

# Troubleshoot PCRf OAM VM Recovery-Openstack

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[CPS VNF Instance Recovery Procedures](#)

[Troubleshoot](#)

[Power on Any Instance from SHUTOFF State](#)

[Recover any Instance from ERROR State](#)

[CPS Application Recovery Procedure](#)

[PCRfCLIENT01 Recovery](#)

[PCRfCLIENT02 Recovery](#)

[Verify](#)

## Introduction

This document describes how to troubleshoot Policy Server (PS) Recovery.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge on these topics:

- Cisco Policy Suite (CPS)
- Openstack
- Compute on which affected instances were deployed now available.
- Compute resources are available in the same availability zone as the affected instance.
- Backup procedures as mentioned in the document are followed/scheduled periodically.

## Components Used

The information in this document is based on CPS and applicable to all versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

# CPS VNF Instance Recovery Procedures

In this section here as described:

- Restore any instance from SHUTOFF state.
- Restore any instance from ERROR state.

## Troubleshoot

### Power on Any Instance from SHUTOFF State

If any instance is in SHUTOFF state due to a planned shutdown or some other reason, please use this procedure to start the instance and enable it's monitoring in Elastic Service Controller (ESC).

Step 1. Check the state of instance via OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep oam-s1
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed |
SHUTOFF|
```

Step 2. Check if the compute is available and ensure state is up.

```
source /home/stack/destackovsrc
nova hypervisor-show destackovs-compute-2 | egrep 'status|state'
| state | up |
| status | enabled |
```

Step 3. Login to ESC Master as admin user and check the state of instance in opdata.

```
echo "show esc_datamodel opdata tenants tenant Pcrf deployments * state_machine | tab" |
/opt/cisco/esc/confd/bin/confd_cli -u admin -C | grep qns-s2
SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed VM_ERROR_STATE
```

Step 4. Power on the instance from openstack.

```
source /home/stack/destackovsrc-Pcrf
nova start SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed
```

Step 5. Wait five minutes for the instance to boot up and come to active state.

```
source /home/stack/destackovsrc-Pcrf
nova list -fields name,status | grep oam-s1
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed
| ACTIVE |
```

Step 6. Enable VM Monitor in ESC after instance is in active state.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed
```

For Further recovery of instance configurations, refer instance type specific procedures provided.

## Recover any Instance from ERROR State

This procedure can be used if state of CPS instance in openstack is ERROR:

Step 1. Check the state of instance in OpenStack.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,host,status | grep oam-s1
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 | SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed
| ERROR|
```

Step 2. Check if the compute is available and running fine.

```
source /home/stack/destackovsrc
nova hypervisor-show destackovs-compute-2 | egrep 'status|state'
| state                | up                |
| status               | enabled          |
```

Step 3. Login to ESC Master as admin user and Check the state of instance in opdata.

```
echo "show esc_datamodel opdata tenants tenant Pcrf deployments * state_machine | tab" |
/opt/cisco/esc/confd/bin/confd_cli -u admin -C | grep oam-s1
```

```
SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed VM_ERROR_STATE
```

Step 4. Reset the state of instance to force the instance back to an active state instead of an error state, once done, reboot your instance.

```
source /home/stack/destackovsrc-Pcrf
nova reset-state -active oam-s1_0_170d9c14-0221-4609-87e3-d752e636f57f
nova reboot --hard oam-s1_0_170d9c14-0221-4609-87e3-d752e636f57f
```

Step 5. Wait five minutes for the instance to boot up and come to active state.

```
source /home/stack/destackovsrc-Pcrf
nova list --fields name,status | grep oam-s1
| c5e4ebd4-803d-45c1-bd96-fd6e459b7ed6 |SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed |
ACTIVE |
```

Step 6. If, Cluster Manager changes state to ACTIVE after reboot, Enable VM Monitor in ESC after Cluster Manager instance is in active state.

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action ENABLE_MONITOR SVS1-tmo_oam-s1_0_fd8b0bb8-a2d7-4dae-8048-0c3d86c5d8ed
```

Step 7. Post recovery to running/active state, refer instance type specific procedure to recover config/data from backup.

## CPS Application Recovery Procedure

### PCRFCLIENT01 Recovery

Policy SVN recovery:

Mostly to keep Policy SVN in a different cinder volume, mounted on PCRFCLIENTXX at **/var/www/svn/repos/**, thus the changes of losing policy svn are reduced even if the instance is lost. If your deployment does not have a different cinder volume for policy svn, or the cinder where policy svn was stored is also lost, follow the follow procedure to recover Policy SVN on PCRFCLIENT01.

Step 1. Login to the Cluster Manager VM as the root user.

Step 2. Note the UUID of SVN repository through this command:

```
svn info http://pcrfclient02/repos | grep UUID
```

The command gives output the UUID of the repository:

**For Example Repository UUID: ea50bbd2-5726-46b8-b807-10f4a7424f0e**

Step 3. Check if the policy SVN is in sync when it uses the command provided. If a value is returned, then SVN is already in sync. And you don't need to sync it from PCRFCLIENT02 and you should skip step 4. Recovery from last backup can still be used of required as described later in this section.

```
/usr/bin/svn propget svn:sync-from-url --revprop -r0 http://pcrfclient01/repos
```

Step 4. Re-establish SVN master/slave synchronization between the pcrfclient01 and pcrfclient02 with pcrfclient01 as the master by executing series of commands on PCRFCLIENT01

```
/bin/rm -fr /var/www/svn/repos
/usr/bin/svnadmin create /var/www/svn/repos
/usr/bin/svn propset --revprop -r0 svn:sync-last-merged-rev 0
http://pcrfclient02/repos-proxy-sync
/usr/bin/svnadmin setuuid /var/www/svn/repos/ "Enter the UUID captured in step 2"
/etc/init.d/vm-init-client
/var/qps/bin/support/recover_svn_sync.sh
```

Step 5. If Policy SVN on PCRFCLIENT01 is in sync with PCRFCLIENT02, but the latest svn does not reflect in Policy Builder, it can be imported through the last backup with the command on Cluster Manager VM.

```
config_br.py -a import --svn /mnt/backup/<file-name.tgz>
```

### PCRFCLIENT02 Recovery

Mostly to keep Policy SVN in a different cinder volume, mounted on PCRCLIENTXX at **/var/www/svn/repos/**, thus the changes of losing policy svn are reduced even if the instance is lost. If your deployment do not have a different cinder volume for policy svn, or the cinder where policy svn was stored is also lost, follow the follow procedure to recover Policy SVN on PCRCLIENT02.

Step 1. Secure shell to the pcrclient01

```
ssh pcrclient01
```

Step 2. Run the script to sync the SVN repos from pcrclient01 to pcrclient02

```
/var/qps/bin/support/recover_svn_sync.sh
```

## Verify

Verify the health status of pcrclient:

```
run diagnostics.sh from pcrclient
```

Ensure that the PB, Control Centre & Grafana GUI are accessible & working properly.

- ```
run diagnostics.sh from pcrclient
```

  

```
run diagnostics.sh from pcrclient
```