

## Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[RCMChassisTrap neu laden](#)

[Datenerfassung und -analyse](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie `RCMChassisReload` Falle aufgrund von `RCM Initiated Reload` in StarOS.

## Hintergrundinformationen

Der Redundancy Configuration Manager (RCM) ist eine proprietäre Knoten-/Netzwerkfunktion (NF) von Cisco, die Redundanz der StarOS-basierten Benutzerebene (UP) bzw. Benutzerebenenfunktion (UPF) bietet. Der RCM bietet eine N:M-Redundanz von UP/UPFs, wobei "N" die Anzahl der aktiven UP/UPFs und kleiner als 10 ist und "M" die Anzahl der Standby-UP/UPFs in der Redundanzgruppe ist. Der RCM überwacht seine UP/UPFs auf Ausfälle und initiiert einen Switchover auf Standby-UP/UPFs.

Ungeplante Switchovers treten aufgrund von Problemen im UP auf und werden ohne manuellen Eingriff neu gestartet. Wenn ein ungeplanter Switchover stattfindet, erkennt der BFD-Monitor-Pod (Bidirectional Forwarding Detection), dass das UP ausgefallen ist, und veranlasst den RCM Controller, den Switchover-Mechanismus zu starten. Der RCM-Controller wählt einen Standby-UP und die Redundanz-Manager-PODs, um die Konfiguration und Prüfpunkte an den neuen UP weiterzuleiten.

Der manuelle Switchover kann vom RCM aus initiiert werden mit `rcm switchover source aus`.

## RCMChassisTrap neu laden

Die Fehlermeldung `RCMChassisReload` Falle aufgrund von `RCM Initiated Reload` wird in StarOS angezeigt.

Ähnliche Protokolle werden gemeldet, wenn das Neuladen aufgrund eines BFD-Fehlers und der manuellen Befehlsausführung erfolgt.

Protokolle aufgrund von BFD-Fehlern:

```
2022-Nov-03+12:35:28.682 [snmp 22002 info] [1/0/6083 <vpnmgr:5> trap_api.c:11832] [software internal system syslog] Internal trap notification 1427 (RCMChassisReload) RCM Chassis Reload
```

### Reason: (2) RCM Initiated Reload

```
2022-Nov-03+12:35:28.682 [srp 84201 info] [1/0/6083 <vpnmgr:5> vpnmgr_rcm.c:1492] [context: RCM, contextID: 5] [software internal system syslog] RCM: Attempting to reload UPF.  
2022-Nov-03+12:35:28.735 [snmp 22002 info] [1/0/5271 <cspctrl:0> trap_api.c:17907] [software internal system syslog] Internal trap notification 1521 (CseShutDownNotify) Shutdown reason "Reload chassis requested by CLI command"
```

### Protokolle aufgrund des manuellen Switchover-Befehls:

```
2022-Nov-03+12:41:04.984 [snmp 22002 info] [1/0/6073 <vpnmgr:5> trap_api.c:11832] [software internal system syslog] Internal trap notification 1427 (RCMChassisReload) RCM Chassis Reload  
Reason: (2) RCM Initiated Reload  
2022-Nov-03+12:41:04.984 [srp 84201 info] [1/0/6073 <vpnmgr:5> vpnmgr_rcm.c:1492] [context: RCM, contextID: 5] [software internal system syslog] RCM: Attempting to reload UPF.  
2022-Nov-03+12:41:05.014 [snmp 22002 info] [1/0/5265 <cspctrl:0> trap_api.c:17907] [software internal system syslog] Internal trap notification 1521 (CseShutDownNotify) Shutdown reason "Reload chassis requested by CLI command"
```

## Datenerfassung und -analyse

Die RCM-Switchovers werden im `rcm show-statistics switchover` Befehlsausgabe.

Im Beispiel ist der neueste Switchover um 15:28:14 on Nov 3

was due to BGP failover on the UP/UPF, while prior switchover was at 15:14:23 on Nov 3 due to manual command switchover from RCM.

```
[unknown] rcm# rcm show-statistics switchover  
Thu Nov 3 15:39:10.486 UTC+00:00  
message :  
{  
  "stats_history": [  
    {  
      "status": "Success",  
      "started": "Nov 3 15:28:12.315",  
      "ended": "Nov 3 15:28:14.107",  
      "switchoverreason": "BGP Failure",  
      "source_endpoint": "192.168.60.3",  
      "destination_endpoint": "192.168.60.4"  
    },  
    {  
      "status": "Success",  
      "started": "Nov 3 15:13:48.808",  
      "ended": "Nov 3 15:14:23.670",  
      "switchoverreason": "Planned Switchover",  
      "source_endpoint": "192.168.60.4",  
      "destination_endpoint": "192.168.60.3"  
    },  
    {
```

Falls der Grund für die `RCMChassisReload` wird nicht aus dem Protokoll identifiziert und sammelt dann die Daten:

- Sammeln `show support details` von aktiven und Standby-UP/UPFs.
- Erfassen Sie Syslog-Informationen von aktiven und Standby-UPs/UPFs.
- Sammeln `rcm support-summary` und Syslog-Informationen vom RCM abrufen.
- RCM Pod-Ereignisse überprüfen: Kubernetes-Pods verifizieren

```
ubuntu@CUPS-RCM-01:~$ kubectl get pods -n rcm  
NAME READY STATUS RESTARTS AGE  
documentation-65d698cfbb-194lg 1/1 Running 0 161d
```

```
etcd-rcm-etcd-cluster-0 2/2 Running 0 161d
grafana-dashboard-etcd-rcm-65bd789-t57pq 1/1 Running 0 161d
ops-center-rcm-ops-center-6f946946c7-wlpnq 5/5 Running 0 161d
prometheus-rules-etcd-5c5cff47c6-vlizr7 1/1 Running 0 161d
rcm-bfdmgr-7fd47466c4-xm99h 1/1 Running 0 161d
rcm-checkpointmgr-0 1/1 Running 0 161d
rcm-checkpointmgr-1 1/1 Running 0 161d
rcm-checkpointmgr-2 1/1 Running 0 161d
rcm-checkpointmgr-3 1/1 Running 0 161d
rcm-configmgr-569f6d89c5-g7ztg 1/1 Running 0 161d
rcm-controller-775c4cc7bb-q96m6 1/1 Running 0 161d
smart-agent-rcm-ops-center-5c475b6bd-2plc6 1/1 Running 1 161d
```

## Sammeln Sie die **describe** Kommando des Kontrollstellenmanagers

```
ubuntu@CUPS-RCM-01:~$ kubectl describe pod rcm-checkpointmgr-0 -n rcm
```

```
Name: rcm-checkpointmgr-0
Namespace: rcm
Priority: 0
Node: rcm/10.10.1.1
Start Time: Wed, 01 Jun 2022 23:38:40 +0000
Labels: component=rcm-checkpointmgr
controller-revision-hash=rcm-checkpointmgr-566cdd886f
release=rcm-rcm-chkptmgr
statefulset.kubernetes.io/pod-name=rcm-checkpointmgr-0
Annotations: cnf.projectcalico.org/containerID:
0dea15df9e41a9195d9827cdb257430bab3257bad3417281fb6c8f3d3ed146cc
cnf.projectcalico.org/podIP: 10.42.0.72/32
cnf.projectcalico.org/podIPs: 10.42.0.72/32
prometheus.io/port: 8081
prometheus.io/scrape: true
sidecar.istio.io/inject: false
Status: Running
IP: 10.10.0.72
IPs:
IP: 10.10.0.72
Controlled By: StatefulSet/rcm-checkpointmgr
Containers:
rcm-checkpointmgr:
Container ID: docker://b86826c43e191f0266a1489ef6f0398b21c1801d6a79e40093aed6e3c023ba4d
Image: dockerhub.cisco.com/smi-fuse-docker-internal/mobile-cnat-rcm/rcm-
chkptmgr/v21.27.x/rcm_chkptmgr:0.0.5-38a8de3
Image ID: docker://sha256:adc4013783f60f6413fa81eb2bf16a652fddcd8d164e469368c2587560e42bc8
Ports: 9900/TCP, 9300/TCP, 8080/TCP, 8081/TCP
Host Ports: 0/TCP, 0/TCP, 0/TCP, 0/TCP
Command:
/usr/local/bin/run-app
State: Running
Started: Wed, 01 Jun 2022 23:38:44 +0000
Ready: True
Restart Count: 0
Environment:
K8S_NAMESPACE: rcm
GODEBUG: madvdontneed=1
GOGC: 25
GOTRACEBACK: crash
SERVICE_NAME: rcm-checkpointmgr
DATACENTER_NAME: DC
CLUSTER_NAME: Local
APPLICATION_NAME: RCM
RCM_CHKPT_POD_IP: (v1:status.podIP)
RCM_CHKPT_POD_NAME: rcm-checkpointmgr-0 (v1:metadata.name)
INFRA_PROMETHEUS_PORT: 8081
Mounts:
/config/rcm-logging from rcm-logging-volume (ro)
```

```
/var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-6828r (ro)
Conditions:
Type Status
Initialized True
Ready True
ContainersReady True
PodScheduled True
Volumes:
rcm-logging-volume:
Type: ConfigMap (a volume populated by a ConfigMap)
Name: infra-logging-conf
Optional: false
kube-api-access-6828r:
Type: Projected (a volume that contains injected data from multiple sources)
TokenExpirationSeconds: 3607
ConfigMapName: kube-root-ca.crt
ConfigMapOptional: <nil>
DownwardAPI: true
QoS Class: BestEffort
Node-Selectors: nodeType=RCM
Tolerations: node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events: <none>
```

Überprüfen Sie die aktuellen Protokolle des Pod.

```
ubuntu@CUPS-RCM-01:~$ kubectl logs rcm-checkpointmgr-0 -n rcm | more
2022/11/09 20:19:01.554 rcm-checkpointmgr [DEBUG] [TopologyData.go:295]
[infra.topology.core] Setting state of the application as APP_STARTED
2022/11/09 20:19:01.558 rcm-checkpointmgr [DEBUG] [TopologyData.go:295]
[infra.topology.core] Setting state of the application as APP_STARTED
```

Wenn ein Pod abgestürzt ist, können die Protokolle des vorherigen Pod mit `-p` Option

```
ubuntu@CUPS-RCM-01:~$ kubectl logs
```

## Zugehörige Informationen

[RCM Konfigurations- und Administrationshandbuch](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.