High Availability Best Practices

XOP Networks: Document number 400-0177-001

Version 1, 2018-08-28

Table of Contents

1. Initial Installation Configuration 2
1.1. Firewall 2
1.2. Database 3
1.3. Network 4
2. Software Update 7
2.1. Update procedure 7
3. Secondary Server Resync 10
3.1. Background 10
3.2. Resync procedure 10
Appendix A: Troubleshooting 13
A.1. Network Connectivity Checks 14
Appendix B: License Configuration 16

1. Initial Installation Configuration

1.1. Firewall

The firewall rules are stored in the file **/etc/sysconfig/iptables**. The Master Service must be configured to allow connections to its database by the Secondary Servers. These connections arrive on port **3306**. To verify that the port is open, issue this command on the Primary Server:

```
grep 3306 /etc/sysconfig/iptables
```

The results should look like

```
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 3306 -j ACCEPT
```

An example of a complete iptables configuration file is:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [8:1424]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m state --state NEW -m udp --dport 5060 -j ACCEPT
COMMIT
*mangle
-A OUTPUT -p udp -m udp --sport 5060 -j DSCP --set-dscp-class cs3
-A OUTPUT -p udp -m udp --dport 5060 -j DSCP --set-dscp-class cs3
-A OUTPUT -p udp -m udp --sport 16384:32767 -j DSCP --set-dscp-class ef
COMMIT
```

1.2. Database

The database configuration is stored in the file **/etc/my.cnf** on each server in the cluster.

1.2.1. Primary Server

The Master server should have a database configuration similar to the following:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

server-id=1
auto_increment_offset    = 1
auto_increment_increment = 2

log-bin = /var/lib/mysql/bin.log
log-bin-index = /var/lib/mysql/log-bin.index

binlog-do-db = xopdb
binlog-ignore-db = xopdb_local
expire_logs_days        = 14
max_binlog_size         = 500M
innodb_flush_log_at_trx_commit = 1
sync_binlog = 1

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

IMPORTANT

If there are more than two members in the cluster, then **auto_increment_increment** must be set to a value equal to the number of servers in the cluster.

The Primary Server must have a database account created to support replication requests from each Secondary Server. To create this user, use the following commands (as the root user):

```
mysql
mysql> CREATE USER ‘repl’@’%’ INDENTIFIED BY ‘slavepass’;
mysql> GRANT REPLICATION SLAVE ON *.* TO ‘repl’@’%’;
mysql>flush privileges;
```

1.2.2. Secondary Server

A Secondary Server server should have a database configuration similar to the following:

```
[mysqld]
bind-address=localhost

datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0


server-id = 2
auto_increment_offset    = 2
auto_increment_increment = 2

replicate-do-db = xopdb
replicate-ignore-db = xopdb_local
replicate-ignore-table = xopdb.ports
replicate-ignore-table = xopdb.system_parms
replicate-ignore-table = xopdb.sessions
replicate-ignore-table = xopdb.session_keys
replicate-ignore-table = xopdb.session_parms
replicate-ignore-table = xopdb.circuit_groups
```

IMPORTANT

If there are more than two members in the cluster, then **auto_increment_increment** must be set to a value equal to the number of servers in the cluster.

1.3. Network

This procedure assumes you have cloned a redundant pair of servers, and need to change the IP addresses. See *Best Practice 463 – OVA Deployment* for information on copying a virtual machine.

IMPORTANT

At the time of change, the network port is disabled, and you will need to issue these commands at the console.

1. **[Primary Server]** Set the new network configuration

   From the Virtual Machine console (not an ssh session), issue these commands:

```
sysconf net <new_master_hostname> <new_nic1_ip> <new_nic1_netmask> <new_nic1_gateway>
sysconf dns <newdns1> [<newdns2>]
sysconf delhost <old_master_ip>
```

If there is a second IP address, also issue these commands:

```
sysconf net2 <new_nic2_ip> <new_nic2_netmask> <new_nic2_gateway>
sysconf delhost <old_secondary_ip>
sysconf addhost <new_secondary_ip> <new_secondary_name>
```

2. **[Primary Server]** Verify the new network configuration

   ```
   reboot
   ```

   Log in to the console again, and check the configuration.

   ```
   ip addr
   ```

3. **[Primary Server]** Enable the network interfaces

   Using the *virtual machine’s* control panel enable the network ports.

4. **[Secondary Server]** Set the new network configuration

   From the Virtual Machine console (not an ssh session), issue these commands:

   ```
   sysconf net <new_secondary_hostname> <new_secondary_ip> <new_netmask> <new_gateway>
   sysconf dns <newdns1> [<newdns2>]
   ```

   If there is a second IP address, also issue these commands:

   ```
   sysconf net2 <new_nic2_ip> <new_nic2_netmask> <new_nic2_gateway>
   sysconf delhost <old_master_ip> <old_secondary_ip>
   sysconf addhost <new_master_ip> <new_master_name>
   ```

5. **[Secondary Server]** Verify the new network configuration

   ```
   reboot
   ```

Log in to the console again, and check the configuration.

```
ip addr
```

6. **[Secondary Server]** Enable the network interfaces

   Using the *virtual machine's* control panel enable the network ports.

7. **[Primary Server]** Set the Secondary Server

   ```
   sysconf member <new_secondary_ip> <old_secondary_ip>
   ```

8. **[Primary Server]** Apply a new license

   Apply a new license.

9. **[Secondary Server]** Apply a new license

   Apply a new license.

10. **[Primary Server]** Verify High Availability status

    Change one of the settings for one of the services defined, and verfiy that the change is replicated on the newly configured cluster member.

    Open the *Additions—High Availability* page. Verify that the status of the cluster member is fully synchronized.

    NOTE Be sure to wait for the **Synchronization Interval** time to elapse to ensure that the status shown is current.

11. **[Secondary Server]** Verify call processing

    Manually make a test call into the Secondary Server to verify it processes the call.

2. Software Update

Updating the software on a High Availability cluster requires a set of steps, performed in a specific order on each member.

NOTE These steps are for applying software updates when the updates include voice, matrix, or base rpms. Updating these rpms generally involves a restart of the voice services.

NOTE This procedure assumes the traffic is running on the primary server.

2.1. Update procedure

1. **[Primary Server]** *(optional)* Save the current system data

   Use the *Adminstration—Maintenance* page to make a database backup and download it.

2. **[Secondary Server]** Stop database replication

   ```
   mysql -e 'stop slave'
   ```

3. **[Secondary Server]** Verify call processing

   For alternate-routing network configurations, use these steps:

   - Manually make a test call into the Secondary Server to verify it processes the call.
   - Verify that the upstream PBX/gateway is configured to route calls to the Secondary Server when the Primary Server is unavailable.

4. **[Primary Server]** Stop voice services

   ```
   service voxd stop
   service matrix stop
   ```

5. **[PBX/Switch]** Verify call processing

   Make a test call to verify that the standby Secondary Server receives and processes the call.

6. **[Primary Server]** Upgrade the software package

   Using the *Release Notes* document for the new software, update the packages.

NOTE Usually this process will use the *Adminstration—Software Update* page to upload and install the new software packages.

1. **[Primary Server]** Restore traffic to the Primary Server

   Reboot the server or manually restart the application services, and then make a call into the system.

   Using Realview, verify that the call is being processed by the Primary Server.

   NOTE

   The High Availability status for the standby Secondary Server will be Impaired, since database replication has not yet been restored there.

2. **[Primary Server]** *(optional)* Verify application features

   Verify all existing and new features on the Primary Server.

3. **[Secondary Server]** Enable database replication

   ```
   mysql
   start slave
   show slave status\G
   ```

   NOTE

   The output from the **show slave status** command should have the values shown below

   ```
   Slave_IO_Running: Yes
   Slave_SQL_Running: Yes
   Seconds_Behind_Master: 0
   ```

   Wait until **Seconds_Behind_Master** becomes zero, which means that the cluster member has fully processed all the queued replications from the Primary Server.

4. **[Secondary Server]** Upgrade the software package

   Using the *Release Notes* document for the new software, update the packages. Usually this process will use the *Adminstration—Software Update* page to upload and install the new software packages.

   Reboot the server or manually restart the application services, as per the *Release Notes* document for the new software.

5. **[Primary Server]** Verify High Availability status

   Change one of the settings for one of the services defined, and verfiy that the change is replicated on the newly updated cluster member.

   Open the *Additions—High Availability* page. Verify that the status of the cluster member is fully synchronized.

NOTE	Be sure to wait for the **Synchronization Interval** time to elapse to ensure that the status shown is current.

6. **[Secondary Server]** Verify call processing

   Manually make a test call into the Secondary Server to verify it processes the call.

3. Secondary Server Resync

3.1. Background

On rare occurrences, a High Availability cluster member may need to be resynchronized with the Provisioning Master server. Reasons for the need to resynchronize include:

- Network outage or cluster member stopped for a long period, such that the history log on the Master server wraps
- Inadvertent database changes made on the cluster member, which cause replication data collisions from the Master

3.2. Resync procedure

The following procedure should be performed by the root user, on the Master server and on the Secondary Server that needs to be resynchronized. It is recommended that you open a separate terminal window to each of the servers.

1. **[Secondary Server]** Make a backup of custom settings

   ```
   mysqldump –udbadmin xopdb system_parms > system_parms.sql
   ```

2. **[Primary Server]** Make a database backup and copy it to the Secondary Server

   ```
   service webd stop
   service voxd stop
   mysql -e 'show master status\G'
   mysqldump –udbadmin xopdb > master_db.sql
   service webd start
   service voxd start
   scp master_db.sql <cluster_member>:
   ```

   NOTE <cluster_member> is the address of the member being resynchronized. Be sure to include the colon after the address.

   NOTE Stopping and restarting the voiced and webd services is optional. If there are no changes being made to the system, then these services can remain running.

3. **[Secondary Server]** Reset replication queue

```
mysql
mysql> stop slave;
mysql> reset slave;
mysql> quit;
```

4. **[Secondary Server]** Verify Master database has arrived

```
ll master_db.sql
```

NOTE Verify the date on the file is the current date.

5. **[Secondary Server]** Apply the copied database

```
service voxd stop
service webd stop
mysql xopdb < master_db.sql
mysql xopdb < system_parms.sql
```

6. **[Secondary Server]** Restart replications from the Master

```
mysql
mysql>
change master to master_host=’<master_host>’,master_user=’repl’,master_password=
’slavepass’,
master_log_file=’<file_from_above>’,master_log_pos=<position_from_above>;
mysql>start slave;
mysql>show slave status\G
mysql>quit
```

NOTE The output from the **show slave status** command should have these values shown:

```
Slave_IO_Running: Yes
Slave_SQL_Running: Yes
```

7. **[Secondary Server]** Restart application services

```
service voxd start
service webd start
```

8. **[Primary Server]** Verify High Availability status

   Change one of the settings for one of the services defined, and verfiy that the change is replicated on the newly resynchronized cluster member.

   Open the *Additions—High Availability* page. Verify that the status of the cluster member is fully synchronized.

   > **NOTE** Be sure to wait for the **Synchronization Interval** time to elapse to ensure that the status shown is current.

Appendix A: Troubleshooting

Symptom	Cause	Resolution
High Availability page is not visible under the *Additions* menu	License does not include High Availability	Install the correct license.
Data is different on the Standby machine	• The secondary machine was stopped for an extended period of time (generally a few weeks), then the history of changes made to the master would wrap-around and the synchronization would not be able to automatically restart. • The virtual machine snapshot for the secondary machine was copied from a different server pair. • Software update was done on the secondary machine before being done on the master. • Someone accidentally configured the secondary machine using the web portal.	Perform the **Secondary Server Resync** procedure.
High Availability status shows Impaired	View the detailed status under the *Additions—High Availability*.	Take actions depending on the details shown.
Replicate Provisioning shows **Failed**	Member is down, unreachable, or database replication conflict.	* For database conflict errors, Perform the **Secondary Server Resync** procedure. * For errors other than database conflict, perform the **Network Connectivity Checks** procedure, described below.
Replicate Reports shows **Failed**	Server is down, unreachable, or there is a permissions error.	Perform the **Network Connectivity Checks** procedure, described below.

Desired State is not equal to **Current State**	A software component has failed or is misconfigured	* Perform the **Network Connectivity Checks** procedure, described below. * Contact XOP support.
Clock State shows **Unsynced**	Clock server address is incorrect, or clock server is unreachable.	* From the command-line shell, try to ping the clock server. * From the command-line shell, issue the command **ntpdate**. Verify that the clock server can be reached.

A.1. Network Connectivity Checks

To test network connectivity from a Master server to a Standby or Cluster Member server

Use the following shell command procedure as the root user from the **Standby** server:

```
ping <master_member>
```

If there is no response, then check the console of the master member. If it is active, then check the network wiring and firewall settings.

```
mysql -urepl -h <master_member>
```

You should receive a *Access denied for user ... (using password: NO)* response. If there is no response, then:

- Check the firewall on the master server for port 3306
- Check the **/etc/my.cnf** file on the master to verify the database is listening for external connections (**bind-address**=**localhost** should be commented-out or removed).

```
mysql -urepl -pslavepass -h <master_member>
```

You should be logged-in successfully. If not, the database permissions on the Master server are incorrect. Contact XOP support.

Use the following shell command procedure as the root user from the **Master** server:

```
ping <cluster_member>
```

If there is no response, then check the console of the master member. If it is active, then check the network wiring and firewall settings.

```
ssh <cluster_member>
```

If you are prompted for a password, then the ssh keys are incorrectly installed on the <cluster_member>. Contact XOP support.

Appendix B: License Configuration

In order to support High Availability, additional license entries are required for both the Primary Server and each Secondary Server.

The additional license entries needed for the Primary Server are:

```
replication : true
active_cluster_member : true
provisioning_master: true
```

NOTE It is possible to have a Primary Server which does not process calls (media streams). In this case, the **active_cluster_member** member would be omitted from the license file.

The additional license entries needed for a Secondary Server are:

```
replication : true
active_cluster_member : true
```