Genesys Mobile Services Deployment Guide

Configuring an External Cassandra

12/19/2025

Contents

Configuring an External Cassandra

Genesys Mobile Services (GMS) is packaged with an embedded Cassandra; however, GMS also supports deployments with an external Cassandra(s). An external Cassandra might be used in the following scenarios:

- You already have a Cassandra/Datastax deployment.
- You are securing your data in segregated networks, cages, and racks.
- You want multiple redundancy features, such as distinct data centers, rack, and chassis awareness.

Configuring GMS for an external Cassandra is a multi-step process to enable connection, authentication, and authorization. The steps include setting configuration options in Configuration Manager (or Genesys Administrator), changing configuration settings in the `cassandra.yaml` file, and executing Cassandra Query Language (CQL) commands.

> **Important**
> All external Cassandra nodes must be of the same version.

Configuration Options

The following tables list the configuration options applicable to an external Cassandra deployment. Changes take effect after restart.

cassandra Section

Option	Default Value	Description
nodes		List of Cassandra hosts or IP addresses, comma separated. For example: `host1,192.168.1.2`
port	0	The listening port of the Cassandra server (that is, the port on which Thrift listens for clients).
create-embedded-server	true	Set this option to **`false`** to connect to an external Cassandra instance. If set to `true`, creates and connects to the Cassandra server embedded with GMS and ignores all other options in the cassandra section.

Option	Default Value	Description
create-schema	true	If set to `true`, creates (if needed) keyspaces and column families for GMS. If set to `false`, does not create keyspaces.
keyspace-prefix		Specifies the prefix for GMS keyspace naming. The default value is empty for backward compatibility. Note: If this value is left empty, the `gsg` and `gsg_dd` keyspaces will be created in Cassandra.
strategy-class	SimpleStrategy	Specifies the strategy class that Cassandra uses for the cluster. Valid values are: `SimpleStrategy`, which defines a single cluster without multiple Data Centers. `NetworkTopologyStrategy`, which is a network strategy in conjunction with the `cassandra-topology` properties file (located in the install configuration directory for each Cassandra instance), defines the Data Centers for the Cassandra cluster. Multiple Data Centers are typically geographically dispersed.
strategy-option	replication_factor:4	Specifies the replication factor value according to the strategy-class: If the strategy class is `SimpleStrategy`, set this value to `replication_factor:2`, where 2 is the number of Cassandra nodes. If the strategy class is `NetworkTopologyStrategy`, set this value to `DC1:2;DC2:3`, where `DC` is the Data Center topology.

cassandra-authentication-security Section

Note: The user name and password is replicated to all nodes.

Option	Description
username	the Cassandra user name
password	the Cassandra user password

Connection to an External Cassandra

The following steps are required to enable GMS to connect to an external Cassandra.

1. In Configuration Manager, locate and open your GMS Application object.
2. On the Options tab, `cassandra` section, set the following options:
   - nodes = <your Cassandra hosts or IP addresses>
   - port = <your Cassandra port>
   - create_embedded_server = `false`
   - strategy-class = `SimpleStrategy` or `NetworkTopologyStrategy`
   - strategy-option = `replication_factor:2` or `DC1:2;DC2:3`
3. Restart GMS.

Authentication on External Cassandra

Note: Supports Cassandra version 2.0.x and higher.

The following steps are prerequisites prior to enabling authentication.

Configure cassandra.yaml File

1. On the external Cassandra, open the `cassandra.yaml` configuration file.
2. Make sure that `cluster_name` is the same for all nodes.
3. Locate the seed nodes. This is the field for all Cassandra nodes; change it accordingly (for the seed node, this will be it's own port, for the non-seed nodes, this will be the IP address of the seed node).
4. Make sure that `listen_address` is changed from `127.0.0.1` to the current IP address.
5. Make sure that `rpc_address` is changed from `127.0.0.1` to the current IP address.

The following steps are required to enable authentication.

Configure cassandra.yaml File

1. On the external Cassandra, open the `cassandra.yaml` configuration file.
2. Locate the `authenticator` field.
3. Change the value from `AllowAllAuthenticator` to `PasswordAuthenticator`. Note: The full classname is `org.apache.cassandra.auth.PasswordAuthenticator`.
4. Save the file.
5. Repeat these steps on each external Cassandra instance.

Execute CQL Commands

1. On the external Cassandra, using the cqlsh utility (included with Cassandra), create your username and password. **Note:** The default superuser is `cassandra` with pasword `cassandra`. The following example shows a `genesys` user with `genesys` password.

Note: This step is required to be completed on only one external Cassandra instance. It will then be replicated to the other nodes.

```
$ cqlsh -u cassandra -p cassandra cassandra_host cassandra_port
> CREATE USER genesys WITH PASSWORD 'genesys';
> LIST USERS;
name | super
-----------+-------
 genesys | False
 cassandra | True
```

On Windows OS / Cassandra versions 2.1 or higher, replace:

```
$ cqlsh -u cassandra -p cassandra cassandra_host cassandra_port
```

with:

```
{path_to_cassandra}\bin>{path_to_python}\python.exe cqlsh cassandra_host -u cassandra
-p cassandra
```

Set the options of `cqlsh` before parameters or set your python 2.7 path in PATH environment variable like this:

```
PATH={path_to_python};%PATH%
```

Therefore, you can launch the `cqlsh` script using the `cqlsh.bat` command:

```
cqlsh.bat -u cassandra –p cassandra cassandra_host
```

Using the default cassandra port of `native_transport_port` (default is `9042`). Otherwise you will need to add the port parameter to the cqlsh script.

Set Configuration Options

1. In Configuration Manager, locate and open your GMS Application object.
2. On the Options tab, `cassandra-authentication-security` section, set the following options with the same username and password that you just created on the external Cassandra.
   - username, for example, `genesys`
   - password, for example, `genesys`
3. Restart GMS. The Pelops and Hector clients connect to the external Cassandra using the login and password.

Authorization on External Cassandra

Note: Supports Cassandra version 2.0.x and higher.

After creating the authentication, you must enable authorization and create keyspaces.

Configure cassandra.yaml File

1. On the external Cassandra, open the `cassandra.yaml` configuration file.
2. Locate the `authorizer` field.
3. Change the value from `AllowAllAuthorizer` to `CassandraAuthorizer`. Note: The full classname is `org.apache.cassandra.auth.CassandraAuthorizer`.
4. Save the file.
5. Repeat these steps on each external Cassandra instance.

Execute CQL Commands

To authorize actions on the keyspace, you must first create the keyspace(s), and then grant permissions on them.

1. On the external Cassandra, using the cqlsh utility (included with Cassandra), create your keyspaces. The following example shows the `gsg` and `gsg_dd` keyspace.

Note: This step is required to be completed on only one external Cassandra instance. It will then be replicated to the other nodes.

```
$ cqlsh -u cassandra -p cassandra cassandra_host cassandra_port
> LIST USERS;
name | super
-----------+-------
 genesys | False
 cassandra | True
> LIST ALL PERMISSIONS OF genesys;
 (0 rows)

> CREATE KEYSPACE gsg WITH REPLICATION = { 'class' : 'SimpleStrategy', 'replication_factor' :
3 };
> CREATE KEYSPACE gsg_dd WITH REPLICATION = { 'class' : 'SimpleStrategy',
'replication_factor' : 3 };
> GRANT ALTER ON KEYSPACE gsg TO genesys;
> GRANT CREATE ON KEYSPACE gsg TO genesys;
> GRANT DROP ON KEYSPACE gsg TO genesys;
> GRANT MODIFY ON KEYSPACE gsg TO genesys;
> GRANT SELECT ON KEYSPACE gsg TO genesys;
> LIST ALL PERMISSIONS OF genesys;
username | resource | permission
----------+----------------+------------
 genesys | <keyspace gsg> | CREATE
 genesys | <keyspace gsg> | ALTER
 genesys | <keyspace gsg> | DROP
 genesys | <keyspace gsg> | SELECT
 genesys | <keyspace gsg> | MODIFY
(5 rows)
```

```
> GRANT ALTER ON KEYSPACE gsg_dd TO genesys;
> GRANT CREATE ON KEYSPACE gsg_dd TO genesys;
> GRANT DROP ON KEYSPACE gsg_dd TO genesys;
> GRANT MODIFY ON KEYSPACE gsg_dd TO genesys;
> GRANT SELECT ON KEYSPACE gsg_dd TO genesys;
> LIST ALL PERMISSIONS OF genesys;
username | resource | permission
----------+------------------+------------
 genesys | <keyspace gsg> | CREATE
 genesys | <keyspace gsg> | ALTER
 genesys | <keyspace gsg> | DROP
 genesys | <keyspace gsg> | SELECT
 genesys | <keyspace gsg> | MODIFY
 genesys | <keyspace gsg_dd> | CREATE
 genesys | <keyspace gsg_dd> | ALTER
 genesys | <keyspace gsg_dd> | DROP
 genesys | <keyspace gsg_dd> | SELECT
 genesys | <keyspace gsg_dd> | MODIFY
(10 rows)
```

Note: You do not need to set any additional option in the GMS application.

2. Restart GMS. The Pelops and Hector clients connect to the external Cassandra and are authorized to manage the GMS keyspaces (`gsg` and `gsg_dd`).

Final Steps

- In the GMS Application > Security section > Log On As SYSTEM Account.
- The time zone for all nodes must be the same. Make sure that you synchronize the time before testing.