CA CloudMinder™

Disaster Recovery Guide

1.52

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA CloudMinder™ Advanced Authentication
- CA CloudMinder™ Single Sign-On
- CA Directory
- CA IdentityMinder™
- CA AuthMinder™
- CA RiskMinder™
- CA SiteMinder®
- CA SiteMinder® for Secure Proxy Server
- CA Layer 7

Contents

Chapter 5: DR Site Operations 39

Chapter 1: Disaster Recovery

This section contains the following topics:

Protection from Disaster

In the event of a disaster, users can lose access to services that are critical to their jobs. As a result, these users cannot provide services to other users. The ability to restore access to services depends on the remote installation of CA CloudMinder at a site that is called the Disaster Recovery (DR) site.

The primary site and DR site run in a hot/warm configuration.

- All customer traffic goes to the primary site until a failure occurs. At that point, traffic is manually switched to the DR site.
- The DR site is a clone of the primary site with certain exceptions as described below. The DR site may or may not be internally redundant. This choice is made based on availability and cost considerations.

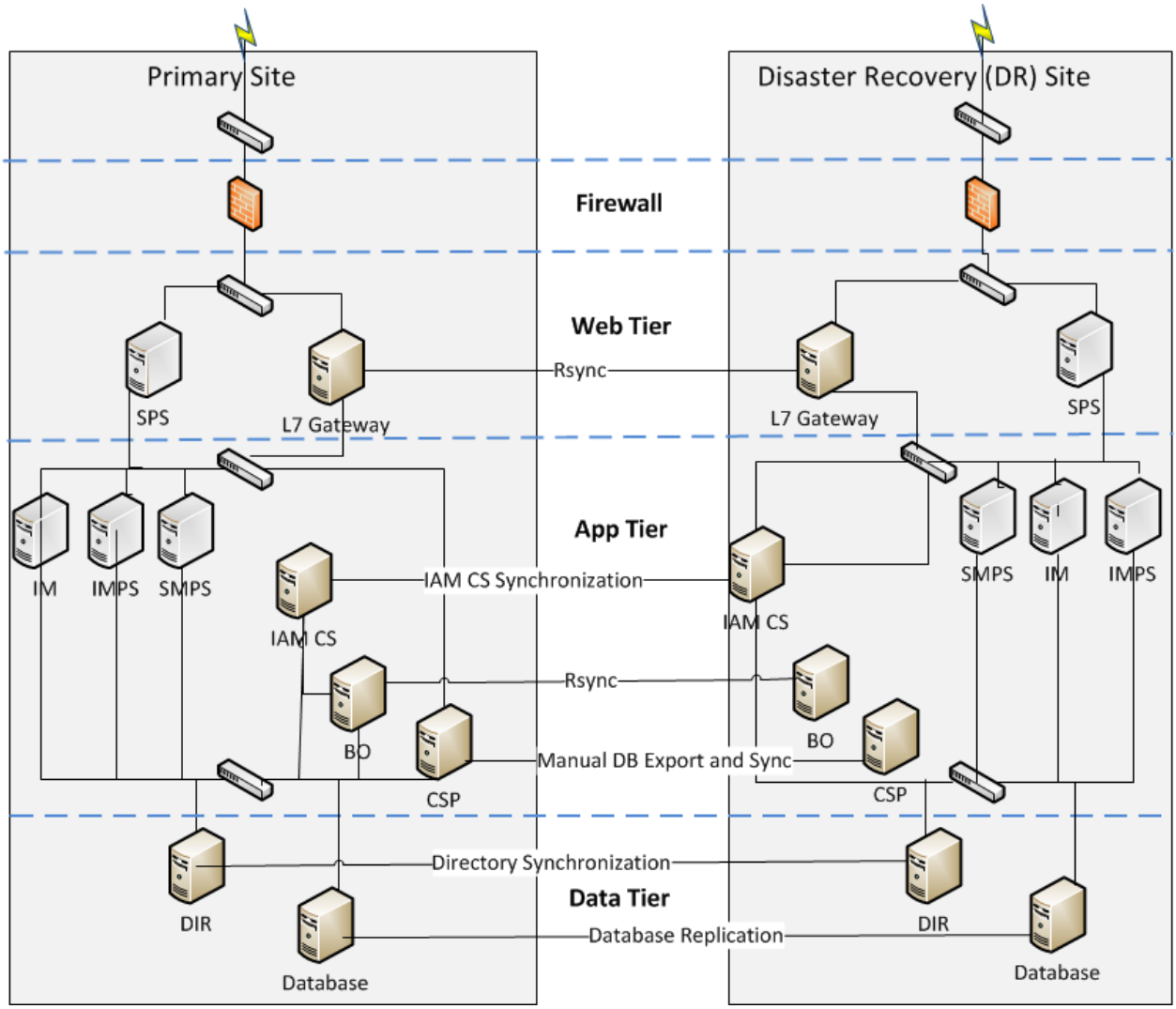
Server activity at the DR site varies by tier.

- In the data tier, CA Directory and the database are active to support data replication from the primary site.
- In the web tier and application tier, all functions are dormant except for CA IAM CS. This dormant mode is necessary for applications that access the database (for reasons explained below). Although the web tier does not directly access the database, it cannot function without the application tier.

Disaster Recovery Architecture

The following diagram illustrates the disaster recovery architecture. For ease of reading, the diagram omits redundant components at the primary site, however, redundancy is part of the primary site. This diagram uses the following terminology:

- IM -- Identity Management server
- IMPS -- Provisioning Server
- SMPS -- SiteMinder Policy Server
- BO -- Business Objects Report Server
- DIR -- Directory Server
- SPS -- Secure Proxy Server



Database Replication

For Oracle, CA CloudMinder recommends Data Guard, Oracle's standby database solution, to support disaster recovery. For PostgreSQL, CA CloudMinder recommends Streaming Replication, PostgreSQL's standby database solution to support disaster recovery.

With this approach, the primary site owns the master database and the DR site owns the standby database. Data is replicated from master to standby until a failure occurs. At that time, the standby database is promoted to a master database for use by the DR site.

During normal operation, the standby database can only be written using the replication stream. It cannot be directly written by the applications at the DR site. For this reason, certain operations at the DR site, such as software installation, require that the application being installed connect to the master database at the primary site. For PostgreSQL, CA CloudMinder recommends Streaming Replication, PostgreSQL's standby database solution to support disaster recovery.

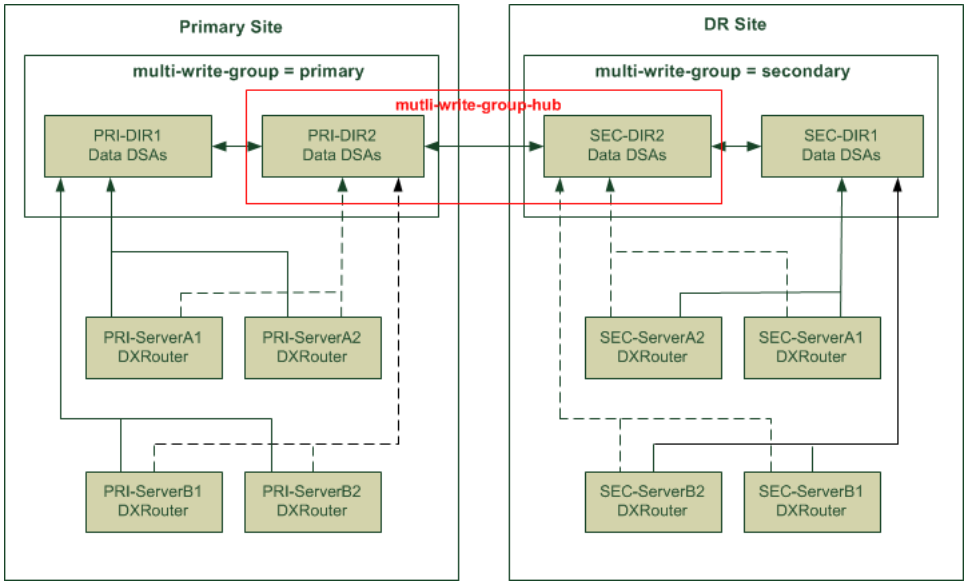
CA Directory Replication

Configuration for Tenant Deployment

CA Directory is configured to use distinct multi-write groups at each site, with bi-directional asynchronous replication between sites. The CA Directory configuration is generated by CA CloudMinder at both the primary site and DR site during tenant deployment, which is covered in a subsection of this chapter.

Two data DSAs are deployed for each tenant, a User DSA and a Provisioning DSA. For each of these two logical data DSAs, two instances are deployed at the primary site and one or two instances at the DR site. One data DSA at each site is the master data DSA that is targeted for write operations from the DXrouters. The other non-master DSA is responsible for asynchronous replication to the other site.

The following diagram shows a typical dual-site deployment from the perspective of CA Directory configuration. For each site, the directory servers appear at the top of diagram. The other server systems, which deploy Dxrouters, appear below the directory servers. A multi-write-group is defined at the directory servers and each DXrouter indicates a write-precedence for the DIR1 directory server (where the master DSAs reside). Replication between sites is enabled by defining the multi-write-group-hub on the DIR2 directory servers at each site.



Response to DSA Failure

In the event of a master DSA failure, the DXrouters switch traffic to the non-master DSA automatically. This allows the primary site to continue operation without interruption. In the event of a non-master DSA failure, data replication from the primary site to the secondary site will stop. This does not impact primary site operation. However, if the non-master DSA cannot be restored within a reasonable time period, consider reconfiguring the master DSA as the multi-write-group hub. You remove the CA Directory server hosting the non-master DSAs from the hosting container configuration. You can restore this server later when the failure is resolved.

Host Name Requirements

Host names that are associated with the load balancer VIPs must be identical between the two sites. This requirement exists because these host names appear in the application-level configuration that is shared between sites. Other host names, such as those associated with the various server systems, can differ between sites. However, if the DR site is not redundant (which means it does not use load balancers), the server system host names at the DR site must match the corresponding VIP names at the primary site.

Due to the reuse of certain host names, the system cannot rely entirely on DNS name resolution. The system maintains the mapping of host name to IP addresses in a local hosts file on each system that uses these host names. Additional host name requirements exist if the CSP console system and the Identity Management server are on the same system. The Disaster Recovery Installation (see page 13) section describes these requirements.

Port Assignments

To allow communication between the primary and DR sites, we recommend that specific ports be used. These port assignments are not required in all situations. For example, port assignments are not required if a firewall is not installed or a VPN is set up between two sites where communication between all Primary and DR site servers are allowed.

Data Tier

Server	Must Communicate with other site	Server at other site	Ports
Oracle	Yes	Oracle	1521
Directory	Yes	Directory	9080, 20394, 20396, 20398, 50000 - 50050, 20900 – 20950

Application Tier

Server	Must Communicate with other site	Server at other site	Ports
Provisioning Server	No	Not applicable	Not applicable
CA IAM Connector Server	Yes	CA IAM Connector Server	9080, 22001, 22002
Policy Server	No	Not applicable	Not applicable
CSP Console	Yes	CA Directory	9080
CSP Console	Yes	CA IAM Connector Server	9080, 22001, 22002, 443
CSP Console	Yes	Provisioning Server	20391
CSP Console	Yes	Policy Server	9080
CSP Console	Yes	Secure Proxy Server	443

Server	Must Communicate with other site	Server at other site	Ports
CSP Console	Yes	Identity Management server	9080, 8080
Identity Management server	Yes	CA Directory	9080, 22001, 22002, 443
Identity Management server	Yes	CA IAM Connector Server	20391
Identity Management server	Yes	Provisioning Server	9080
Identity Management server	Yes	Policy Server	443
Identity Management server	Yes	Secure Proxy Server	9080, 8080
Identity Management server	Yes	Identity Management server	9080, 22001, 22002, 443
BO Report Server	Yes	BO Report Server	873 (Rsync)

Web Tier

Server	Must Communicate with other site	Server at other site	Ports
Secure Proxy Server	No	Not applicable	Not applicable
Layer 7	Yes	Layer 7	873 (Rsync)

Chapter 2: Updates at the Primary Site

This section contains the following topics:

Policy Server (Primary)

Update the host file to use an alias for the CSP Directory DSA hostname.

Follow these steps:

1. Create an alias name called cspdiralias for the Directory Host.
2. Map this alias to the IP of Primary site Directory Server 1 where the CSP console DSA is hosted.

CSP Console (Primary)

Follow these steps:

1. Update the host file to use an alias for the CSP Directory DSA hostname.
   a. Create an alias name called cspdiralias for the Directory Host.
   b. Map this alias to the IP of Primary site Directory Server 1 where the CSP console DSA is hosted.
2. Locate the CA CloudMinder 1.51 properties.sh file that was backed up before the upgrade.

   Restore that file into the /tmp folder.
3. Navigate to the following location:

   `/opt/CA/saas/repo/application/`
4. Run the command as shown in the following format:

   `./UpdateCSPDir.sh -csp_dir_host` *`IP Address of CSP console DIR Host System`*

   For example: ./UpdateCSPDir.sh -csp_dir_host 10.252.1.102

Optionally, you can include the CSP console DIR Port and CSP console DIR alias name. For example:

`./UpdateCSPDir.sh -csp_dir_host` *`IP Address of CSP console DIR Host System`* `-csp_dir_port` *`CSP console DIR Port Number`* `-csp_dir_alias` *`CSP console DIR Host Alias`*

For example: ./UpdateCSPDir.sh -csp_dir_host 10.252.1.102 -csp_dir_port 50000 -csp_dir_alias cspdiralias

If you omit these parameters, the default port is 50000 and the default alias is cspdiralias.

5. Restart the SiteMinder Admin UI service by using these commands:

   ```
   service S98smAdminUI stop
   ```

   Wait 30 seconds, then issue the second command.

   ```
   service S98smAdminUI start
   ```

Identity Management Server (Primary)

Follow these steps:

1. Update the host file with aliases for the CSP Directory DSA hostname and the CSP Console server.
   a. Create an alias called cspdiralias for the Directory Host.
   b. Map this alias to the IP of Primary site Directory Server 1 where the CSP console DSA is hosted.
   c. Create an alias called csphostalias for the Primary CSP console server.
   d. Map this alias to the IP address of Primary site CSP console server, where the SiteMinder Admin UI is installed.
2. Update the Identity Management server to use the alias name for the CSP Directory DSA host.

   In the Identity Management management console, export the directory XML for the CSP Directory.

   a. Edit the exported XML file and locate the following line in that file:
      `<Connection host="<hostname of CSP DSA host> port="50000" />`
   b. Change the line to appear as follows:
      `<Connection host="cspdiralias" port="50000" />`
   c. Save the file.
3. Update the CSP Directory by importing the updated XML file through Identity Management Management Console.

4. Locate the properties.sh file that was backed up before the upgrade.

   Restore that file into the /tmp folder.

5. Run the changeCSPHostname script as follows:

   ```
   cd /opt/CA/saBas/repo/application/
   ./changeCSPHostname.sh
   ```

6. Restart the JBoss service on both Identity Management servers one at a time.

   ```
   service im stop
   service im start
   ```

Repeat steps 1 through 5 on each system that hosts an Identity Management server at the primary site.

Layer 7 Gateway (Primary)

Follow these steps:

1. Make sure that you have a my.cnf file in the /etc/ directory.
2. Add your mysql root password at the end of the file. The format is:

   ```
   [client]
   # The following password will be sent to all standard MySQL clients
   password=my_password
   ```

Repeat these steps on each Layer 7 server at the primary site.

Chapter 3: Installation at the DR Site

This section contains the following topics:

Installation Order

You install system components in a specific order, beginning with the data tier. You then move upward through the architecture, installing the application servers and components and finally the web and interface components, as follows:

- Oracle or PostgreSQL database, for Identity Management runtime data
- Oracle or PostgreSQL database, for reporting data
- CA Directory server
- CA SiteMinder® Policy server
- CSP console
- Secure Proxy server
- Identity Management server
- Business Objects server, if you plan to install CA Business Intelligence to enable reporting for your environment.
- Layer 7 Gateway

Install each component and confirm that it is running before you install the next component. Most of these components are not running after installation. For example, Identity Management server is prevented from running after installation.

You install all instances of each component before moving on to install the next component. For example, for a two-instance high-availability deployment, first install two instances of CA Directory server, then install two instances of the Provisioning server.

Database (DR)

The DR site requires the same installation of Oracle or PostgreSQL that you installed at the primary site.

- If you installed Oracle at the primary site, you install Oracle at the DR site. You use Oracle Data Guard to configure replication between sites. For information on Data Guard setup, refer to the Oracle documentation at http://www.oracle-base.com/articles/11g/data-guard-setup-11gr2.php.
- If you installed PostgreSQL at the primary site, you install PostgreSQL at the DR site. Use Streaming Replication to configure replication between sites. For information, refer to these locations:
  - http://wiki.postgresql.org/wiki/Streaming_Replication
  - http://www.rassoc.com/gregr/weblog/2013/02/16/zero-to-postgresql-streaming-replication-in-10-mins/

Directory Server (DR)

Install the CA Directory Server using the same procedure that you performed at the primary site. Perform that procedure on each system to be used for a CA Directory Server at the DR site.

Note: The CA Directory configuration is generated by CA CloudMinder at the primary site during tenant deployment.

Policy Server (DR)

You install the Policy Server at the DR site in the same way you installed it at the primary site with some minor changes.

Prerequisite Steps

1. Update the host file on the system with the Policy Server to use an alias for the CSP DSA hostname.

   Map an alias, cspdiralias, to the IP Address of the CA Directory with the CSP DSA at the DR site.

2. Edit the properties file to set the database properties to match the Primary database properties. Match the entries for server hostname, usernames, passwords, tablespaces names and tablespace filenames and pathnames.

3. Configure VIPs for this server at the DR site based on whether or not load balancing is used. The table uses the following codes:

   - Policy Server hostnamesIM = Identity Management
   - SPS = Secure Proxy Server
   - SMPS = SiteMinder Policy Server

Property	Primary Site Value	DR Site Value (load balancing)	DR Site Value (no load balancing)
_aa_tws_base_url	http://<SMPS-LB-VIP>:9090/tenant-services/cm/tenantws	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts
_aa_im_base_url	http://<IM-LB-VIP>:8080/iam/im/	same as primary	Same as Primary with <IP of DR IM> mapped to <IM-LB-VIP> in /etc/hosts
_aa_tomcat_host_address	<SMPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts
_shim_aaui_host_port	<SPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_shim_sm_webagent_host_port	<SPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_tws_im_ws_host	<IM-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts

Perform the Installation

Install the Policy Server using the same *CA CloudMinder Installation Guide* procedure that you performed at the primary site. Repeat this procedure on each system that should become a Policy Server.

CSP Console (DR)

Prerequisite Steps

1. Update the host file on the system with the CSP console to use an alias called cspdiralias for the CSP DSA hostname.
2. Use ssh\putty to log in to the CSP console system at the primary site:
3. From the primary site CSP console host, create the CSP DSA CA Directory Server for the DR site by executing these commands:

   ```
   cd /opt/CA/saas/repo/application/
   ./deployCSPDSA.sh -csp_dir_host DR CSP Directory Host
   -csp_dir_password CSP dir password -csp_dir_webservices_password
   DSA Web Services password
   ```

4. Set the following properties for the CSP console installation:

   ```
   _csp_deploy_dsa=false; export _csp_deploy_dsa
   _csp_dir_host=cspdiralias; export _csp_dir_host
   ```

5. Before installation, edit the properties file to set the database properties to match the Primary database properties. Match the entries for server hostname, usernames, passwords, tablespaces names and tablespace filenames and pathnames.
6. Configure VIPs for this server at the DR site based on whether or not load balancing is used. The table uses the following codes:
   - IM = Identity Management
   - SPS = Secure Proxy Server
   - SMPS = SiteMinder Policy Server

Property	Primary Site Value	DR Site Value (load balancing)	DR Site Value (no load balancing)
_aa_tws_base_url	http://<SMPS-LB-VIP>:9090/tenant-services/cm/tenantws	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts

Property	Primary Site Value	DR Site Value (load balancing)	DR Site Value (no load balancing)
_aa_im_base_url	http://<IM-LB-VIP>:8080/iam/im/	same as primary	Same as Primary with <IP of DR IM> mapped to <IM-LB-VIP> in /etc/hosts
_aa_tomcat_host_address	<SMPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts
_shim_aaui_host_port	<SPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_shim_sm_webagent_host_port	<SPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_tws_im_ws_host	<IM-LB-VIP>	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_csp_dir_host	<Primary Dir1> (Change to alias name cspdiralias for next upgrade)	cspdiralias with <IP of DR DIR> mapped to cspdiralias in /etc/hosts	cspdiralias with <IP of DR DIR> mapped to cspdiralias in /etc/hosts

Perform the installation

Install the CSP console using the same *CA CloudMinder Installation Guide* procedure that you performed at the primary site.

Secure Proxy Server (DR)

Installation of Secure Proxy Server registers this server with the Policy Servers, which creates a unique shared secret on the Secure Proxy Server system. The shared secret is paired with a trusted host name, which is independent of the standard host name. On each Secure Proxy Server instance, a unique shared secret and trusted host name exist; they are not shared between the primary and DR sites.

Prerequisite Step

Configure VIPs for this server at the DR site based on whether or not load balancing is used. The table uses the following codes:

- IM = Identity Management
- SPS = Secure Proxy Server
- SMPS = SiteMinder Policy Server
- IAMCS = CA IAM Connector Server

Property	Primary Site Value	DR Site Value (load balancing)	DR Site Value (no load balancing)
_policy_server_hostname	<SMPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts
_im_hostname	<IM-LB-VIP>	same as primary	Same as Primary with <IP of DR IM> mapped to <IM-LB-VIP> in /etc/hosts
_jcs_hostname	<IAMCS-LB-VIP>	same as primary	Same as Primary with <IP of DR JCS> mapped to <JCS-LB-VIP> in /etc/hosts

Perform the Installation

Install the Secure Proxy Server using the same *CA CloudMinder Installation Guide* procedure that you performed at the primary site. Repeat this step on each Secure Proxy Server at the DR site.

Identity Management Server (DR)

Perform these steps on a system that you choose for the Identity Management server at the DR site.

Prerequisite Steps

1. Edit the properties file to set the database properties to match the Primary database properties. This includes server hostname, usernames, passwords, tablespaces names, and tablespace file names, and path names.
2. Add a host entry to map cspdiralias to the DR directory host with the CSP console DSA.

3. Add a host entry to map csphostalias to CSP console Host IP at the DR site.
4. Update properties.sh file used for the installation with the following values.

   _CSPDirHost=cspdiralias;

   _cspHostName=csphostalias;
5. Configure VIPs for this server at the DR site based on whether or not load balancing is used. The table uses the following codes:
   - IM = Identity Management
   - SPS = Secure Proxy Server
   - SMPS = SiteMinder Policy Server

Property	Primary Site Value	DR Site Value (load balancing)	DR Site Value (no load balancing)
_sm_host	<SMPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts
_CSPDirHost	<Primary Dir1> (Change to alias name cspdiralias for next upgrade)	cspdiralias with <IP of DR DIR> mapped to cspdiralias in /etc/hosts	cspdiralias with <IP of DR DIR> mapped to cspdiralias in /etc/hosts
_cspHostName	<Primary CSP> (change to alias name csphostalias for next upgrade)	csphostalias with <IP of DR CSP> mapped to csphostalias in /etc/hosts	csphostalias with <IP of DR CSP> mapped to csphostalias in /etc/hosts
_envBaseURL	http://<SPS-LB-VIP>/iam/im	same as primary	Same as Primary with <IP of DR SPS> mapped to <SPS-LB-VIP> in /etc/hosts
_internalBaseURL	http://<IM-LB-VIP>:8080/iam/im/	same as primary	Same as Primary with <IP of DR IM> mapped to <IM-LB-VIP> in /etc/hosts
_authMinderHost	<SMPS-LB-VIP>	same as primary	Same as Primary with <IP of DR SMPS> mapped to <SMPS-LB-VIP> in /etc/hosts

Perform the Installation

Install the Identity Management Server using the same *CA CloudMinder Installation Guide* procedure that you performed at the primary site; however, apply the following guidelines:

- Make the_multicast_address and _multicast_groupname different from the primary site to avoid clustering between the primary and DR sites.
- Each Identity Management server in the JBoss cluster has a unique ServerPeerId used by JMS. Use the same server peer IDs on the corresponding servers between sites. The server peer IDs are assigned at installation time and, by default, start at 1. Use of the default settings at both sites is sufficient to achieve the desired correspondence.

Repeat this procedure on each system that should become an Identity Management server.

Business Objects Report Server (DR)

Business Object servers are members of a cluster that share data by two means: the Oracle database and a shared file system.

The shared file system holds the Input File Repository which stores report templates and the Output File Repository which stores generated reports. To achieve high availability, implement the shared file system with no single point of failure. We recommend using the shared file system on a RAID disk system that is accessible to all Business Object servers. For example, you can use a storage area network (SAN) server.

Layer 7 Gateway (DR)

CA Directory and the Oracle Database are already replicated between the primary and DR sites. Layer 7 provides a script called ssg_export_full.sh to migrate the MySQL database between the primary site and the DR site.

Follow these steps:

1. Install the base Layer 7 Gateway using the same *CA CloudMinder Installation Guide* procedure that you performed at the primary site with the following changes:
   - Exclude the Create OTK/OIDC Database step up
   - Stop at the step preceding the step to install license and policies.

2. On the primary system, export the configured OAuth, SiteMinder, and OpenID Connect services and Policies using the following procedure.
3. SSH to Primary Gateway server 1.
4. Make sure ssg_export_full.sh under the /opt/SecureSpan/DR folder is executable. Use this command:
   `chmod 755 ./ssg_export_full.sh`
5. Make sure that you have a my.cnf file in the /etc/ directory.

   Add your mysql root password at the end of the file. The format is:

   ```
   [client]
   # The following password will be sent to all standard MySQL clients
   password=my_password
   ```
6. At the primary site on Layer 7 server 1, execute the following command:

   `./ssg_export__full.sh`
7. Use sftp to copy the output file (ssg_export_orig_*timestamp*.sql) to the DR site Gateway server under the /opt/SecureSpan/DR directory.
8. Stop the DR site Gateway process using this command: service ssg stop
9. At the DR site Gateway, enter the following command:

   `mysql -u root -h hostname ssg < ssg_export_orig_timestamp.sql`

   For *hostname*, enter the hostname you used when you installed MySQL.
10. Start the DR site Gateway process by entering the following command:

    `service ssg start`
11. Shut down the Gateway. Issue this command:

    `service ssg stop`

Chapter 4: Configuration of Disaster Recovery

This section contains the following topics:

DR Site in Standby State

Use the following procedures to put the DR site in standby.

Identity Management Server

1. Navigate to the following location:

   ```
   /opt/CA/saas/repo/application
   ```

2. Run the following command:

   ```
   ./DR_mode mode=standby
   ```

3. Edit the properties file to set the Identity Management Server to the DR database.

4. Edit the following files to point system to the DR database.

   ```
   jbosshome/server/all/deploy/iam_im_imtaskpersistencedb-ds.xml
   jbosshome/server/all/deploy/iam_im_reportsnapshot-ds.xml
   jbosshome/server/all/deploy/iam_im_objectstore-ds.xml
   jbosshome/server/all/deploy/iam_im_imarchivedb-ds.xml
   jbosshome/server/all/deploy/iam_im_imauditdb-ds.xml
   jbosshome/server/all/deploy/iam_im_imworkflowdb-ds.xml
   jbosshome/server/all/deploy/iam_im_webfort-ds.xml
   ```

SiteMinder Policy Server

1. Navigate to the following location:

   `/opt/CA/saas/repo/application/`

2. Run the following command:

   `./DR_mode mode=standby`

3. Edit the following files to point to the DR database:
   - /opt/CA/AdvancedAuth/conf/arcotcommon.ini
   - /opt/CA/AdvancedAuth/Tomcat/conf/context.xml
   - /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/META-INF/context.xml
   - /opt/CA/AdvancedAuth/odbc32v70wf/odbc.ini
   - /opt/CA/siteminder/db/system_odbc.ini

CSP Console

1. Navigate to the following location:

   `/opt/CA/saas/repo/application/`

2. Run the following command:

   `./DR_mode mode=standby`

3. Edit following file to point to the DR database.

   `/opt/CA/siteminder/db/system_odbc.ini`

Secure Proxy Server

1. Navigate to the following location:

   `/opt/CA/saas/repo/application/`

2. Run the following command:

   `./DR_mode mode=standby`

Primary Site in Live State

Follow these steps:

1. Log in to the CSP console system at the primary site.
2. Navigate to the following location:

   `/opt/CA/saas/repo/application/`

3. Run the following command:

   ```
   ./DR_mode mode=live
   ```

4. Repeat these steps on the following systems:
   - Identity Management server
   - Policy Server
   - Secure Proxy Server
   - Provisioning Server
   - IAM Connector Server
   - Directory server

High Availability Configuration

1. Log in to the CA Directory 1 system at the primary site.
2. Go to this location:

   ```
   /opt/CA/IdentityManager/ProvisioningDirectory/highavailability
   ```

3. Run following script ./highavailability
   a. Select yes for DR Express setup.
   b. Select yes for Primary site.
   c. Enter the Primary directory hostnames with comma separation. For example:

      ```
      P_DIR1hostname,P_DIR2hostname,….P_DIRnHostname
      ```

   d. Enter DR directory hostnames with comma separation. For example:

      ```
      DR_DIR1hostname,DR_DIR2hostname,… DR_DIRnHostname
      ```

4. Repeat steps 1 to 3 on all other CA Directory systems at the primary site.
5. Log in to the directory 1 system at the DR site.
6. Go to /opt/CA/IdentityManager/ProvisioningDirectory/highavailability/
7. Run following script ./highavailability
   a. Select yes for DR Express setup.
   b. Select no for Primary site.
   c. Enter DR directory hostnames with comma separation. For example:

      ```
      DR_DIR1hostname,DR_DIR2hostname,… DR_DIRnHostname
      ```

   d. Enter the Primary directory hostnames with comma separation. For example:

      ```
      P_DIR1hostname,P_DIR2hostname,….P_DIRnHostname
      ```

8. Repeat steps 5 to 7 on all other CA Directory systems at the DR site.

Configuration in the CSP console

Use this procedure to modify the container where you are adding disaster recovery servers.

On hosting container pages, the IMPS Tenant Service Host and Disaster Recovery Tenant Service Host fields allow multiple entries. These are for entering the CA IAM CS server hosts if the CA IAM CS and provisioning server are on different systems. Setting site IDs for the DR site requires that the Provisioning Directory replication already exists. The topic High Availability Configuration (see page 29) addresses this prerequisite.

Follow these steps:

1. Using a web browser, log in to the primary site CSP console.
2. Update the Disaster Recover Directory Server Hostname list by adding the CA Directory system name.
3. Add the DR instances of the Identity Management server, Provisioning Server, Policy Server, CA IAM CS to the Disaster Recovery Router Server hostnames.
4. Add the DR Provisioning Server hostname to the Disaster Recovery Provisioning Server Hostnames.
5. Add the DR CA IAM CS hostname to the Disaster Recovery Tenant Service Host.
6. Click submit.

   A status column shows which steps are being executed on the server. You can click search again to update the status with the latest step being executed. The status column is updated with error messages. Errors relate to connection problems or disk space on Provisioning Directory systems.

The CSP console log file typically has more information on errors. The log file can be found at this location:

```
/opt/CA/siteminder/adminui/server/default/log/server.log
```

Report Server Replication

Support for Business Object Reporting requires synchronization between the input and output directory between the Primary and Disaster Recovery site. You use rsync and a cron job for this synchronization.

Follow these steps:

1. Open the TCP port 873.
2. On all Business Objects Report Servers on both sites, create a public key.

   This key is used with the remote server so that the cron job is not prompted for a password entry. Run the following command:

   ```
   # ssh-keygen -t rsa
   ```

   Press enter three times to create a default pub key.
3. Copy the generated public key from the primary site to the DR site using the following command, replacing [username] and [remote_host] with the proper values:

   ```
   # ssh-copy-id -i ~/.ssh/id_rsa.pub [username]@[remote_host]
   ```

   Enter a password when prompted.

   Repeat step 3 by copying the DR site public key to the primary site.
4. Create a file called mirrorfrsinputunder /etc/init.d/ and add the following content:

```
#!/bin/bash

#set -x #echo on

##
## Shell Daemon For: Mirroring frsinput directory
##
##
PIDFILE="/var/run/mirrorfrsinput.pid"
LOGFILE="/var/log/mirrorfrsinput.log"

mirror ()
{
         pgrep -f "$0 $1" > $PIDFILE

        while inotifywait -r -q -e close_write -e delete -e modify
-e close_nowrite -e access -e attrib -e create -e move -e moved_from
-e moved_to -e close --format "%f"
/opt/CA/SharedComponents/CommonReporting3/bobje/data/frsinput/;
do

         rsync -aWuq --no-motd --inplace --del --ignore-errors
--force
/opt/CA/SharedComponents/CommonReporting3/bobje/data/frsinput/
<BO User>@<Other Site BO Server or NFS Share
machine>:/opt/CA/SharedComponents/CommonReporting3/bobje/data/f
rsinput/
```

```
        ret=$?

        done
}

start ()
{
        /usr/bin/nohup `mirror` > $LOGFILE &

        ret=$?
}

case "$1" in
        stop)
                /bin/kill $(cat $PIDFILE)
                ;;
        start)
                start
                ;;
        *)
                echo "$0 [ start | stop ]"
                exit 0
                ;;
esac

exit $?
```

5. Update the permission for the above script to be executable as follows:

   ```
   chmod 775 mirrorfrsinput
   ```

6. Repeat steps 4 and 5 on all Business Objects Report Servers or NFS share systems on both sites.

7. Create a file called mirrorfrsoutput under /etc/init.d/ and add the following content:

   ```
   #!/bin/bash

   #set -x #echo on

   ##
   ## Shell Daemon For: Mirroring frsinput directory
   ## (poorly coded, quick and dirty, example)
   ##
   PIDFILE="/var/run/mirrorfrsoutput.pid"
   LOGFILE="/var/log/mirrorfrsoutput.log"
   ```

```
mirror ()
{
         pgrep -f "$0 $1" > $PIDFILE

         while inotifywait -r -q -e close_write -e delete -e modify
-e close_nowrite -e access -e attrib -e create -e move -e moved_from
-e moved_to -e close --format "%f"
/opt/CA/SharedComponents/CommonReporting3/bobje/data/frsoutput/
; do

                  rsync -aWuq --no-motd --inplace --del
--ignore-errors --force
/opt/CA/SharedComponents/CommonReporting3/bobje/data/frsoutput/
<BO User>@<Other Site BO Server or NFS Share
machine>:/opt/CA/SharedComponents/CommonReporting3/bobje/data/f
rsoutput/

        ret=$?

        done
}

start ()
{
        /usr/bin/nohup `mirror` >> $LOGFILE 2>&1 &

        ret=$?
}

case "$1" in
        stop)
                /bin/kill $(cat $PIDFILE)
                ;;
        start)
                start
                ;;
        *)
                echo "$0 [ start | stop ]"
                exit 0
                ;;
esac

exit $?
```

8. Update the permissions for the preceding script to be executable as follows:

   ```
   chmod 775 mirrorfrsoutput
   ```

9. Repeat steps 7 and 8 on all Business Object Report Server or NFS share systems at both sites.

10. Start the synchronization from the primary site to the DR site Business Object Report Server. Execute the following commands on any Business Object Report Server or common NFS share system.

    ```
    /etc/init.d/mirrorfrsinput start
    /etc/init.d/mirrorfrsoutput start
    ```

    Note: The scripts should only be started in one of the Business Object Report Servers at the active site. Ensure that these scripts are stopped on all other Business Object Report Servers at all sites.

11. Create a monitor process to monitor the above two processes.

    In case of failover, the same set of commands need to be run from DR site to synchronize it back to the primary site.

12. To stop the processes run the following commands.

    ```
    /etc/init.d/mirrorfrsinput stop
    /etc/init.d/mirrorfrsoutput stop
    ```

    Note: Stopping these processes will stop auto synchronization.

Derby Database Synchronization

The CSP Derby Database requires synchronization between the primary site and the DR site.

Follow these steps:

1. On the primary site system with the CSP console, export the Derby database. Use these commands:

    ```
    cd /opt/CA/saas/repo/application/CSPExport
    ./ derbyExport.sh
    ```

    Note: Running script again removes the output generated by the previous execution.

2. Copy the derby-exported-files.tar to the following directory on the DR site.

    ```
    /opt/CA/saas/repo/application/CSPExport
    ```

3. Make smuser the owner of the TAR file.
4. Make sure SiteMinder Admin UI service is stopped until DR site becomes active.
5. Import the Derby database. Use these commands:

    ```
    cd /opt/CA/saas/repo/application/CSPexport
    ./derbyImport.sh
    ```

At this point, all servers at the DR site, except for CA IAM CS and CA Directory, are stopped and no server restarts automatically following a power up sequence. If necessary, the roles of the primary site and DR site can be reversed. This reversal is useful in cases where the two sites use a passive failback strategy (see page 40).

Create a Softlink for the Redirectjsp

Follow these steps if each tenant that was created before CA CloudMinder 1.51.

1. SSH into the Linux console on the SPS server
2. Navigate to:

   ```
   /opt/CA/secure-proxy/Tomcat/webapps/affwebservices
   ```

3. Create a softlink for the redirectjsp/ folder:

   ```
   ln -s redirectjsp <tenant_tag>
   ```

Google and Facebook OAuth

For systems where Google or Facebook OAuth are configured, perform the following steps.

1. Log in Policy Server at the primary site.
2. Copy all files from /opt/CA/siteminder/config/properties/ to the same location on the DR site system.
3. Copy all files from the primary site Secure Proxy Server system to the same location on the DR site Secure Proxy Server system:
   - /opt/CA/secure-proxy/proxy-engine/examples/siteminderagent/forms
   - /opt/CA/secure-proxy/Tomcat/webapps/affwebservices/redirectjsp

Network Peers for Connector Servers

In a high-availability deployment, CA IAM CS systems are load balanced. The load balanced CA IAM CS systems should be configured as network peers so that they can share configuration and requests. This approach ensures the distribution of configuration updates across sites, but has no impact on the distribution of ordinary requests which remain site-bound.

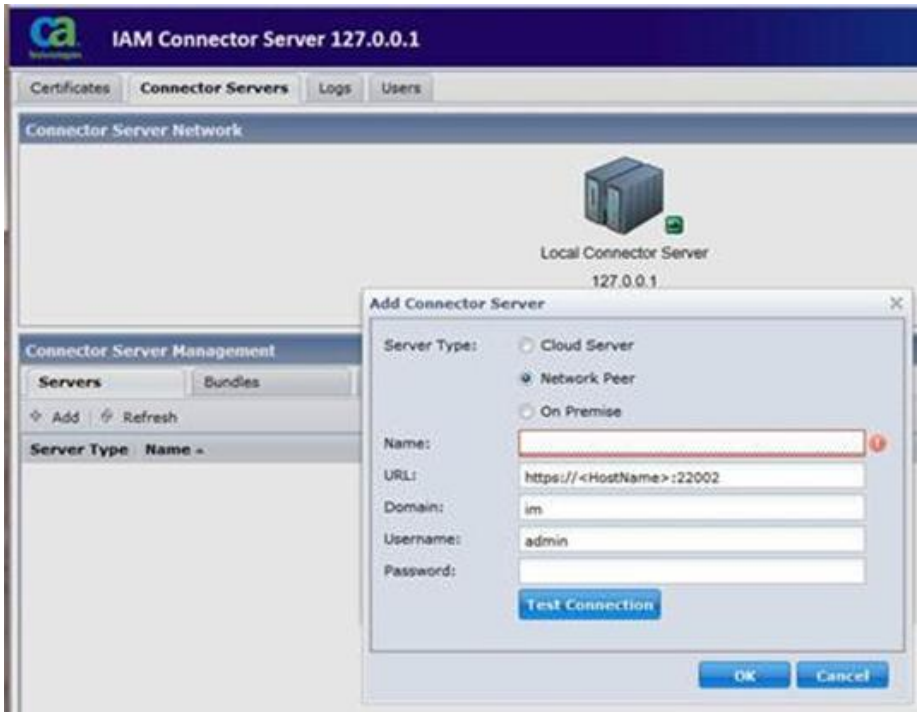
For this procedure, you use the management console of each connector server. Similar network peer configuration needs to be made for CA IAM CS systems at the DR site to share the configuration with primary site.

Follow these steps:

Log in to the CA IAM CS console using the admin account.

1. Select the Servers tab.
2. Select the Add button to add a new server.
3. When the Add Connector Server dialog appears, select the Network Peer radio button.

Equation 1: Connector Server UI



4. Enter the details.

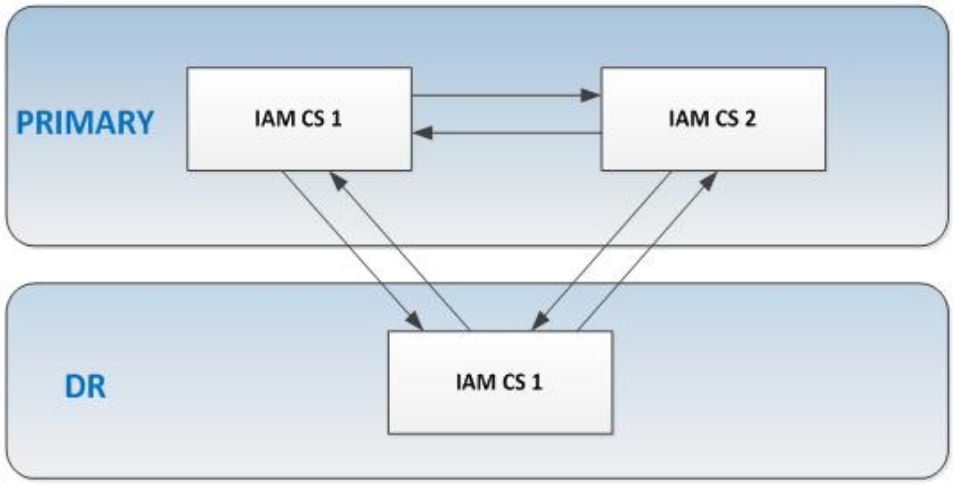
   The domain can usually be left unchanged.

5. Select Test Connection to make sure a connection can be established between the connector servers.
6. Select OK.

Each of the other peers must be added under each CA IAM CS. If a connection cannot be established, check that the clocks on the peers are synchronized.

Configuration needs to be replicated on primary and DR sites as follows:

- A peer configuration for Primary CA IAM CS 1 and CA IAM CS 2 must be added to the CA IAM CS 1 at the DR site
- A peer configuration for Primary CA IAM CS 1 and DR CA IAM CS 1 must be added to Primary CA IAM CS 2 at the Primary site
- A peer configuration for Primary CA IAM CS 2 and DR CA IAM CS 1 must be added to Primary CA IAM CS 1 at the Primary site



Chapter 5: DR Site Operations

This section contains the following topics:

DR Site Testing

After software installation and tenant deployment completes, the DR site can be tested using the following procedure. You also use this procedure for any subsequent test periods that are required.

Follow these steps:

Before testing:

1. Bring down all the servers at the DR site and take a snapshot, but omit the database.
2. Prepare the database:
    a. Stop database replication.
    b. Put the standby Oracle database into standby snapshot mode. This mode sets a marker that enables reverting to this point in time and allows the standby database to be written.
    c. In case of Postgres, start the Standby without recovery mode
3. On the Primary site, disable network connections to the DR site servers by removing the corresponding hosts from the host file on each system. If no host mappings exist, add host mappings for all DR site server hostnames so that they point to random unreachable IPs.
4. Restart all DSAs on the Primary site Directory 2 (designated Hub for replication between sites). This action breaks the replication between the DSAs, which is needed for testing DR site.
5. Start all the servers at the DR site.
6. At the DR site, disable network connections to the DR site servers by removing the corresponding hosts from the host file on each system. If no host mappings exist, add host mappings for all of the Primary site server hostnames so that they point to random unreachable IPs.
7. Restart all DSAs at the DR site Directory (designated Hub for replication between sites). This action breaks the replication between the DSAs, which is needed for testing DR site.

8. Restart all the services on each of DR servers.
9. Run the required tests.

   This step assumes that a DR Test tenant is already created. The hostname that is associated with this tenant maps permanently to the DR site. This situation is different from the normal tenant-associated hostnames that float between the primary site and DR sites as part of the failover and failback procedures.

   Note: If you are creating a tenant at the DR Site, the provisioning server needs to be running.
10. After testing, stop the DR site servers in all tiers except for Oracle.
11. Revert to snapshots.
12. Prepare Oracle:
    a. Revert the database contents to the previously established marker by leaving standby snapshot mode. The database is now a normal standby database.
    b. Resume database replication.
13. Start all the DR servers. Note, all the servers should still be in standby mode.
14. On the Primary site, enable network connections to the DR site servers by adding the corresponding hosts from the host file on each system. If the hostnames are resolved from DNS server, you do not need to add host entries.

Note: To test either site when it is inactive, including prior to a failback, repeat this procedure. After testing is completed and normal operation is restored, sometime is required to re-synchronize the data tier between sites. The time required depends on the rate of data accumulation and the inter-site bandwidth. We recommend a very short test period to minimize recovery time.

DR Site Failover and Failback

Failover to the DR Site

At the time of a primary site failure, the data tier will possess all of the data necessary to allow the DR site to take over operation. The failover procedure is as follows:

1. An outage is detected at the primary site.
2. Incoming customer traffic is stopped from entering the primary site.
3. Operations in progress at the primary site are allowed to complete or time out during a period of at least 3 minutes after incoming traffic has stopped.
4. Database replication between sites, if still operational, is allowed to complete.

5. Database replication between sites is stopped.

   If you are using Oracle, any stale sessions in the primary database will generate an error during failover through Oracle. To resolve this error, issue the following command to kill all open sessions before preparing for failover.

   ```
   ALTER DATABASE COMMIT TO SWITCHOVER TO PHYSICAL STANDBY WITH SESSION SHUTDOWN
   ```

   If you are using Postgres, any stale sessions in the primary database will generate an error during failover. To resolve this error, issue the following command to kill all open sessions before preparing for failover.

   ```
   pg_ctl stop –m fast
   ```

6. On all operational servers at the Primary site, run the following commands to convert them into Standby mode as follows:

   ```
   cd /opt/CA/saas/repo/application
   DR_mode.sh mode=standby
   ```

7. Convert the standby database to a master. Follow the standard Oracle or Postgres failover procedures depending on what database is set up in your environment.

8. Follow the instructions for Derby Database Synchronization (see page 34).

9. On all of the DR site servers, run the following commands to convert them to Live mode:

   ```
   cd /opt/CA/saas/repo/application
   DR_mode.sh mode=live
   ```

   Use the following order for running the script on DR site servers:

   - Directory
   - Provisioning Server
   - CA IAM CS
   - Policy Server
   - CSP console
   - Secure Proxy Server
   - Identity Management server

10. Customer traffic is redirected to the DR site by means of DNS changes, or other methods, that remap the tenant-associated hostnames to the DR site.

11. The DR site is now active.

Configuration after DR site is active

Follow these steps:

1. Update each tenant so that you use Active databases at the DR site.
   a. Log in to User Console as the CSP Administrator.
   b. Update the JDBC connection that is used for reporting to use the DR database instead of the primary database.

      Choose System, JDBC Connection Management, Modify JDBC connection.
   c. Change the database hostname in snapshot database connection to the active database.

      Choose Reports, Snapshot Tasks, Manage Snapshot, Modify Snapshot Database Connection.

   Perform this step for every tenant.
2. Update Layer7 to use the Active database at the DR site
   a. Log in to Layer7 Policy Manager console.
   b. Change the database hostname in each of JDBC connections to use Active Database. Use this path:

      Tasks, Manage JDBC connections

      Select each one and edit it.
3. If the database has failed at primary site, restore it.
   - Convert the master database at the primary site to standby.
   - Begin database replication from DR site to primary site.

Failback to the Primary Site

The failback procedure is the reverse of the failover procedure. Like failover, failback is manually initiated. Your decision to failback depends on the capabilities at the DR site:

- If the DR site has equivalent redundancy and performance to the primary site, you may decide not to failback. Every failback requires another outage. Therefore, the DR site carries the load until it fails.
- If the primary site has capabilities that are superior to the DR site, you can failback as soon as the primary site is repaired and the data tier is resynchronized between sites.

Follow the same procedure as noted in Failover section by converting the DR site to Standby and Primary site to Live. Then perform the following steps:

1. On all DR site servers, run the following commands to convert them to Live mode.

   ```
   cd /opt/CA/saas/repo/application
   DR_mode.sh mode=standby
   ```

2. On all of the Primary site servers, run the following commands to convert them to Live mode.

   ```
   cd /opt/CA/saas/repo/application
   DR_mode.sh mode=live
   ```

   Use the following order for running the script on primary site servers:

   - Directory
   - Provisioning Server
   - CA IAM CS
   - Policy Server
   - CSP console
   - Secure Proxy Server
   - Identity Management server

3. If the database has failed at primary site, restore it.
   - Convert the master database at the primary site to standby.
   - Begin database replication from the DR site to the primary site.

Configuration after the Primary Site is Active

1. Update each tenant so that you use Active database at the primary site.
   a. Log in to User Console as CSP Administrator.
   b. Update the JDBC connection that is used for reporting to use the DR database instead of the primary database.

      Choose System, JDBC Connection Management, Modify JDBC connection.
   c. Change the database hostname in snapshot database connection to the active database.

      Choose Reports, Snapshot Tasks, Manage Snapshot, Modify Snapshot Database Connection.

   Perform this step for every tenant.
2. Update Layer7 to use the Active database at the primary site.
   a. Log in to the Layer7 Policy Manager console.
   b. Change the database hostname in each of JDBC connections to use the Active Database. Use this path:

      Tasks, Manage JDBC connections

      Select each one and edit it.