GR Installation - VMware

- GR Installation Process, page 1
- Overview, page 1
- Prerequisites, page 2
- Reference for CPS VM and Host Name Nomenclature, page 3
- Arbiter Installation, page 5
- Standalone Arbiter Deployment On VMware, page 8
- Configure Remote/Peer Site VM, page 11
- Database Configuration, page 14
- Balance Backup Database Configuration, page 16
- Session Cache Hot Standby, page 19
- Policy Builder Configuration, page 22
- Access Policy Builder from Standby Site when Primary Site is Down, page 26
- qns.conf Configuration Changes for Session Replication, page 27
- Configurations to Handle Database Failover when Switching Traffic to Standby Site Due to Load Balancer Fail/Down, page 28

GR Installation Process

In this chapter, Active/Standby Geographic Redundancy model has been used to describe the database and configuration changes required to modify the current installed HA system into Geo-HA.

If you want to deploy historical Active/Active model, just deploy additional flipped pair of this active/standby model.

Overview

An overview of active/standby model has been provided in this section.
1 Active/Standby solution has only one CPS cluster at each site, CA-PRI (referred as ClusterA Primary henceforth) at S1 site (referred as Geo-site-1/site-1 henceforth) and CA-SEC (referred as ClusterA secondary henceforth) at S2 site (referred as Geo-site-2/site-2 henceforth).

**Figure 1: Geographical Sites**

In the above figure, you have primary cluster (Geo Site 1/S1), secondary cluster (Geo Site 2/S2) and arbiter (Geo Site 3/S3).

- Geo site 1/S1 could be any site (for example, Mumbai)
- Geo site 2/S2 could be any site (for example, Chennai)
- Geo site 3/S3 could be any site (for example, Kolkata)

2 For Site1 PCEF, there are two CPS clusters. One is primary, CA-PRI on S1 and other is secondary, CA-SEC on S2. They are geographically redundant.

3 Upon failure of primary CPS Cluster, secondary CPS cluster would seamlessly serve the subscriber's sessions. For that, session replication is enabled between primary and secondary clusters and for session replication high bandwidth is expected. For more information, contact your Cisco technical representative.

4 We recommend to use Replication interface for Database replication between Geo sites (that is, S1 and S2) to segregate Network traffic with Database replication traffic. For example, setting up separate VLAN's for segregating Network and Database traffic.

5 The secondary CPS cluster is not configured as passive.

6 We recommend to place the arbiter on site-3.

7 We recommend the SPR and balance databases to be on SSD and session database to be on tmpfs for optimized performance.

**Prerequisites**

- Base install (CPS-HA) has been completed on both sites and verified basic validation on both sites.
- Call model has been validated on both HA sites as per your TPS/traffic.
- CPS VMs should have Replication IP address.
Familiarity with *CPS Installation Guide for VMware*.
Familiarity with *CPS Release Notes*.

- For third site, Arbiter must be deployed and running the same build (The ISO used to prepare the Geo-Redundant Setup).
- The database configuration is planned.

## Reference for CPS VM and Host Name Nomenclature

**Note**

This section is for reference only. You need to follow the nomenclature based on your network requirements. As a prerequisite, HA must be already deployed.

For better usability of the system, install the HA system according to the following nomenclature:

1. In order to know the exact geo site details, we recommend to have the following entries in VMSpecification sheet of CPS_deployment_config_template.xlsx or VMSpecification.csv.
   - Host Name Prefix field value as Sx:

<table>
<thead>
<tr>
<th>Cluster Name</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-PRI</td>
<td>S1-</td>
</tr>
<tr>
<td>CA-SEC</td>
<td>S2-</td>
</tr>
</tbody>
</table>

2. In order to know the exact cluster name and role (primary/secondary) details, we recommend to have the following entries in Hosts sheet of CPS_deployment_config_template.xlsx or Hosts.csv:
   - Guest Name field value as:
     - CA-PRI-XXX for primary cluster (like CA-PRI-lb01, CA-PRI-qns01, and so on.) and CA-SEC-XXX for secondary cluster (like CA-SEC-qsn01, CA-SEC-lb01, and so on.)

3. We recommend to distribute session manager VMs equally between primary and secondary clusters, example:
   - sessionmgr01, sessionmgr02, sessionmgr03, sessionmgr04 on CA-PRI and sessionmgr01, sessionmgr02, sessionmgr03, sessionmgr04 on CA-SEC

4. The following convention must be used while creating cross site replica-set for the session database:
   - You must create the session database replica-set members on same VM and same port on both sites. For example, among four replica-set members (except arbiter), if `sessionmgr01:27717` and `sessionmgr02:27717` are two members of replica-set from SITE1 then choose `sessionmgr01:27717` and `sessionmgr02:27717` of SITE2 as other two replica-set members as shown in following example:

   ```
   [SESSION-SET]
   SETNAME=set01
   ```
OPLOG_SIZE=5120
ARBITER=SITE-ARB-sessionmgr05:27717
ARBITER_DATA_PATH=/var/data/sessions.1/set1
PRIMARY-MEMBERS
MEMBER1=SITE1-sessionmgr01:27717
MEMBER2=SITE1-sessionmgr02:27717
SECONDARY-MEMBERS
MEMBER1=SITE2-sessionmgr01:27717
MEMBER2=SITE2-sessionmgr02:27717
DATA_PATH=/var/data/sessions.1/set1
[SESSION-SET-END]

5 pcrfclient01 and pcrfclient02 of each site require Management/Public IP

6 Site1 HA Blade naming conventions of VMs looks like (This information is for reference only):

Table 2: Naming Convention

<table>
<thead>
<tr>
<th>Blade</th>
<th>Virtual Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Blade 1</td>
<td>S1-CA-PRI-cm</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-lb01</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-pcrfclient01</td>
</tr>
<tr>
<td>CC Blade 2</td>
<td>S1-CA-PRI-lb02</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-pcrfclient02</td>
</tr>
<tr>
<td>CPS Blade 1</td>
<td>S1-CA-PRI-qns01</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-sessionmgr01</td>
</tr>
<tr>
<td>CPS Blade 2</td>
<td>S1-CA-PRI-qns02</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-sessionmgr02</td>
</tr>
<tr>
<td>CPS Blade 3</td>
<td>S1-CA-PRI-qns03</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-sessionmgr03</td>
</tr>
<tr>
<td>CPS Blade 4</td>
<td>S1-CA-PRI-qns04</td>
</tr>
<tr>
<td></td>
<td>S1-CA-PRI-sessionmgr04</td>
</tr>
</tbody>
</table>

7 Site2 HA configuration looks like (This information is for reference only):

Table 3: Naming Convention

<table>
<thead>
<tr>
<th>Blade</th>
<th>Virtual Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Blade 1</td>
<td>S1-CA-SEC-cm</td>
</tr>
<tr>
<td></td>
<td>S1-CA-SEC-lb01</td>
</tr>
<tr>
<td></td>
<td>S1-CA-SEC-pcrfclient01</td>
</tr>
</tbody>
</table>
## Arbiter Installation

### On Third Site

<table>
<thead>
<tr>
<th>Blade</th>
<th>Virtual Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Blade 2</td>
<td>S1-CA-SEC-lb02&lt;br&gt;S1-CA-SEC-perfclient02</td>
</tr>
<tr>
<td>CPS Blade 1</td>
<td>S1-CA-SEC-qns01&lt;br&gt;S1-CA-SEC-sessionmgr01</td>
</tr>
<tr>
<td>CPS Blade 2</td>
<td>S1-CA-SEC-qns02&lt;br&gt;S1-CA-SEC-sessionmgr02</td>
</tr>
<tr>
<td>CPS Blade 3</td>
<td>S1-CA-SEC-qns03&lt;br&gt;S1-CA-SEC-sessionmgr03</td>
</tr>
<tr>
<td>CPS Blade 4</td>
<td>S1-CA-SEC-qns04&lt;br&gt;S1-CA-SEC-sessionmgr04</td>
</tr>
</tbody>
</table>

**Important**

Currently, SNMP and statistics are not supported on third site arbiter.

Do not install Arbiter if third site is not there or Arbiter is already installed on primary site.

Additionally, if third site blades are accessible from one of the GR sites, you can spawn the Arbiter VM from one of the sites, say, Site1, and installer will sit on third site blades. In that case also, this section is not applicable. Just have appropriate configurations done *(On Primary Site, on page 8)* so that destination VM is on a third site's blade.

The automatic GR site failover happens only when arbiters are placed on third site thus we recommend the MongoDB arbiter to be on third site that is, S3.

**Note**

Arbiter VM name should be sessionmgrxx.

Site3 HA configuration looks like *(This information is for reference only)*:
Table 4: Naming Convention

<table>
<thead>
<tr>
<th>Blade</th>
<th>Virtual Machines</th>
<th>vCPU</th>
<th>Memory (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPS Blade 1</td>
<td>S3-ARB-cm</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>S3-CA-ARB-sessionmgr01</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>

For more information about deploying VMs, refer to *CPS Installation Guide for VMware*.

---

**Step 1**

Configure system parameters for deployment for new Arbiter VM. We need the following CSV files to deploy and configure arbiter VM:

They are:

- VLANs.csv
- Configuration.csv
- VMSpecification.csv
- AdditionalHosts.csv
- Hosts.csv

1. **VLAN.csv**: Here configurations need to be as per targeted deployment/availability. An example configuration is shown:

   **Table 5: VLAN.csv**

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Network Target Name</th>
<th>Netmask</th>
<th>Gateway</th>
<th>VIP Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>VM Network</td>
<td>x.x.x.x</td>
<td>x.x.x.x</td>
<td>-</td>
</tr>
<tr>
<td>Management</td>
<td>VM Network-1</td>
<td>x.x.x.x</td>
<td>x.x.x.x</td>
<td>-</td>
</tr>
</tbody>
</table>

2. **Configuration.csv**: Here configurations need to be as per targeted deployment/availability.

3. **VMSpecification.csv**: Here configurations need to be as per targeted deployment/availability.

4. **AdditionalHosts.csv**: Here configurations need to be as per targeted deployment/availability. An example configuration is shown where we need to provide site1 and site2 session managers details:

   **Table 6: AdditionalHosts.csv**

<table>
<thead>
<tr>
<th>Host</th>
<th>Alias</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp-primary</td>
<td>ntp</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>ntp-secondary</td>
<td>btp</td>
<td>x.x.x.x</td>
</tr>
</tbody>
</table>
5 Hosts.csv: Take the template file /var/qps/install/current/scripts/deployer/templates from Cluster Manager VM and make changes.

An example configuration is shown:

**Figure 2: Hosts.csv**

<table>
<thead>
<tr>
<th>Host</th>
<th>Alias</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-PRI-sessionmgr01</td>
<td>-</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>CA-PRI-sessionmgr02</td>
<td>-</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>CA-SEC-sessionmgr01</td>
<td>-</td>
<td>x.x.x.x</td>
</tr>
<tr>
<td>CA-SEC-sessionmgr02</td>
<td>-</td>
<td>x.x.x.x</td>
</tr>
</tbody>
</table>

**Note**

- Datastore name should be as per deployment/availability.
- Arbiter VM alias should be sessionmgrXX only. In the above example, it is sessionmgr01.

**Step 2** Convert the Excel spreadsheet into a CSV file and upload the file to the Cluster Manager VM in /var/qps/config/deploy/csv directory.

a) Execute the following commands to import CSV files and conversion to JSON data:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

b) Execute the following command to validate the imported data:

```
cd /var/qps/install/current/scripts/deployer/support/
python jvalidate.py
```

The above script validates the parameters in the Excel/csv file against the ESX servers to make sure ESX server can support the configuration and deploy VMs.

**Step 3** For each host that is defined in the Hosts sheet of the deployment spreadsheet, perform the manual deployment (Refer to the Manual Deployment section in the CPS Installation Guide for VMware).

**Example:**

An example is shown below:

```
/var/qps/install/current/scripts/deployer
./deploy.sh sessionmgr01
```
On Primary Site

Optional: Do not perform the following steps if Arbiter is installed on third site.

If third site is not available then deploy arbiter VM on Primary Cluster that is, CA-PRI.

Arbiter VM name should be sessionmgrXX only. XX should be replaced with a digit higher than the last used digit of the session manager. For example, if there are a total of six sessionmgrs (sessionmgr01-sessionmgr06) then, the Arbiter session manager must be sessionmgr07.

To deploy arbiter on primary site, perform the following steps:

Step 1 Configure system parameters for deployment.
Add the following arbiter entry in Hosts sheet of deployment template sheet or Hosts.csv file. An example entry is shown below:

Figure 3: Arbiter Entries

<table>
<thead>
<tr>
<th>Hypervisor Name</th>
<th>Guest Name</th>
<th>Role</th>
<th>Alias</th>
<th>Datastore</th>
<th>Networks --&gt;</th>
<th>Internal</th>
<th>Management Gx</th>
<th>Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.x.x.x</td>
<td>CA-PRI-sessionmgr07</td>
<td>smart</td>
<td>sessionmgr07</td>
<td>datastore1</td>
<td>x.x.x</td>
<td>x.x.x</td>
<td>x.x.x</td>
<td></td>
</tr>
</tbody>
</table>

Step 2 Import modified CSV files using the following command:
/var/qps/install/current/scripts/import/import_deploy.sh

Step 3 Execute the following command to validate the imported data:

cd /var/qps/install/current/scripts/deployer/support/
python jvalidate.py

Note The above script validates the parameters in the Excel/csv file against the ESX servers to make sure ESX server can support the configuration and deploy VMs.

Step 4 For each host that is defined in the Hosts sheet of the excel document perform the manual deployment (Refer to the Manual Deployment section in the CPS Installation Guide for VMware).
An example is shown below:

/var/qps/install/current/scripts/deployer
./deploy.sh sessionmgr07

Standalone Arbiter Deployment On VMware

To install Arbiter on VM, perform the following steps:
Before You Begin

whi

---

**Step 1** Convert the Cluster Manager VM to an Arbiter (VMware).

*Note* Here you are converting the Cluster Manager deployed at Site3 to an Arbiter. For more information on how to deploy Cluster Manager VM, refer to *Deploy the Cluster Manager VM* section in the *CPS Installation Guide for VMware*.

**Step 2** Run `install.sh` from ISO directory.

cd /mnt/iso
./install.sh

Please enter install type [mobile|wifi|mog|pats|arbiter|dra|andsf]: arbiter ----> Select arbiter for this option

Would you like to initialize the environment... [y|n]: y ----> Enter y to continue

**Step 3** When prompted for Please pick an option for this setup:

Select 1 for new Arbiter deployment. For further steps, refer to Example: New Deployment of Arbiter, on page 10.

**Step 4** To enable the firewall, it is required to add the following configuration in `/etc/facter/facts.d/qps_firewall.txt` file:

```plaintext
firewall_disabled=0
internal_address=XX.XX.XX.XX ---> update XX.XX.XX.XX to your internal IP address
internal_device=0 ---> update 0 to your device ID
internal_guest_nic=eth0 ---> update eth0 to other port if it is not using default NIC for internal address
```

**Step 5** When `install.sh` finishes its run, execute the `reinit.sh` script to apply the appropriate configurations to the system:

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

**Step 6** After performing the upgrade/new installation, unmount the ISO image. This prevents any “device is busy” errors when a subsequent upgrade/new installation is performed.

```
cd /root
umount /mnt/iso
```

**Step 7** (Optional) After unmounting the ISO, delete the ISO image to free the system space.

```
rm xxxx.iso
```

where, `xxxx.iso` is the name of the ISO image used.

**Step 8** (Optional) Change the host name of the Arbiter.

a) Run `hostname xxx`, where `xxx` is the new host name for the Arbiter.

b) Edit `/etc/sysconfig/network` to add the new host name for the Arbiter.
Example: New Deployment of Arbiter

Step 1
Install arbiter VM.

cd /mnt/iso
./install.sh
Please enter install type [mobile|wifi|mog|arbiter]: arbiter

--------------------------------
Install Configuration
type: arbiter
version: 8.9.9
dir: /var/qps/install/8.9.9
--------------------------------
Extracting Installation Scripts...
Extracting Puppet Files...
Extracting RPM Files...
Bootstrapping yum repository...
Copying qps software...
Done copying file to: /var/qps/install/8.9.9
Would you like to initialize the environment... [y|n]: y
Initializing vmware specific configuration ...
Attempting to upgrade java with yum
Attempting to upgrade httpd with yum
Attempting to upgrade vim with yum
Attempting to upgrade genisoimage with yum
Attempting to upgrade svn with yum
Attempting to upgrade mongo with yum
Attempting to upgrade mongorestore with yum
Attempting to upgrade nc with yum
Attempting to upgrade socat with yum
Attempting to upgrade bc with yum
Attempting to install bash with yum
Attempting to upgrade pystache with yum
Attempting to upgrade fab with yum
Attempting to upgrade sshpass with yum
Attempting to upgrade openssl with yum
Attempting to install nss with yum
Attempting to upgrade telnet with yum
Attempting to upgrade traceroute with yum
Attempting to upgrade unzip with yum
Attempting to upgrade python with yum
Attempting to upgrade wget with yum

iptables: Setting chains to policy ACCEPT: filter [ OK ]
nptables: Flushing firewall rules: [ OK ]
nptables: Unloading modules: [ OK ]
Starting httpd:
[DONE] vmware specific configuration ...
Done adding /etc/profile.d/broadhop.sh
Please select the type of installation to complete:
1) New Deployment
2) Upgrade from existing 9.0 system
3) In-Service Upgrade from 7.0.5 onwards (eg: 7.0.5 to 9.x)

Deploying...
Copying /etc/puppet to /var/qps/images/puppet.tar.gz...
Creating MD5 Checksum...
Updating tar from: /var/qps/env_config/ to /var/www/html/images/
Creating MD5 Checksum...
Building /var/qps/bin...
Copying /var/qps/bin to /var/qps/images/scripts_bin.tar.gz...
Creating MD5 Checksum...
Building local facter ...
Creating facter file /etc/facter/facts.d/qps_facts.txt...

Step 2
Re-initiate the feature files by executing the following command:
/var/qps/install/current/scripts/upgrade/reinit.sh

---

### Configure Remote/Peer Site VM

#### Session Manager VM Information on Local Site

**Note**
The following steps need to be performed on other sites as well.

**Note**
In this section, to configure remote/peer site VM in local site, sessionmgr has been taken as an example. You can use this section to add peer policy server (qns) and peer policy directors (lbs) entries in AdditionalHosts file.

---

**Step 1**

Add the following entry in AdditionalHosts sheet of CPS deployment template or AdditionalHosts.csv on CA-PRI-cm: Objective of this section is for primary cluster to add other cluster (that is, secondary cluster) session manager's details.

a) Add sessionmgr VM information of secondary cluster (that is, Name, Replication Interface IP addresses).
b) In Alias column add psessionmgrxx (that is, peer sessionmgr).
c) Add arbiter VM entry, also in Alias column add the same host name.

- If it is on third site, then add IP address of arbiter VM which is reachable from all other sessionmgrs from both sites.
- Else add internal interface IP address of arbiter VM.

**Example:**

---
Policy Director (lb) VM Information on Local Site

Before You Begin
Redis must be enabled as IPC. For more information on how to enable REDIS, refer to CPS Installation Guide for VMware.

Step 1
Add the following entry in AdditionalHosts sheet of CPS deployment template or AdditionalHosts.csv on CA- Site1-cm: Objective of this section is for local site to add other site (that is, remote clusters) policy director (lb) VM details.

a) Add policy director (lb) VM information of secondary cluster (that is, Name, Policy Director (LB) External Interface Name).

b) In Alias column add plbx (that is, peer policy director (lb). For example, plb01, plb02 and so on).
Add IP address of remote policy director (lb) VM which is reachable from all policy director (lb) VMs of primary cluster.

Example:
Example of /var/qps/config/deploy/csv/AdditionalHosts.csv (on CA- Site1-cm):

<table>
<thead>
<tr>
<th>Host</th>
<th>Alias</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-Site2-lb01, plb01</td>
<td>xx.xx.xx.xx</td>
<td></td>
</tr>
<tr>
<td>CA-Site2-lb02, plb02</td>
<td>xx.xx.xx.xx</td>
<td></td>
</tr>
</tbody>
</table>

Step 2 Add the number of remote redis instances in Configuration.csv with key as remote_redis_server_count and value as the number of redis instances running on remote site:
Example:
If the remote site contains three redis instances per policy director (lb), add the following:
```
remote_redis_server_count,3
```
For more information in `remote_redis_server_count`, refer to CPS Installation Guide for VMware.

Step 3  Import modified CSV files by executing the following command:
```
/var/qps/install/current/scripts/import/import_deploy.sh
```

Step 4  Update redis entry `-DenableQueueSystem=true` in `/etc/broadhop/qns.conf` file if redis is enabled for IPC.

Step 5  Execute the following commands in Cluster Manager to copy updated `/etc/hosts` file to all deployed VMs:
```
SSHUSER_PREFERROOT=true copytoall.sh /etc/hosts /etc/hosts
```
```
copytoall.sh /etc/broadhop/redisTopology.ini /etc/broadhop/redisTopology.ini
```

Step 6  Verify that the `/etc/broadhop/redisTopology.ini` contains the remote policy director (lb) redis instances entry as follows:
```
cat /etc/broadhop/redisTopology.ini
```
```
policy.redis.qserver.1=lb01:6379
policy.redis.qserver.2=lb01:6380
policy.redis.qserver.3=lb01:6381
policy.redis.qserver.4=lb02:6379
policy.redis.qserver.5=lb02:6380
policy.redis.qserver.6=lb02:6381
remote.policy.redis.qserver.1=plb01:6379
remote.policy.redis.qserver.2=plb01:6380
remote.policy.redis.qserver.3=plb01:6381
remote.policy.redis.qserver.4=plb02:6379
remote.policy.redis.qserver.5=plb02:6380
remote.policy.redis.qserver.6=plb02:6381
```

If the number of redis instances/lb instances are to be increased/decreased on the remote cluster(s), the same should first be updated in all other clusters in the CSV files as mentioned in Step 1, on page 12 and Step 2, on page 12.

Repeat the steps from Step 3, on page 13 to Step 6, on page 13 after changing the CSV files so as to update the `redisTopology` file on all the VMs.
Database Configuration

While configuring mongo ports in a GR environment, there should be a difference of 100 ports between two respective sites. For example, consider there are two sites: Site1 and Site2. For Site1, if the port number used is 27717, then you can configure 27817 as the port number for Site2. This is helpful to identify a mongo member’s site. By looking at first three digits, one can decide where the mongo member belongs to. However, this is just a guideline. You should avoid having mongo ports of two different sites to close to each other (for example, 27717 on Site-1 and 27718 on Site2).

**Reason:** The reason is that the build_set.sh script fails when you create shards on the site (for example, Site1). This is because the script calculates the highest port number in the mongoConfig on the site where you are creating shards. This creates clash between the replica-sets on both sites. Since the port number which it allocates might overlap with the port number of mongoConfig on other site (for example, Site2). This is the reason why there should be some gap in the port numbers allocated between both the sites.

---

**Step 1**
Log in to pcrfclient01 as root user.

**Step 2**
Modify the /etc/broadhop/gr_cluster.conf file.

a) Add cluster name that is, clusterA followed by pcrfclient01/pcrfclient02 management interface public IP address of the Primary ClusterA.

   For example, `clusterA:xx.xx.xx.xx:yy.yy.yy.yy`

   where,

   `xx.xx.xx.xx` is the pcrfclient01 management interface public IP address of the Primary ClusterA.

   `yy.yy.yy.yy` is the pcrfclient02 management interface public IP address of the Primary ClusterA.

b) On next line add site name that is, clusterA followed by pcrfclient01/pcrfclient02 Management-interface public IP address of the Secondary ClusterA (these public IP addresses should be pingable from Site1).

   For example, `clusterA:xx.xx.xx.xx:yy.yy.yy.yy`

   where,

   `xx.xx.xx.xx` is the pcrfclient01 management interface public IP address of the Secondary ClusterA.

   `yy.yy.yy.yy` is the pcrfclient02 management interface public IP address of the Secondary ClusterA.

These entries need to match with site name entries without suffix _PRI/_SBY given in qns.conf file.

File contents will look like:
```
cat /etc/broadhop/gr_cluster.conf
#<site name>:<pcrfclient01 IP address>:<pcrfclient02 IP address>
#Primary sites
#Secondary sites
```

**Step 3**
Verify MongoConfig: Do not miss to add `#SITE_START` and `#SITE_END` tags to the block of replica set entries in /etc/broadhop/mongoConfig.cfg file, where `x` is the site number. To add these tags at proper location, refer to sample configuration file (`geo_mongoconfig_template`) present in /etc/broadhop directory.
Example:
For example, if Site1 and Site2 are the two sites, then you need to add Site1 and Site2 entries in mongoconfig.cfg file as per the sample configuration file (geo_mongoconfig_template) present in /etc/broadhop directory.

Step 4 After configuring mongoConfig.cfg file, install databases using build_set.sh script.

Step 5 For pcrfclient01, set priority 2 for primary site replica-set members, which are replicated across site(s) using the following mentioned example commands:

Example:
cd /var/qps/bin/support/mongo/; ./set_priority.sh --db session
cd /var/qps/bin/support/mongo/; ./set_priority.sh --db spr
cd /var/qps/bin/support/mongo/; ./set_priority.sh --db admin
cd /var/qps/bin/support/mongo/; ./set_priority.sh --db balance

Note: set_priority.sh command be executed from Cluster Manager.

Step 6 Verify replica set status and priority is set correctly using the following command from pcrfclient01:
diagnostics.sh --get_replica_status

Step 7 When the Session replication is configured then the Host collection of the Cluster database should have all the “admin replica-set” members, entries with Internal and Replication VLAN IP’s. By default, db.hosts file gets populated if you configure /etc/broadhop/gr_cluster.conf file. If the entries are not present then use the following commands to add these entries (XX is internal/replication IP address of “admin replica-set” and YY is siteld (defined in qns.conf):

```
mongo --host <admin DB primary host> --port <admin DB port> clusters
> db.hosts.update({"ip" : "XX"},{"siteName" : "YY", "ip" : "XX"}, true)
```

Example:
```
[root@CA-PRI-pcrfclient01 mongo]# mongo CA-PRI-sessionmgr02:27721/clusters
MongoDB shell version: 2.6.3
connecting to: CA-PRI-sessionmgr02:27721/clusters
set05:PRIMARY> db.hosts.find()
{ "id" : ObjectId("545e0596f4ce7b3cc119027d"), "siteName" : "clusterA_PRI", "ip" : "192.168.109.127" }
{ "id" : ObjectId("545e0596f4ce7b3cc119027e"), "siteName" : "clusterA_PRI", "ip" : "192.168.109.128" }
{ "id" : ObjectId("545e0596f4ce7b3cc1190281"), "siteName" : "clusterA_SBY", "ip" : "192.168.109.227" }
{ "id" : ObjectId("545e0596f4ce7b3cc1190282"), "siteName" : "clusterA_SBY", "ip" : "192.168.109.228" }
```

(Optional) By default, db.hosts gets populated if there is a difference between IP addresses of sessionmgr* VMs in /etc/hosts file on both sites.

Example:
For sessionmgr01 SITE-A, in /etc/hosts file, if the entry is: 10.10.10.1 sessionmgr01 sessionmgr01-SITE-A
and for SITE-B on sessionmgr01, in /etc/hosts, if the entry is: 172.20.20.1 sessionmgr01-SITE-A
As, IP addresses of sessionmgr VMs are different in this case, user needs to run the following scripts on both SITES.

```bash
cd /var/qps/bin/support/mongo/; ./set_clusterinfo_in_admindb.sh
```

**Step 8**
From primary pcrcfclient01 copy `mongoConfig.cfg` and `gr_cluster.conf` files to both primary and secondary Cluster Managers (CM).

**Step 9**
From both CMs, execute the following commands, where first one will build "etc" and next two will copy these files to all other deployed VMs:

```bash
/var/qps/install/current/scripts/build/build_etc.sh
SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/gr_cluster.conf /etc/broadhop/gr_cluster.conf
SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/mongoConfig.cfg /etc/broadhop/mongoConfig.cfg
```

---

**Balance Backup Database Configuration**

CPS provides extra high availability for balance database during failover. During failover or switchover, or when primary is not available due to network reachability, balance writes happen in the backup database. After primary database is available, the records in backup database are reconciled with the primary.

The balance backup database configuration in mongoConfig appears like any other balance database with two members of replica-set on a given site. The replica-set must be created in the same manner in which regular balance database replica-sets are created.

---

**Step 1**
In Policy Builder, click **Reference Data > Systems > name of your primary system > Plugin Configurations** and select **Balance Configuration** from right side. In **Balance Configuration**, configure the primary database information. For parameter description, refer to **CPS Mobile Configuration Guide**.

An example configuration is shown:

**Figure 4: Balance Backup Database Configuration - 1**

---

**CPS Geographic Redundancy Guide, Release 12.0.0**
Step 2

In Policy Builder, click Reference Data > Systems > name of your backup system > Plugin Configurations and select Balance Configuration from right side. In Balance Configuration, configure the backup database information. For parameter description, refer to CPS Mobile Configuration Guide.

An example configuration is shown:

Figure 5: Balance Backup Database Configuration - 2

Step 3

The following is an example output for balance backup database:

diagnostics.sh --get_re

The balance database replica-sets for Site1 and Site2 are displayed in the example output.

CPS Diagnostics GR Multi-Node Environment

------------------------------------------
Checking replica sets...

|set name| port | ip address| replica state| host name| health| last sync| priority|
------------------------------------------
| ADMIN:set08|
| Member-1| 27721| 172.20.18.54| ARBITER| L2-CA-ARB-sessionmgr15| ON-LINE| 1 sec| 1 |
| Member-2| 27721| 172.20.17.83| PRIMARY| L2-CA-PRI-sessionmgr09| ON-LINE| 1 sec| 2 |
| Member-3| 27721| 172.20.17.87| SECONDARY| L2-CA-PRI-sessionmgr10| ON-LINE| 1 sec| 3 |

CPS Geographic Redundancy Guide, Release 12.0.0
<table>
<thead>
<tr>
<th>BALANCE:set05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member-1 - 27718 : 172.20.18.54 - ARBITER - L2-CA-ARB-sessionmgr15 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 3</td>
</tr>
<tr>
<td>Member-2 - 27718 : 172.20.17.40 - PRIMARY - L2-CA-PRI-sessionmgr02 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 4</td>
</tr>
<tr>
<td>Member-3 - 27718 : 172.20.17.38 - SECONDARY - L2-CA-PRI-sessionmgr01 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
<tr>
<td>Member-4 - 27718 : 172.20.19.29 - SECONDARY - L2-CA-SEC-sessionmgr02 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 2</td>
</tr>
<tr>
<td>Member-5 - 27718 : 172.20.19.27 - SECONDARY - L2-CA-SEC-sessionmgr01 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BALANCE:set09a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member-1 - 47718 : 172.20.18.54 - ARBITER - L2-CA-ARB-sessionmgr15 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 0</td>
</tr>
<tr>
<td>Member-2 - 47718 : 172.20.17.87 - PRIMARY - L2-CA-PRI-sessionmgr10 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 2</td>
</tr>
<tr>
<td>Member-3 - 47718 : 172.20.17.83 - SECONDARY - L2-CA-PRI-sessionmgr09 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BALANCE:set10a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member-1 - 17718 : 172.20.18.54 - ARBITER - L2-CA-ARB-sessionmgr15 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 0</td>
</tr>
<tr>
<td>Member-2 - 17718 : 172.20.17.83 - PRIMARY - L2-CA-PRI-sessionmgr09 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 2</td>
</tr>
<tr>
<td>Member-3 - 17718 : 172.20.17.87 - SECONDARY - L2-CA-PRI-sessionmgr10 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REPORTING:set07</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member-1 - 27719 : 172.20.18.54 - ARBITER - L2-CA-ARB-sessionmgr15 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 0</td>
</tr>
<tr>
<td>Member-2 - 27719 : 172.20.17.44 - PRIMARY - L2-CA-PRI-sessionmgr04 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 2</td>
</tr>
<tr>
<td>Member-3 - 27719 : 172.20.17.42 - SECONDARY - L2-CA-PRI-sessionmgr03 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SESSION:set01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member-1 - 27717 : 172.20.18.54 - ARBITER - L2-CA-ARB-sessionmgr15 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 0</td>
</tr>
<tr>
<td>Member-2 - 27717 : 172.20.17.38 - PRIMARY - L2-CA-PRI-sessionmgr01 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 4</td>
</tr>
<tr>
<td>Member-3 - 27717 : 172.20.17.40 - SECONDARY - L2-CA-PRI-sessionmgr02 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 3</td>
</tr>
<tr>
<td>Member-4 - 27717 : 172.20.19.27 - SECONDARY - L2-CA-SEC-sessionmgr01 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 2</td>
</tr>
<tr>
<td>Member-5 - 27717 : 172.20.19.29 - SECONDARY - L2-CA-SEC-sessionmgr02 - ON-LINE -</td>
</tr>
<tr>
<td>0 sec - 1</td>
</tr>
</tbody>
</table>
### Session Cache Hot Standby

---

**Important** Cisco recommends to configure standby session for GR.

CPS runs a distributed database called MongoDB. MongoDB uses a replication concept for high availability called replica-sets. A replica-set is made up of independent MongoDB instances that run in one of the following three modes:

- **Primary**: A primary database is the only database available that can accept writes.
• Secondary: A secondary database is a database that is read only and is actively synchronizing to a primary database by replaying the primary's oplog (operations log) on the local node.

• Recovering: A secondary database that is currently synchronizing to the primary and has not caught up to the primary.

Session data is highly concurrent, the application always reads and writes from the primary database. The secondary database(s) provide HA for the primary in the event of VM shutdown or process shutdown. Hot standby session cache replica set is configured to take over the load while primary database is failing over to secondary session cache database. In this fail-over process, it minimizes the call failures and provides high system availability.

Prerequisites

• Hot standby replica-set must be created on different blades (for maximum protection).

• Admin database and session cache databases must be separate replica-sets.

• Hot standby replica-set should be added to shard configuration as backup database true.

Configuration

**Step 1**
The hotstandby database must be configured just like any other session cache database in mongo config and a replica-set needs to be created.
The following is an example backup database configuraton in mongoDB:

```
[SESSION-SET1] SETNAME=set01
ARBITER=pcrfclient01-prim-site-1:37718
ARBITER_DATA_PATH=/data/sessions.3
MEMBER1=sessionmgr01-site1:27718
MEMBER2=sessionmgr02-site1:27718
DATA_PATH=/data/sessions.3
[SESSION-SET1-END]
```

This needs to be created using `build_set` script for VMware. For more information, refer to *CPS Installation Guide for VMware*.

For OpenStack, user `/api/system/config/replica-sets`. For more information, refer to *CPS Installation Guide for OpenStack*.

**Step 2**
Verify CPS application is running on both the sites (pcrfclient01 and pcrfclient02) and without any application errors.

**Example:**
By executing `diagnostics.sh` script you can get the diagnostics of application. The `diagnostics.sh` output should not contain any application errors.

**Step 3**
Verify whether shard command is available in OSGi console or not. From pcrfclient01, login as root user into the OSGi console and run the help.
You will find the following shard command:

```
telnet qns01 9091
osgi> help
---QNS Commands---
```
reload - Reload reference data
genpassword <db password>

---Sharing Commands---
addshard seed1[,seed2] port db-index [backup]  
rebalance  
migrate  
---Controlling the Console---
more - More prompt for console output  
disconnect - Disconnects from telnet session  
help <command> - Display help for the specified command.

Step 4  To configure hot standby session management, execute the following commands:
telnet qns01 9091  
addshard sessionmgr03,sessionmgr04 27717 1 backup  
addshard sessionmgr03,sessionmgr04 27717 2 backup  
addshard sessionmgr03,sessionmgr04 27717 3 backup  
addshard sessionmgr03,sessionmgr04 27717 4 backup  
rebalance  
migrate  
disconnect  
y

Step 5  To verify the configuration:

1  Login to primary administration database using port#<admin DB port> and verify the collection shards in shading database.

```
mongo sessionmgr01:27721
MongoDB shell version: 2.6.3
connecting to: sessionmgr01:27721/test
set05:PRIMARY> use sharding
switched to db sharding
set05:PRIMARY> db.shards.find()
{   "_id" : 1,   "seed_1" : "sessionmgr03",   "seed_2" : "sessionmgr04",   "port" : 27717,   "db" : "session_cache_2",   "online" : true,
   "count" : NumberLong(0),   "backup_db" : true }
{   "_id" : 2,   "seed_1" : "sessionmgr03",   "seed_2" : "sessionmgr04",   "port" : 27717,   "db" : "session_cache_3",   "online" : true,
   "count" : NumberLong(0),   "backup_db" : true }
{   "_id" : 3,   "seed_1" : "sessionmgr04",   "seed_2" : "sessionmgr04",   "port" : 27717,   "db" : "session_cache_4",   "online" : true,
   "count" : NumberLong(0),   "backup_db" : true }
{   "_id" : 4,   "seed_1" : "sessionmgr03",   "seed_2" : "sessionmgr04",   "port" : 27717,   "db" : "session_cache",   "online" : true,
   "count" : NumberLong(0),   "backup_db" : true }
set05:PRIMARY
```

Failover Detection

There are three possible ways a MongoDB node can fail and trigger a fail over to another node:
1. **Replica set step down:** This scenario is the cleanest method since it disconnects all client sockets and immediately initiates a new election for a master node.

2. **Process abort:** This scenario occurs when a node aborts due to an internal failure. Since this is unplanned, the other replica nodes will not request a new election for a master node until a majority of the nodes have detected the master as down.

3. **VM power off:** This scenario occurs when a node is powered off without a proper shutdown. In this case sockets are usually hung on all clients and the other replica nodes will not request a new election for a master node until a majority of the nodes have detected the master as down.

The Cisco Policy Server detects client failure by:

1. Utilizing the pre-packaged MongoDB Java driver software to detect failure.
2. Detecting server power off via server pings to rapidly detect power off situations.

**Limitation**

You can configure only one backup database. Thus, in GR Active/Standby configuration, if you configure backup database on the standby site, during local primary to local secondary database fail over on active site, the sessions would be saved on the backup database which is on secondary site. This might increase cross-site traffic temporarily.

**Policy Builder Configuration**

**Step 1**
Configure and publish Policy Builder changes from each site. Use `about.sh` command to find out Policy Builder URL. Cisco recommends to configure and publish Policy Builder data separately from each site. But if the user wants to publish Policy Builder data from single site to all other sites then it is difficult to access Policy Builder data from other sites when the primary site goes down.

To access Policy Builder data from other sites when primary site is down, refer [Access Policy Builder from Standby Site when Primary Site is Down](#) on page 26.

**Step 2**
Set appropriate Primary Database IP address, Secondary Database IP address and Port numbers for the following plug-ins:

- USuM Configuration
- Balance Configuration
- Custom Reference Data Configuration
- Voucher Configuration
- Audit Configuration
Step 3  Set Balance Configuration > Db Read Preference as SecondaryPreferred for all databases except balance database.

*Figure 6: Db Read Preference*

*Db Read Preference*  
SecondaryPreferred  

*Max Replication Wait Time Ms*  
100

An example Cluster configuration is given:

*Figure 7: Policy Builder Screen*

Also update Lookaside Key Prefixes and Admin Database sections. For more information, refer to CPS Mobile Configuration Guide.
Step 4

It is recommended to publish Policy Builder changes from each site. If a user is using primary site to publish Policy Builder changes then publishing into all the following cluster repositories is not recommended:

Table 7: Publishing

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Publish URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-PRI</td>
<td>http://&lt;Management interface public IP address of CA-PRI-perfclient01&gt;/repos/run</td>
</tr>
<tr>
<td>CA-SEC</td>
<td>http://&lt;Management interface public IP address of CA-SEC-perfclient01&gt;/repos/run</td>
</tr>
</tbody>
</table>
Step 5  
Add all the above repositories. Repository and Publish screen looks like:

*Figure 8: Repository Screen*

![Repository Screen](image1)

*Figure 9: Publish Screen*

![Publish Screen](image2)
Step 6 Validate both setups using diagnostics.sh, after publishing the repository (wait for five minutes) OR follow the Validate VM Deployment section in the Cisco Policy Suite Installation Guide for this release.

Access Policy Builder from Standby Site when Primary Site is Down

Step 1 This is recommended only when primary site is down and secondary is only for reading/viewing purpose. It is applicable only where user publishes policy builder data from single site that is, primary site to all other sites.

Step 2 Open Policy Builder from secondary site (use about.sh command to find out PB URL).

Step 3 Create new data repository SEC-RUN-RO using URL 'http://Management interface public IP address of secondary pcrfclient01/repos/run', screen looks like:

Figure 10: New Data Repository

Step 4 Access Policy Builder from secondary site using newly created repository.
qns.conf Configuration Changes for Session Replication

The following changes are required in qns.conf file when session replication is required for active/active or active/standby GR deployments.

For active/active GR deployment, Geo HA feature needs to be enabled. For more information, refer to Active/Active Geo HA - Multi-Session Cache Port Support.

**Step 1** Add the following GR related parameters in /etc/broadhop/qns.conf file of Cluster A Primary cluster manager VM that is, CA-PRI-cm:
- DGeoSiteName=clusterA_PRI
- DSiteId=clusterA_PRI
- DRemoteSiteId=clusterA_SBY
- DheartbeatMonitorThreadSleepMS=500
- Dcom.mongodb.updaterConnectTimeoutMS=1000
- Dcom.mongodb.updaterSocketTimeoutMS=1000
- DdbConnectTimeout=1200
- Dmongo.client.thread.maxWaitTime=1200
- DdbSocketTimeout=600
- DclusterFailureDetectionMS=2000

**Step 2** Add the following GR related parameters in /etc/broadhop/qns.conf file of Cluster A Secondary cluster manager VM that is, CA-SEC-cm:
- DGeoSiteName=clusterA_SBY
- DSiteId=clusterA_SBY
- DRemoteSiteId=clusterA_PRI
- DheartbeatMonitorThreadSleepMS=500
- Dcom.mongodb.updaterConnectTimeoutMS=1000
- Dcom.mongodb.updaterSocketTimeoutMS=1000
- DdbConnectTimeout=1200
- Dmongo.client.thread.maxWaitTime=1200
- DdbSocketTimeout=600
- DclusterFailureDetectionMS=2000

**Step 3** For multi-cluster, the following setting should be present only for GR (multi-cluster) CPS deployments:
- DclusterFailureDetectionMS=1000

**Note** In an HA or GR deployment with local chassis redundancy, the following setting should be set to true. By default, this is set to false.
- Dremote.locking.off

**Step 4** Create etc directory on each cluster using /var/qps/install/current/scripts/build/build_etc.sh script.

**Step 5** Copy the changes in qns.conf to other VMs:
copytoall.sh /etc/broadhop/qns.conf /etc/broadhop/qns.conf

**Step 6** Restart all software components on the target VMs:
restartall.sh

**Step 7** Validate setup using diagnostics.sh or follow Validate VM Deployment section in the CPS Installation Guide for VMware for this release.
Configurations to Handle Database Failover when Switching Traffic to Standby Site Due to Load Balancer Fail/Down

Note To understand traffic switch over, refer to Load Balancer VIP Outage.

Step 1 Add the list of databases that needs to be migrated to primary on other site after traffic switch over in mon_db_for_lb_failover.conf file (/etc/broadhop/mon_db_for_lb_failover.conf) in Cluster Manager.

Note Contact your Cisco Technical Representative for more details.

Add the following content in the configuration file (mon_db_for_lb_failover.conf):

The following is an example and needs to be changed based on your requirement.

#this file contains set names that are available in mongoConfig.cfg. Add set names one below other.
#Refer to README in the scripts folder.
SESSION-SET1
SESSION-SET2
BALANCE-SET1
SPR-SET1

Step 2 Rebuild etc directory on cluster by executing the following command:

/var/qps/install/current/scripts/build/build_etc.sh