SecurityGateway: Configuring Active-Active Database Replication

This document describes how to configure multiple SecurityGateway servers in an Active-Active cluster. In this document, each SecurityGateway server in the cluster is referred to as a node. This document expects that each SecurityGateway node has its own database running on the same machine. This is not a requirement but is done to simplify the configuration process. If you would like to not have your database running on the SecurityGateway node the steps required for configuration may vary slightly.

Even though each node is active, we still refer to primary and secondary nodes to distinguish between servers during the configuration process. The primary node can be any SecurityGateway server in the cluster. If you have a SecurityGateway server that is already up and running, it should be the Primary node as the configurations from that server will be copied to the secondary nodes.

Limitations

- SecurityGateway does not handle the routing of network traffic. We recommend using a third-party load balancer to handle the routing of traffic.
- Replication of archive databases is not supported
- HTTPS settings (including certificates) are per node and will need to be specified for any node added to the cluster/database. Certificates are stored on each node and not in the database.
    - If you want to use the same certificate on each node, you need to manually import that certificate on each node and configure each SG node to use the certificate.
    - You can find these settings by logging into SG and going to Setup / Users | System | Encryption.
        - The STARTTLS Whitelist and STARTTLS Required list configurations are shared.

Requirements

- SecurityGateway version 8.0
- Two or more Firebird 3 Server installations.
- Two or more working SecurityGateway installations configured to use an external Firebird Database servers
- IBReplicator version 5
    - https://www.ibphoenix.com/download/ibreplicator
    - Commercial product that requires licensing. An evaluation license is available.
        - Pricing
            - The "Replication Server License" is counted as a "Replicant License" as well, so for example, a machine that acts as the Replication Server, and has a single Source database, and which is replicating to a remote

Target database, will need only two licenses, not three, i.e a "Replication Server License" and a "Replicant" license.
        - Understanding IBReplicator Licensing
    - All Administrators should review the IBReplicator user manual
    - Download
        - We recommend using the 32 bit version of IBReplicator. If there is a need, the 64 bit "replication server" can be downloaded separately and used on 64bit Windows.
        - https://www.ibphoenix.com/files/IBPReplicatorSetup-5.0.6-Win32.zip
- Shared network storage for Message Data and Bayesian Learning.
    - The SecurityGateway service on each node must be configured to run as a user that has access to the shared network storage.
- A load balancer is needed if you would like for an SG instance to automatically switch to a replicated database if the database it is connected to becomes unavailable.
    - If a load balancer is going to be used to load balance or fail over database traffic, the path to the SecurityGateway database file must be the same on all Firebird servers or a database file alias can be defined. This would require running sgdbtool.exe -setdbconnect on all SecurityGateway servers already connected to the primary database and specifying the alias name as the path.
- If you are not starting with brand new clean SecurityGateway installs you will need to back up the entire SecurityGateway database from the primary server and restore that backup on the secondary server so that both servers are using the exact same configurations.
    - This will overwrite all configurations and data stored on the secondary SecurityGateway node.
    - Depending on your configuration you made need to use Firebirds gbak.exe to complete this step.
- Replication Users must be created in each Firebird Database. IBReplicator will authenticate as this user when making changes to the database. This allows it to ignore any changes to the database that it makes.

Configuration

1) Create a backup of the SecurityGateway database from the primary/existing SecurityGateway server.

a) Open an Administrator command prompt
    i) To open an Administrator command prompt, search for command prompt, right click and select run as Administrator.
b) Navigate to your SecurityGateway\App directory. The default path is %PROGRAMFILES%\MDaemon Technologies\SecurityGateway\App.
c) Run "net stop SecurityGateway".
d) Run "sgdbtool.exe backup $PATH$" Where $PATH$ is the full path, including file name, where you would like the backup to be saved.

2) Restore the database backup file to the secondary Firebird database server(s).

a) Copy the database backup file created in step 1 to a SecurityGateway server that has already been configured (using sgdbtool.exe setdbsconnect) to connect to the secondary Firebird database server.
b) On the SecurityGateway Server Open an Administrator command prompt.
c) Navigate to your SecurityGateway\App directory. The default path is %PROGRAMFILES%\MDaemon Technologies\SecurityGateway\App.
d) Run "net stop SecurityGateway"
e) Run "sgdbtool restore $PATH$" Where $PATH$ is the full path, including file name, where you copied the backup file to in step 2a.
f) Repeat step 2 for each secondary Firebird database server.

3) Create a "Replication User" in each copy of the database. This must be performed for the primary Firebird database server and all secondary Firebird database servers.

a) On the SecurityGateway server open an Administrator command prompt
b) Run "sgdbtool.exe createdbuser".
c) Enter the IP or Hostname to the Firebird database server.
d) Enter the Port Firebird is listening on.
e) Enter the path to the SecurityGateway database on the Firebird database server.
f) Enter the username for the Firebird database.
g) Enter the password for the Firebird database account specified.
h) Enter "REPL" for the username for the replication user account.
i) Enter a password for the replication user account.
    i) Remember the password you enter as you will need it later.
j) You should see "Firebird user successfully created and granted RDB$ADMIN role"
    i) If you do not see this, retry step 3.
k) Repeat Step 3 for each Firebird database server.

4) Prepare each copy of the database for replication. This must be performed for all secondary Firebird database servers. Do not perform this step for the primary Firebird database server.

a) On the SecurityGateway server open an Administrator command prompt
b) Run "sgdbtool.exe setdbreplication".
c) Enter the IP or Hostname to the secondary Firebird database server.
d) Enter the Port Firebird is listening on.
e) Enter the path to the SecurityGateway database on the secondary Firebird database server.
f) Enter the username for the Firebird database.
g) Enter the password for the Firebird database account specified.
h) Enter a unique number as the database replication instance ID
    i) This value must be different for each instance of the DB.
    ii) If this is the only secondary server database you have, enter 2.

i) You should see “Database successfully prepared for replication”
   i) If you do not, retry step 4.

j) Repeat step 4 on each secondary SecurityGateway database instance.
   i) Do NOT run this on the primary SecurityGateway database instance.
   ii) Make sure to use a unique value for each database instance.

5) Install IBReplicator

a) IBReplicator may be installed on any server that can connect to all of the FireBird database servers. This includes but is not limited to the primary Firebird database server.
b) On the selected server extract the IBReplicator installer from the IBPReplicatorSetup ZIP file that was downloaded.
c) Right click on the IBReplicatorSetup Installer and select Run as Administrator
d) On the Select Components dialog of the installation, make sure Replication Server and Replication management tools are selected.
   i) The Avalerion CDC plugin is not required.

6) Create IBReplicator configuration

a) Click the Windows button to open the Start Menu and run IBReplicator / Replication Manager.
b) Select File | New Configuration
c) Select Firebird as the Server type
d) For the Connection String enter the path where you would like the Replication Database to be created (c:\databases\replication.fdb)
e) In the User Name field enter the Administrator user name for the database.
   i) The username specified will be used to create the Administrator account in the replication database
   ii) SYSDBA is usually the default Administrator account.
f) In the Password field enter the Password you would like to use.
   i) Be sure to save the username and password that you enter as it will be needed in the future.
g) Click Create

7) Register IBReplicator

a) Select Tools | License Manager
b) Click Add
c) Enter your License ID
d) Enter your License Key
e) Click OK
f) Repeat step 18 for your second license
   i) You should have a Server license and a Replicant license.
g) Click Close

8) Add Primary Database to IBReplicator

a) Select Database | Add
b) Select “Firebird” as the Type

c) In the Descriptive name field enter a description. For example, “SG Primary Database”.
d) In the Server field enter the connection string to the primary SecurityGateway database in the format <IP ADDRESS>/<PORT>:<PATH>
    i) For example 192.168.1.100/3050:C:\databases\SECURITYGATEWAY.fbd.
    ii) The hostname of the server may also be specified.
e) In the Administrative username field enter “REPL”.
f) In the Administrative password field enter the password of the replication user that was created in step 3.
g) In the Character set field select UTF8.
h) In the Administrative role field enter “RDB$ADMIN”
i) Click “Test Connection” to verify the connection details
    i) If the connection fails, verify you have entered everything correctly and that the Firebird service is running.
j) Click OK

9) Add Secondary Database(s) to IBReplicator

a) Repeat step 8 to add each secondary SecurityGateway database.
b) Be sure to enter a different value in the Descriptive name field.
c) Be sure to enter a connection string that points to the secondary SecurityGateway database.

10) Define Replication Scheme (Primary to Secondary)

a) Select Replication | Schema | New
b) In the Schema name field enter a name for the Schema.
    i) For example, “SecurityGateway: Primary to Secondary”
c) Click the Connection tab
d) In the Registered Database field, verify that the primary SecurityGateway database, “SG Primary Database” is selected.
e) In the Replication username field enter “REPL”.
    i) Do not specify SYSDBA.
f) In the Replication password field enter the password for the account created in step 3.
g) In the Replication role field enter “RDB$ADMIN”
h) Click Test Connection
    i) If there is an error, verify the information you entered is correct and that the Firebird service is running.
i) Click OK

11) Add Replication Target

a) From the Registered database drop down select the secondary SecurityGateway database
b) In the Replication username field enter “REPL”.
    i) Do not specify SYSDBA.
c) In the Replication password field enter the password for the account created in step 3.
d) In the Replication role field enter “RDB$ADMIN”
e) Click Test Connection
    i) If there is an error, verify the information you entered is correct and that the Firebird service is running.
f) Click OK

12) Define Replicated Tables

a) Select Replication | Tables | AutoGenerate
b) Click the Select all button
c) Select the Use asterisk checkbox
d) Click the Generate button
    i) When complete it should show “0 errors found.”
e) Click Close

13) Remove Sequences from Replication

a) Select Replication | Sequences | Define
b) Select a sequence in the “Source objects and mappings” list
c) Press CTRL+A to select all sequences
d) Drag and drop the selected items to the “Target objects” list
e) Click OK
f) The Replicated sequences node in the Tree view should be empty

14) Define Replication Table Order

a) In the Tree view, expand the Target databases node
b) Expand the target database node
c) Expand the “Replicated tables and procedures” node
d) Select the table from the list below and use the “Move Up” button in the toolbar to move the table to the top of the list. Repeat this process for each table, moving each just below the previous.
    i) Domains
    ii) Users
    iii) Messages
    iv) ArchiveStores

15) Define Key Columns (Unique Constraints)

a) Select the Domains Table
b) Right click on the table to display the context menu
c) Select Keys
d) In the “Source objects and mappings” list, select the “ID” column and double click it to remove it as a key column.
e) In the “Target objects” list, double click on the “NAME” column to add it as a key column.
f) Repeat the above with the following table. Remove the ID column as a key column for each and add the specified columns as key columns.
    i) LISTS
        (1) OWNERID
        (2) LISTTYPE
        (3) IP
        (4) VAL
    ii) SERVERSETTINGS
        (1) SERVERID
        (2) SECTION
        (3) NAME
    iii) SETTING
        (1) DOMAINID
        (2) SECTION
        (3) NAME
    iv) USERSETTINGS
        (1) USERID
        (2) SECTION
        (3) NAME

16) Create Replication System Objects in the Primary Database

a) In the Tree view, select the source database “SG Primary Database”
b) Right click
c) Select “Create System Objects” from the context menu

17) Synchronize Secondary Database with Primary

a) Select the Target Database “SG Secondary Database”
b) Replication | Synchronize
c) Click the Select All button
d) Click the Synchronize button
e) When the synchronization is finished click Close

18) Define Replication Scheme (Secondary to Primary)

a) Repeat steps 10 – 16 using the secondary database as the source database and the primary database as the target database.
b) Step 17, Synchronization, is not necessary.

19) Select Configuration | Set as default

20) Select Tools | Notify Server | Reload parameters

21) Select Tools | Notify Server | Replicate now

22) Open and review the replication log.

a) A utility that can tail the log file, i.e. WinTail is very helpful when monitoring the log file
b) The default log file location is… %PROGRAMDATA%\IBPReplicator\Replicate.log
c) Verify replication is occurring
d) If there are errors
    i) Review the configuration to make sure all steps were completed correctly
    ii) Verify the IBRepl service is running
    iii) Verify the FireBird service is running on the primary and secondary servers

23) Once you have verified replication is working.

a) Start SecurityGateway on the primary and secondary server.

24) Schedule Replication

a) Select Tools | Scheduler
b) Check the box for “Scheduler Enabled”
c) Select Options | Add
d) From the Frequency drop down select Periodically.
e) From the every (second) drop down select 5.
    i) There may be times that longer intervals are appropriate, especially on very busy servers. If the synchronization does not complete in the interval, or that system is under heavy load a longer time may be selected.
f) Click OK
g) Select Options | Reload Schedule
h) Close the Replication Schedule window.
i) Select Tools | Notify server | Reload parameters
    i) Open and review the Replicate.log file to verify replications are occurring according to the specified schedule.

Once replication is setup, you should be able to login to the SecurityGateway primary or secondary node, make a configuration change, and that change should appear in the other node. Both nodes in the cluster should be able to accept and process email and HTTP traffic.