

Procedimentos de backup e restauração para vários componentes Ultra-M - CPS

Contents

[Introduction](#)

[Informações de Apoio](#)

[Abreviaturas](#)

[Procedimento de backup](#)

[Backup de OSPD](#)

[Backup ESC](#)

[Backup do CPS](#)

[Procedimento de restauração](#)

[Recuperação de OSPD](#)

[Recuperação ESC](#)

[Recuperação de CPS](#)

Introduction

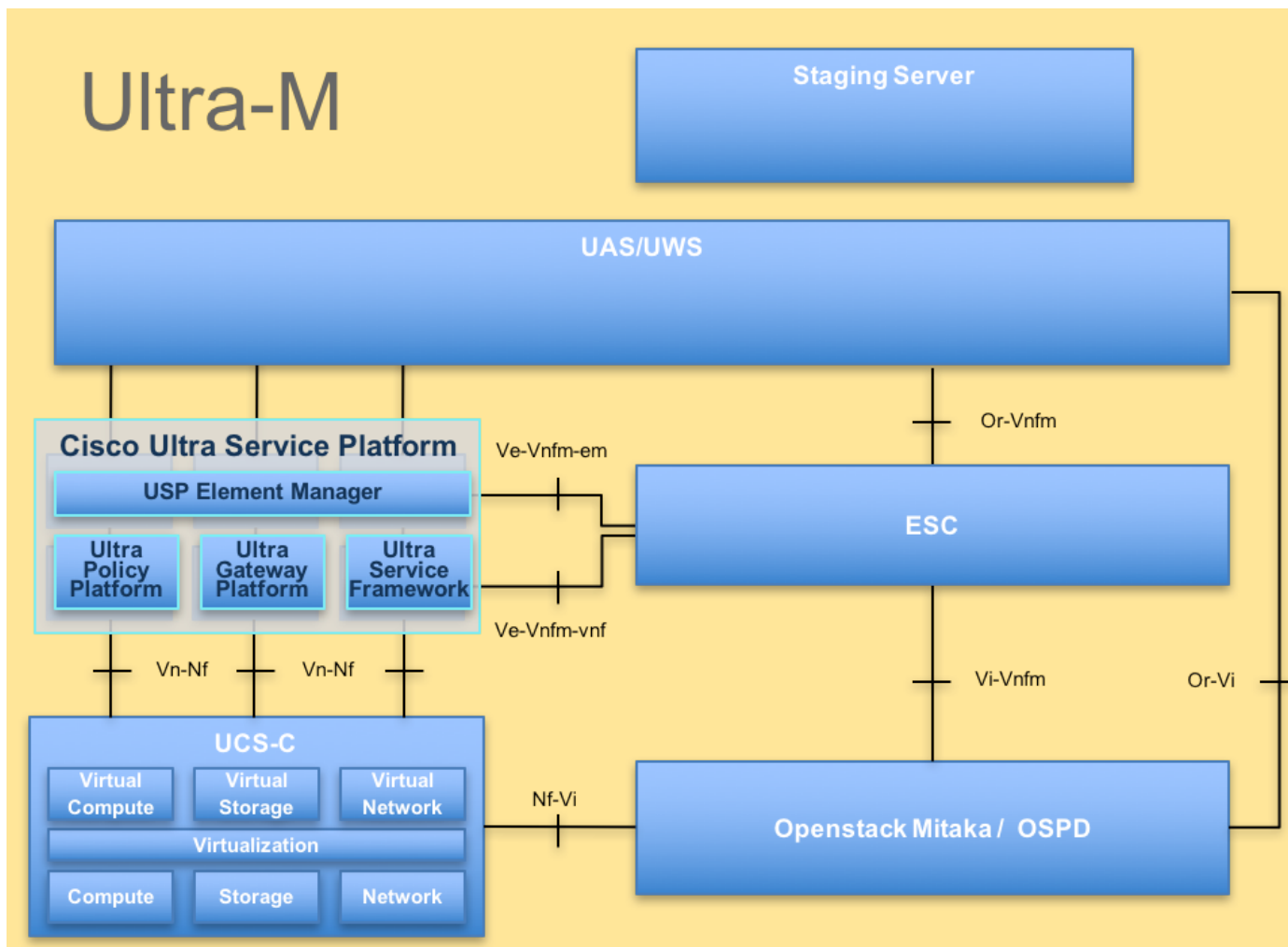
Este documento descreve as etapas necessárias para fazer backup e restaurar uma máquina virtual (VM) em uma configuração Ultra-M que hospeda as funções de rede virtual (VNFs) de chamadas CPS.

Informações de Apoio

O Ultra-M é uma solução de núcleo de pacotes móveis virtualizados, pré-embalada e validada, projetada para simplificar a implantação de VNFs. A solução Ultra-M consiste nos seguintes tipos de máquina virtual (VM):

- Controlador de serviços elásticos (ESC)
- Cisco Policy Suite (CPS)

A arquitetura de alto nível da Ultra-M e os componentes envolvidos são mostrados nesta imagem.



Note: A versão Ultra M 5.1.x é considerada para definir os procedimentos neste documento. Este documento destina-se ao pessoal da Cisco que conhece a plataforma Ultra-M da Cisco.

Abreviaturas

VNF	Função de rede virtual
ESC	Controlador de serviço elástico
MOP	Método de Procedimento
OSD	Discos de Armazenamento de Objeto
HDD	Unidade de disco rígido
SSD	Unidade de estado sólido
VIM	Virtual Infrastructure Manager
VM	Máquina virtual
UUID	Identificador de ID universal exclusivo

Procedimento de backup

Backup de OSPD

1. Verifique o status da pilha do OpenStack e a lista de nós.

```
[stack@director ~]$ source stackrc
[stack@director ~]$ openstack stack list --nested
[stack@director ~]$ ironic node-list
[stack@director ~]$ nova list
```

2. Verifique se todos os serviços em nuvem estão no status carregado, ativo e em execução no nó OSP-D.

```
[stack@director ~]$ systemctl list-units "openstack*" "neutron*" "openvswitch*"
```

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
neutron-dhcp-agent.service	loaded	active	running	OpenStack Neutron DHCP Agent
neutron-openvswitch-agent.service	loaded	active	running	OpenStack Neutron Open vSwitch Agent
neutron-ovs-cleanup.service	loaded	active	exited	OpenStack Neutron Open vSwitch Cleanup Utility
neutron-server.service	loaded	active	running	OpenStack Neutron Server
openstack-aodh-evaluator.service	loaded	active	running	OpenStack Alarm evaluator service
openstack-aodh-listener.service	loaded	active	running	OpenStack Alarm listener service
openstack-aodh-notifier.service	loaded	active	running	OpenStack Alarm notifier service
openstack-ceilometer-central.service	loaded	active	running	OpenStack ceilometer central agent
openstack-ceilometer-collector.service	loaded	active	running	OpenStack ceilometer collection service
openstack-ceilometer-notification.service	loaded	active	running	OpenStack ceilometer notification agent
openstack-glance-api.service	loaded	active	running	OpenStack Image Service (code-named Glance) API server
openstack-glance-registry.service	loaded	active	running	OpenStack Image Service (code-named Glance) Registry server
openstack-heat-api-cfn.service	loaded	active	running	Openstack Heat CFN-compatible API Service
openstack-heat-api.service	loaded	active	running	OpenStack Heat API Service
openstack-heat-engine.service	loaded	active	running	Openstack Heat Engine Service
openstack-ironic-api.service	loaded	active	running	OpenStack Ironic API service
openstack-ironic-conductor.service	loaded	active	running	OpenStack Ironic Conductor service
openstack-ironic-inspector-dnsmasq.service	loaded	active	running	PXE boot dnsmasq service for Ironic Inspector
openstack-ironic-inspector.service	loaded	active	running	Hardware introspection service for OpenStack Ironic
openstack-mistral-api.service	loaded	active	running	Mistral API Server
openstack-mistral-engine.service	loaded	active	running	Mistral Engine Server
openstack-mistral-executor.service	loaded	active	running	Mistral Executor Server
openstack-nova-api.service	loaded	active	running	OpenStack Nova API Server
openstack-nova-cert.service	loaded	active	running	OpenStack Nova Cert Server
openstack-nova-compute.service	loaded	active	running	OpenStack Nova Compute Server
openstack-nova-conductor.service	loaded	active	running	OpenStack Nova Conductor Server
openstack-nova-scheduler.service	loaded	active	running	OpenStack Nova Scheduler Server
openstack-swift-account-reaper.service	loaded	active	running	OpenStack Object Storage (swift) - Account Reaper
openstack-swift-account.service	loaded	active	running	OpenStack Object Storage (swift) - Account Server
openstack-swift-container-updater.service	loaded	active	running	OpenStack Object Storage (swift) - Container Updater

```

openstack-swift-container.service      loaded active running OpenStack Object Storage
(swift) - Container Server
openstack-swift-object-updater.service loaded active running OpenStack Object Storage
(swift) - Object Updater
openstack-swift-object.service        loaded active running OpenStack Object Storage
(swift) - Object Server
openstack-swift-proxy.service          loaded active running OpenStack Object Storage
(swift) - Proxy Server
openstack-zaqar.service                loaded active running OpenStack Message Queuing
Service (code-named Zaqar) Server
openstack-zaqar@1.service              loaded active running OpenStack Message Queuing
Service (code-named Zaqar) Server Instance 1
openvswitch.service                   loaded active exited  Open vSwitch

```

LOAD = Reflects whether the unit definition was properly loaded.

ACTIVE = The high-level unit activation state, i.e. generalization of SUB.

SUB = The low-level unit activation state, values depend on unit type.

37 loaded units listed. Pass --all to see loaded but inactive units, too.

To show all installed unit files use 'systemctl list-unit-files'.

3. Confirme se você tem espaço em disco suficiente disponível antes de executar o processo de backup. Espera-se que este touro tenha pelo menos 3,5 GB.

```
[stack@director ~]$df -h
```

4. Execute esses comandos como o usuário raiz para fazer backup dos dados do nó de nuvem para um arquivo chamado **undercloud-backup-[timestamp].tar.gz** e transfira-os para o servidor de backup.

```

[root@director ~]# mysqldump --opt --all-databases > /root/undercloud-all-databases.sql
[root@director ~]# tar --xattrs -czf undercloud-backup-`date +%F`.tar.gz /root/undercloud-all-
databases.sql
/etc/my.cnf.d/server.cnf /var/lib/glance/images /srv/node /home/stack
tar: Removing leading `/' from member names

```

Backup ESC

1. O ESC, por sua vez, ativa a Virtual Network Function (VNF) interagindo com o VIM.
2. O ESC tem redundância 1:1 na solução Ultra-M. Há 2 VMs ESC implantadas e suportam uma única falha no Ultra-M, ou seja, recuperam o sistema se houver uma única falha no sistema.

Note: Se houver mais de uma falha, ela não é suportada e pode exigir a reimplantação do sistema.

Detalhes do backup ESC:

- Configuração running
- CDB ConfD
- Logs ESC
- Configuração de syslog

3. A frequência do backup do banco de dados ESC é complicada e precisa ser tratada com cuidado enquanto o ESC monitora e mantém as várias máquinas de estado para várias VMs VNF implantadas. Recomenda-se que esses backups sejam realizados após as seguintes atividades em determinado VNF/POD/Site

4. Verifique se a integridade do ESC está boa usando o script health.sh.

```
[root@auto-test-vnfm1-esc-0 admin]# escadm status
0 ESC status=0 ESC Master Healthy

[root@auto-test-vnfm1-esc-0 admin]# health.sh
esc ui is disabled -- skipping status check
esc_monitor start/running, process 836
esc_mona is up and running ...
vimmanager start/running, process 2741
vimmanager start/running, process 2741
esc_confd is started
tomcat6 (pid 2907) is running... [ OK ]
postgresql-9.4 (pid 2660) is running...
ESC service is running...
Active VIM = OPENSTACK
ESC Operation Mode=OPERATION

/opt/cisco/esc/esc_database is a mountpoint

===== ESC HA (MASTER) with DRBD =====

DRBD_ROLE_CHECK=0
MNT_ESC_DATABASE_CHECK=0
VIMMANAGER_RET=0
ESC_CHECK=0
STORAGE_CHECK=0
ESC_SERVICE_RET=0
MONA_RET=0
ESC_MONITOR_RET=0

=====

ESC HEALTH PASSED
```

5. Faça o backup da configuração em execução e transfira o arquivo para o servidor de backup.

```
[root@auto-test-vnfm1-esc-0 admin]# /opt/cisco/esc/confd/bin/confd_cli -u admin -C

admin connected from 127.0.0.1 using console on auto-test-vnfm1-esc-0.novalocal
auto-test-vnfm1-esc-0# show running-config | save /tmp/running-esc-12202017.cfg
auto-test-vnfm1-esc-0#exit

[root@auto-test-vnfm1-esc-0 admin]# ll /tmp/running-esc-12202017.cfg
-rw-----. 1 tomcat tomcat 25569 Dec 20 21:37 /tmp/running-esc-12202017.cfg
```

Backup do banco de dados ESC

1. Faça login na VM ESC e execute o seguinte comando antes de fazer o backup.

```
[admin@esc ~]# sudo bash
[root@esc ~]# cp /opt/cisco/esc/esc-scripts/esc_dbtool.py /opt/cisco/esc/esc-
scripts/esc_dbtool.py.bkup
[root@esc esc-scripts]# sudo sed -i "s,'pg_dump','/usr/pgsql-9.4/bin/pg_dump,'"
/opt/cisco/esc/esc-scripts/esc_dbtool.py

#Set ESC to mainenance mode
[root@esc esc-scripts]# escadm op_mode set --mode=maintenance
```

2. Verifique o modo ESC e certifique-se de que ele esteja no modo de manutenção.

```
[root@esc esc-scripts]# escadm op_mode show
```

3. Banco de dados de backup usando a ferramenta de restauração de backup de banco de dados disponível em ESC.

```
[root@esc scripts]# sudo /opt/cisco/esc/esc-scripts/esc_dbtool.py backup --file  
scp://<username>:<password>@<backup_vm_ip>:<filename>
```

4. Defina ESC de volta para o modo de operação e confirme o modo.

```
[root@esc scripts]# escadm op_mode set --mode=operation
```

```
[root@esc scripts]# escadm op_mode show
```

5. Navegue até o diretório de scripts e colete os logs.

```
[root@esc scripts]# /opt/cisco/esc/esc-scripts
```

```
sudo ./collect_esc_log.sh
```

6. Para criar um instantâneo do ESC, desligue o ESC pela primeira vez.

```
shutdown -r now
```

7. A partir do OSPD, criar um instantâneo de imagem

```
nova image-create --poll escl esc_snapshot_27aug2018
```

8. Verifique se o snapshot foi criado

```
openstack image list | grep esc_snapshot_27aug2018
```

9. Iniciar o ESC do OSPD

```
nova start escl
```

10. Repita o mesmo procedimento na VM ESC em standby e transfira os registros para o servidor de backup

11. Coletar o backup da configuração do syslog no ESC VMS e transferi-lo para o servidor de backup

```
[admin@auto-test-vnfm2-esc-1 ~]$ cd /etc/rsyslog.d  
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/00-escmanager.conf  
00-escmanager.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/01-messages.conf  
01-messages.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/02-mona.conf  
02-mona.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.conf  
rsyslog.conf
```

Backup do CPS

1. Criar um backup do Gerenciador de cluster CPS

Use este comando para exibir as instâncias de nova e anote o nome da instância de VM do gerenciador de cluster:

```
nova list
```

Parar o cluman do ESC

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli vm-action STOP <vm-name>
```

Etapa 2. Verifique o gerenciador de cluster no estado SHUTOFF.

```
admin@esc1 ~]$ /opt/cisco/esc/confd/bin/confd_cli
```

```
admin@esc1> show esc_datamodel opdata tenants tenant Core deployments * state_machine
```

Etapa 3. Crie uma imagem de instantâneo nova conforme mostrado no seguinte comando:

```
nova image-create --poll
```

Note: Certifique-se de que você tenha espaço em disco suficiente para o snapshot.

Importante - Caso a VM se torne inalcançável após a criação do snapshot, verifique o status da VM usando o comando nova list. Se estiver no estado "SHUTOFF", você precisará iniciar a VM manualmente.

Etapa 4. Exiba a lista de imagens com o seguinte comando: nova image-list Figura 1: Saída de exemplo

ID	Name	Status	Server
146719e8-d8a0-4d5a-9b15-2a669cfab81f	CPS_10.9.9_20160803_100301_112.iso	ACTIVE	
1955d56e-4ecf-4269-b53d-b30e73ad57f0	base_vm	ACTIVE	
2bbfb51c-cd05-4b7c-ad77-8362d76578db	cluman_snapshot	ACTIVE	4842ae5a-83a3-48fd-915b-6ca6361adb2c

Etapa 5. Quando um snapshot é criado, a imagem do snapshot é armazenada no OpenStack Glance. Para armazenar o snapshot em um armazenamento de dados remoto, baixe o snapshot e transfira o arquivo no OSPD para (/home/stack/CPS_BACKUP)

Para baixar a imagem, use o seguinte comando no OpenStack:

```
glance image-download --file For example: glance image-download --file snapshot.raw 2bbfb51c-cd05-4b7c-ad77-8362d76578db
```

Etapa 6. Liste as imagens baixadas conforme mostrado no seguinte comando:

```
ls -ltr *snapshot*
```

Example output: -rw-r--r--. 1 root root 10429595648 Aug 16 02:39 snapshot.raw

Passo 7. Armazene o instantâneo da VM do Cluster Manager a ser restaurado no futuro.

2. Faça backup da configuração e do banco de dados.

1. `config_br.py -a export --all /var/tmp/backup/ATP1_backup_all_$(date +%Y-%m-%d).tar.gz` OR
2. `config_br.py -a export --mongo-all /var/tmp/backup/ATP1_backup_mongoall$(date +%Y-%m-%d).tar.gz`
3. `config_br.py -a export --svn --etc --grafanadb --auth-htpasswd --haproxy /var/tmp/backup/ATP1_backup_svn_etc_grafanadb_haproxy_$(date +%Y-%m-%d).tar.gz`
4. `mongodump - /var/qps/bin/support/env/env_export.sh --mongo /var/tmp/env_export_$(date +%Y-%m-%d).tgz`
5. `patches - cat /etc/broadhop/repositories`, check which patches are installed and copy those patches to the backup directory `/home/stack/CPS_BACKUP` on OSPD
6. backup the cronjobs by taking backup of the cron directory: `/var/spool/cron/` from the `Pcrfclient01/Cluman`. Then move the file to `CPS_BACKUP` on the OSPD.

Verifique na crontab -l se é necessário qualquer outro backup

Transferir todos os backups para o OSPD `/home/stack/CPS_BACKUP`

3. Arquivo de cópia de segurança do ESC Master

```
/opt/cisco/esc/confd/bin/netconf-console --host 127.0.0.1 --port 830 -u <admin-user> -p <admin-password> --get-config > /home/admin/ESC_config.xml
```

Transferir o arquivo em OSPD `/home/stack/CPS_BACKUP`

4. Fazer backup de entradas crontab -l

Crie um arquivo txt com crontab -l e ftp para um local remoto (em OSPD `/home/stack/CPS_BACKUP`)

5. Fazer um backup dos arquivos de rota do cliente LB e PCRF

```
Collect and scp the below configurations from both LBs and Pcrfclients  
route -n /etc/sysconfig/network-script/route-*
```

Procedimento de restauração

Recuperação de OSPD

O procedimento de recuperação do OSPD é executado com base nas seguintes suposições

1. O backup do OSPD está disponível no servidor OSPD antigo.
2. A recuperação do OSPD será feita no novo servidor, que é a substituição do antigo servidor

OSPD no sistema. .

Recuperação ESC

1. VM ESC é recuperável se a VM estiver em estado de erro ou desligamento, faça a reinicialização forçada para ativar a VM afetada. Execute estas etapas para recuperar o ESC.
2. Identifique a VM que está no estado ERROR ou Shutdown, depois de identificar a reinicialização forçada da VM ESC. Neste exemplo, você está reiniciando o teste automático-vnfm1-ESC-0.

```
[root@tb1-baremetal scripts]# nova list | grep auto-test-vnfm1-ESC-
| f03e3cac-a78a-439f-952b-045aea5b0d2c | auto-test-vnfm1-ESC-
0 | ACTIVE | - | running | auto-testautovnf1-
uas-orchestration=172.57.12.11; auto-testautovnf1-uas-
management=172.57.11.3
|
| 79498e0d-0569-4854-a902-012276740bce | auto-test-vnfm1-ESC-
1 | ACTIVE | - | running | auto-testautovnf1-
uas-orchestration=172.57.12.15; auto-testautovnf1-uas-
management=172.57.11.5
|
```

```
[root@tb1-baremetal scripts]# [root@tb1-baremetal scripts]# nova reboot --hard f03e3cac-a78a-
439f-952b-045aea5b0d2c\
Request to reboot server <Server: auto-test-vnfm1-ESC-0> has been accepted.
```

```
[root@tb1-baremetal scripts]#
```

3. Se a VM ESC for excluída e precisar ser exibida novamente. Siga abaixo a sequência de etapas

```
[stack@pod1-ospd scripts]$ nova list |grep ESC-1
| c566efbf-1274-4588-a2d8-0682e17b0d41 | vnfm1-ESC-ESC-
1 | ACTIVE | - | running | vnfm1-
UAS-uas-orchestration=172.168.11.14; vnfm1-UAS-uas-
management=172.168.10.4
|
```

```
[stack@pod1-ospd scripts]$ nova delete vnfm1-ESC-ESC-1
Request to delete server vnfm1-ESC-ESC-1 has been
accepted.
```

4. Se a VM ESC não for recuperável e exigir a restauração do banco de dados, restaure o banco de dados do backup anterior.

5. Para a restauração do banco de dados ESC, temos que garantir que o serviço esc seja interrompido antes de restaurar o banco de dados; Para o ESC HA, execute primeiro na VM secundária e depois na VM principal.

```
# service keepalived stop
```

6. Verifique o status do serviço ESC e certifique-se de que tudo esteja parado nas VMs primária e secundária para HA.

```
# escadm status
```

7. Execute o script para restaurar o banco de dados. Como parte da restauração do banco de dados para a instância do ESC recém-criada, a ferramenta também promoverá uma das instâncias para ser um ESC primário, montará sua pasta de banco de dados para o dispositivo drbd e iniciará o banco de dados PostgreSQL.

```
# /opt/cisco/esc/esc-scripts/esc_dbtool.py restore --file  
scp://<username>:<password>@<backup_vm_ip>:<filename>
```

8. Reinicie o serviço ESC para concluir a restauração do banco de dados. Para executar HA em ambas as VMs, reinicie o serviço keepalived.

```
# service keepalived start
```

9. Depois que a VM for restaurada e executada com êxito; certifique-se de que toda a configuração específica do syslog seja restaurada a partir do backup conhecido anterior. Verifique se ele foi restaurado em todas as VMs do ESC.

```
[admin@auto-test-vnfm2-esc-1 ~]$  
[admin@auto-test-vnfm2-esc-1 ~]$ cd /etc/rsyslog.d  
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/00-escmanager.conf  
00-escmanager.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/01-messages.conf  
01-messages.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.d/02-mona.conf  
02-mona.conf
```

```
[admin@auto-test-vnfm2-esc-1 rsyslog.d]$ls /etc/rsyslog.conf  
rsyslog.conf
```

10. Se o ESC precisar ser reconstruído do snapshot OSPD, use esse comando com o uso do snapshot obtido durante o backup.

```
nova rebuild --poll --name esc_snapshot_27aug2018 esc1
```

11. Verifique o status do ESC após a conclusão da reconstrução

```
nova list --fileds name,host,status,networks | grep esc
```

12. Verifique a integridade do ESC com o comando abaixo

```
health.sh
```

```
Copy Datamodel to a backup file
```

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli get esc_datamodel/opdata > /tmp/esc_opdata_`date  
+%Y%m%d%H%M%S`.txt
```

Quando o ESC não inicia a VM

- Em alguns casos, o ESC não iniciará a VM devido a um estado inesperado. Uma solução alternativa é executar um switchover ESC reinicializando o ESC mestre. A transição para o ESC levará cerca de um minuto. Execute health.sh no novo ESC mestre para verificar se ele está ativado. Quando o ESC se tornar Master, o ESC poderá corrigir o estado da VM e iniciar a VM. Como essa operação está agendada, você deve aguardar de 5 a 7 minutos para que

seja concluída.

- Você pode monitorar `/var/log/esc/yangesc.log` e `/var/log/esc/escmanager.log`. Se você NÃO vir a VM sendo recuperada após 5 a 7 minutos, o usuário precisaria ir e fazer a recuperação manual das VMs afetadas.
- Depois que a VM for restaurada e executada com êxito; certifique-se de que toda a configuração específica do syslog seja restaurada a partir do backup conhecido anterior. Verifique se ele foi restaurado em todas as VMs do ESC

```
root@abautotestvnm1em-0:/etc/rsyslog.d# pwd
/etc/rsyslog.d
```

```
root@abautotestvnm1em-0:/etc/rsyslog.d# ll
```

```
total 28
drwxr-xr-x  2 root root 4096 Jun  7 18:38 ./
drwxr-xr-x 86 root root 4096 Jun  6 20:33 ../]
-rw-r--r--  1 root root  319 Jun  7 18:36 00-vnmf-proxy.conf
-rw-r--r--  1 root root  317 Jun  7 18:38 01-ncs-java.conf
-rw-r--r--  1 root root  311 Mar 17  2012 20-ufw.conf
-rw-r--r--  1 root root  252 Nov 23  2015 21-cloudinit.conf
-rw-r--r--  1 root root 1655 Apr 18  2013 50-default.conf
```

```
root@abautotestvnm1em-0:/etc/rsyslog.d# ls /etc/rsyslog.conf
rsyslog.conf
```

Recuperação de CPS

Restaurar VM do Cluster Manager no OpenStack

Etapa 1 Copiar o snapshot de VM do gerenciador de cluster para o blade do controlador, conforme mostrado no seguinte comando:

```
ls -ltr *snapshot*
```

Example output: `-rw-r--r--. 1 root root 10429595648 Aug 16 02:39 snapshot.raw`

Etapa 2 Fazer upload da imagem do snapshot para o OpenStack do Datastore:

```
glance image-create --name --file --disk-format qcow2 --container-format bare
```

Etapa 3 Verificar se o snapshot foi carregado com um comando Nova, conforme mostrado no exemplo a seguir:

```
nova image-list
```

Figura 2: Saída de exemplo

ID	Name	Status	Server
146719e8-d8a0-4d5a-9b15-2a669cfab81f	CPS_10.9.9_20160803_100301_112.iso	ACTIVE	
1955d56e-4ecf-4269-b53d-b30e73ad57f0	base_vm	ACTIVE	
2bbfb51c-cd05-4b7c-ad77-8362d76578db	cluman_snapshot	ACTIVE	4842ae5a-83a3-48fd-915b-6ca6361adb2c
5eebff44-658a-49a5-a170-1978f6276d18	imported_image	ACTIVE	

Etapa 4 Dependendo se a VM do gerenciador de cluster existe ou não, você pode optar por criar o cluman ou reconstruir o cluman:

Se a instância da VM do Cluster Manager não existir, crie a VM Cluman com um comando Heat ou Nova como mostrado no exemplo a seguir:

Crie a VM Cluman com ESC

```
/opt/cisco/esc/esc-confd/esc-cli/esc_nc_cli edit-config /opt/cisco/esc/cisco-cps/config/gr/tmo/gen/<original_xml_filename>
```

O cluster PCRF será gerado com a ajuda do comando acima e, em seguida, restaurará as configurações do gerenciador de cluster a partir dos backups realizados com a restauração config_br.py, mongorestore a partir do dump tomado no backup

```
delete - nova boot --config-drive true --image "" --flavor "" --nic net-id=",v4-fixed-ip=" --nic net-id="network_id,v4-fixed-ip=ip_address" --block-device-mapping "/dev/vdb=2edbac5e-55de-4d4c-a427-ab24ebe66181:::0" --availability-zone "az-2:megh-os2-compute2.cisco.com" --security-groups cps_secgrp "cluman"
```

Se a instância da VM do Cluster Manager existir, use um comando nova rebuild para reconstruir a instância da VM Cluman com o snapshot carregado, como mostrado:

```
nova rebuild <instance_name> <snapshot_image_name>
```

Por exemplo:

```
nova rebuild cps-cluman-5f3tujqvbi67 cluman_snapshot
```

Etapa 5 Listar todas as instâncias conforme mostrado e verificar se a nova instância do gerenciador de cluster foi criada e está em execução:

```
nova list
```

Figura 3. Saída de exemplo

ID	Name	Status	Task State	Power State	Networks
ac3d2dbc-7b0e-4df4-a690-7f84ca3032bd	cluman	ACTIVE	-	Running	management=172.20.67.34; internal=172.20.70.34

Restaurar os patches mais recentes no sistema

1. Copy the patch files to cluster manager which were backed up in OSPD
/home/stack/CPS_BACKUP
2. Login to the Cluster Manager as a root user.
3. Untar the patch by executing the following command: tar -xvzf [patch name].tar.gz
4. Edit /etc/broadhop/repositories and add the following entry: file:/// \$path_to_the plugin/[component name]

5. Run `build_all.sh` script to create updated QPS packages:
`/var/qps/install/current/scripts/build_all.sh`
6. Shutdown all software components on the target VMs: `runonall.sh sudo monit stop all`
7. Make sure all software components are shutdown on target VMs: `statusall.sh`

Note: Todos os componentes do software devem exibir Não monitorado como o status atual.

8. Update the qns VMs with the new software using `reinit.sh` script:
`/var/qps/install/current/scripts/upgrade/reinit.sh`
9. Restart all software components on the target VMs: `runonall.sh sudo monit start all`
10. Verify that the component is updated, run: `about.sh`

Restaure os trabalhos em frente

1. Mova o arquivo de backup do OSPD para o Cluman/Pcrfclient01.
2. Execute o comando para ativar o cronjob a partir do backup.

```
#crontab Cron-backup
```

3. Verifique se os cronjobs foram ativados pelo comando abaixo.

```
#crontab -l
```

Restaurar VMs individuais no cluster

Para reimplantar a VM pcrfclient01:

Etapa 1 Fazer login na VM do Cluster Manager como o usuário raiz.

Etapa 2 Observe o UUID do repositório SVN usando o seguinte comando:

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

O comando exibirá o UUID do repositório.

Por exemplo: UUID do repositório: ea50bbd2-5726-46b8-b807-10f4a7424f0e

Etapa 3 Importar os dados de configuração do Policy Builder de backup no Cluster Manager, como mostrado no seguinte exemplo:

```
config_br.py -a import --etc-oam --svn --stats --grafanadb --auth-htpasswd --users  
/mnt/backup/oam_backup_27102016.tar.gz
```

Note: Muitas implantações executam um trabalho cron que faz backup dos dados de configuração regularmente. Consulte Backup do repositório de subversão para obter mais detalhes.

Etapa 4 Para gerar os arquivos de arquivo da VM no Cluster Manager usando as configurações mais recentes, execute o seguinte comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Etapa 5 Para implantar a VM pcrfclient01, execute um dos seguintes procedimentos:

No OpenStack, use o modelo HEAT ou o comando Nova para recriar a VM. Para obter mais informações, consulte o Guia de Instalação do CPS para OpenStack.

Etapa 6 Restabelecer Sincronização mestre/escravo SVN entre pcrfclient01 e pcrfclient02 com pcrfclient01 como mestre executando a seguinte série de comandos.

Se o SVN já estiver sincronizado, não emita esses comandos.

Para verificar se o SVN está sincronizado, execute o seguinte comando do pcrfclient02.

Se um valor for retornado, o SVN já está sincronizado:

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

Execute os seguintes comandos do 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
```

Etapa 7 Se pcrfclient01 também é a VM do árbitro, execute as seguintes etapas:

a) Crie os scripts mongosb start/stop com base na configuração do sistema. Nem todas as implantações têm todos esses bancos de dados configurados.

Note: Consulte /etc/broadhop/mongoConfig.cfg para determinar quais bancos de dados precisam ser configurados.

```
cd /var/qps/bin/support/mongo
```

```
build_set.sh --session --create-scripts
```

```
build_set.sh --admin --create-scripts
```

```
build_set.sh --spr --create-scripts
```

```
build_set.sh --balance --create-scripts
```

```
build_set.sh --audit --create-scripts
```

```
build_set.sh --report --create-scripts
```

b) Iniciar o processo mongo:

```
/usr/bin/systemctl start sessionmgr-XXXXX
```

c) Aguarde o árbitro iniciar e execute `diagnostics.sh -- get_réplica_status` para verificar a integridade do conjunto de réplicas.

Para reimplantar a VM pcrfclient02:

Etapa 1 Fazer login na VM do Cluster Manager como o usuário raiz

Etapa 2 Para gerar os arquivos de arquivo da VM no Cluster Manager usando as configurações mais recentes, execute o seguinte comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Etapa 3 Para implantar a VM pcrfclient02, execute um dos seguintes procedimentos: No OpenStack, use o modelo HEAT ou o comando Nova para recriar a VM. Para obter mais informações, consulte o Guia de Instalação do CPS para OpenStack.

Etapa 4 Secure shell para o pcrfclient01:

```
ssh pcrfclient01
```

Etapa 5 Executar o seguinte script para recuperar os acordos de recompra SVN do pcrfclient01:

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

Para reimplantar uma VM do gerente de sessão:

Etapa 1 Fazer login na VM do Cluster Manager como o usuário raiz

Etapa 2 Para implantar a VM do sessionmgr e substituir a VM com falha ou corrompida, execute um dos seguintes procedimentos:

No OpenStack, use o modelo HEAT ou o comando Nova para recriar a VM. Para obter mais informações, consulte o Guia de instalação do CPS para OpenStack

Etapa 3 Crie os scripts mongosb start/stop com base na configuração do sistema.

Nem todas as implantações têm todos esses bancos de dados configurados. Consulte `/etc/broadhop/mongoConfig.cfg` para determinar quais bancos de dados precisam ser configurados

```
cd /var/qps/bin/support/mongo
```

```
build_set.sh --session --create-scripts  
build_set.sh --admin --create-scripts  
build_set.sh --spr --create-scripts  
build_set.sh --balance --create-scripts  
build_set.sh --audit --create-scripts  
build_set.sh --report --create-scripts
```

Etapa 4 Proteger o shell para a VM do sessionmgr e iniciar o processo mongo:

```
ssh sessionmgrXX
```

```
/usr/bin/systemctl start sessionmgr-XXXXX
```

Etapa 5 Aguarde até que os membros iniciem e os membros secundários sincronizem e execute `diagnostics.sh — get_réplica_status` para verificar a integridade do banco de dados.

Etapa 6 Para restaurar o banco de dados do Session Manager, use um dos seguintes comandos de exemplo, dependendo se o backup foi executado com a opção `—mongo-all` ou `—mongo`:

- `config_br.py -a import --mongo-all --users /mnt/backup/Name of backup`

or

- `config_br.py -a import --mongo --users /mnt/backup/Name of backup`

Para reimplantar a VM do Policy Diretor (Balanceador de Carga):

Etapa 1 Fazer login na VM do Cluster Manager como o usuário raiz.

Etapa 2 Para importar os dados de configuração do Policy Builder de backup no Cluster Manager, execute o seguinte comando:

```
config_br.py -a import --network --haproxy --users /mnt/backup/lb_backup_27102016.tar.gz
```

Etapa 3 Para gerar os arquivos de arquivo da VM no Cluster Manager usando as configurações mais recentes, execute o seguinte comando:

```
/var/qps/install/current/scripts/build/build_svn.sh
```

Etapa 4 Para implantar a VM lb01, execute um dos seguintes procedimentos:

No OpenStack, use o modelo HEAT ou o comando Nova para recriar a VM. Para obter mais informações, consulte o Guia de Instalação do CPS para OpenStack.

Para reimplantar a VM do Servidor de Políticas (QNS):

Etapa 1 Fazer login na VM do Cluster Manager como o usuário raiz.

Etapa 2 Importar os dados de configuração do Policy Builder de backup no Cluster Manager, como mostrado no seguinte exemplo:

```
config_br.py -a import --users /mnt/backup/qns_backup_27102016.tar.gz
```

Etapa 3 Para gerar os arquivos de arquivo da VM no Cluster Manager usando as configurações mais recentes, execute o seguinte comando:


```
/var/qps/install/current/scripts/build/build_svn.sh
```

Etapa 4 Para implantar a VM qns, execute um dos seguintes procedimentos:
No OpenStack, use o modelo HEAT ou o comando Nova para recriar a VM. Para obter mais informações, consulte o Guia de instalação do CPS para OpenStack

Procedimento geral para restauração de banco de dados

Etapa 1 Execute o seguinte comando para restaurar o banco de dados:

```
config_br.py -a import --mongo-all /mnt/backup/backup_$(date +%Y%m%d%H%M%S).tar.gz where $(date +%Y%m%d%H%M%S) is the timestamp when the export was made.
```

Por exemplo,

```
config_br.py -a import --mongo-all /mnt/backup/backup_27092016.tgz
```

Etapa 2 Faça login no banco de dados e verifique se ele está em execução e está acessível:

1. Faça login no gerenciador de sessões:

```
mongo --host sessionmgr01 --port $port
```

onde \$port é o número da porta do banco de dados a ser verificado. Por exemplo, 27718 é a porta de saldo padrão.

2. Exiba o banco de dados executando o seguinte comando:

```
show dbs
```

3. Mude o shell mongo para o banco de dados executando o seguinte comando:

```
use $db
```

onde \$db é um nome de banco de dados exibido no comando anterior.

O comando 'use' alterna o shell mongo para esse banco de dados.

Por exemplo,

```
use balance_mgmt
```

4. Para exibir as coleções, execute o seguinte comando:

```
show collections
```

5. Para exibir o número de registros na coleção, execute o seguinte comando:

```
db.$collection.count()
```

For example, db.account.count()

O exemplo acima mostrará o número de registros na coleção "conta" no banco de dados Saldo

(balance_mgmt).

Restauração do repositório de subversão

Para restaurar os Dados de Configuração do Policy Builder a partir de um backup, execute o seguinte comando:

```
config_br.py -a import --svn /mnt/backup/backup_`date`.tgz where, `date` is the date when the cron created the backup file.
```

Restaurar painel do Grafana

Você pode restaurar o painel do Grafana usando o seguinte comando:

```
config_br.py -a import --grafanadb /mnt/backup/
```

Validando a restauração

Depois de restaurar os dados, verifique o sistema em funcionamento executando o seguinte comando:

```
/var/qps/bin/diag/diagnostics.sh
```