Genesys Web Engagement

cassandraEmbedded Section

5/8/2025

cassandraEmbedded Section

authenticator

Default Value: AllowAllAuthenticator
Valid Values: AllowAllAuthenticator, PasswordAuthenticator
Changes Take Effect: After start or restart

The authentication backend, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authenticate_c.html.

authorizer

Default Value: AllowAllAuthorizer
Valid Values: AllowAllAuthorizer, CassandraAuthorizer
Changes Take Effect: After start or restart

The authorization backend, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authorize_c.html.

clusterName

Default Value: Cluster
Valid Values: Valid string
Changes Take Effect: After start or restart

The name of the cluster. This setting prevents nodes in one logical cluster from joining another. All nodes in a cluster must have the same value.

commitLogDirectory

Default Value: ./storage/commitlog
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory where the commit log is stored.

commitLogSync

Default Value: periodic
Valid Values: periodic, batch
Changes Take Effect: After start or restart

The method that Cassandra uses to acknowledge writes, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/dml/dml_durability_c.html.

commitLogSyncPeriod

Default Value: 10000
Valid Values: Valid integer
Changes Take Effect: After start or restart

The period that Cassandra uses to acknowledge writes (in milliseconds).

configFile

Default Value:
Valid Values: Valid YAML file path
Changes Take Effect: After start or restart

Embedded Cassandra external configuration YAML file path. Overrides all Cassandra settings.

dataDirectory

Default Value: ./storage/data
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory location where table data (SSTables) is stored. Cassandra distributes data evenly across the location, subject to the granularity of the configured compaction strategy.

enabled

Default Value: true
Valid Values: true, false
Changes Take Effect: After start or restart

Indicates whether the Embedded Cassandra service is enabled.

encryption.client.clientAuth

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables certificate authentication.

encryption.client.enabled

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables client-to-node encryption. You must also generate keys and provide the appropriate key and trust store locations and passwords. No custom encryption options are currently enabled, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLClientToNode_t.html.

encryption.client.keystore

Default Value: conf/.keystore
Valid Values: Valid path
Changes Take Effect: After start or restart

The location of a client-side Java keystore (JKS) suitable for use with Java Secure Socket Extension (JSSE), which is the Java version of the Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocols. The keystore contains the private key used to encrypt outgoing messages.

encryption.client.keystorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the client-side keystore. This must match the password used when generating the keystore and truststore.

encryption.client.truststore

Default Value: conf/.truststore
Valid Values: Valid path
Changes Take Effect: After start or restart

Set if **encryption.client.clientAuth** is true.

encryption.client.truststorePassword

Default Value: *truststore_password*
Valid Values: Valid string
Changes Take Effect: After start or restart

Set if **encryption.client.clientAuth** is true.

encryption.server.clientAuth

Default Value: false
Valid Values: true, false
Changes Take Effect: After start or restart

Enables or disables certificate authentication.

encryption.server.internode

Default Value: none
Valid Values: none, all, dc, rack
Changes Take Effect: After start or restart

Enables or disables inter-node encryption. You must also generate keys and provide the appropriate key and trust store locations and passwords. No custom encryption options are currently enabled, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLNodeToNode_t.html.

encryption.server.keystore

Default Value: conf/.keystore
Valid Values: Valid path
Changes Take Effect: After start or restart

The location of a server-side Java keystore (JKS) suitable for use with Java Secure Socket Extension (JSSE), which is the Java version of the Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocols. The keystore contains the private key used to encrypt outgoing messages.

encryption.server.keystorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the server-side keystore.

encryption.server.truststore

Default Value: conf/.truststore
Valid Values: Valid path
Changes Take Effect: After start or restart

Location of the truststore containing the trusted certificate for authenticating remote servers.

encryption.server.truststorePassword

Default Value: cassandra
Valid Values: Valid string
Changes Take Effect: After start or restart

Password for the truststore.

endpointSnitch

Default Value: GossipingPropertyFileSnitch
Valid Values: SimpleSnitch, GossipingPropertyFileSnitch, PropertyFileSnitch, Ec2Snitch, Ec2MultiRegionSnitch, RackInferringSnitch
Changes Take Effect: After start or restart

A snitch determines which data centers and racks nodes belong to. They inform Cassandra about the network topology so that requests are routed efficiently. They also allow Cassandra to distribute replicas by grouping machines into data centers and racks. Specifically, the replication strategy places the replicas based on the information provided by the new snitch as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architectureSnitchesAbout_c.html.

nativeTransportPort

Default Value: 9042
Valid Values: Valid port number
Changes Take Effect: After start or restart

Port on which the CQL native transport listens for clients.

numTokens

Default Value: 256
Valid Values: Valid integer
Changes Take Effect: After start or restart

Defines the number of tokens randomly assigned to this node on the ring when using virtual nodes (vnodes). The more tokens, relative to other nodes, the larger the proportion of data that the node stores.

partitioner

Default Value: org.apache.cassandra.dht.Murmur3Partitioner
Valid Values: org.apache.cassandra.dht.RandomPartitioner, org.apache.cassandra.dht.RandomPartitioner, org.apache.cassandra.dht.Murmur3Partitioner
Changes Take Effect: After start or restart

A partitioner determines how data is distributed across the nodes in the cluster (including replicas). Basically, a partitioner is a function for deriving a token representing a row from its partition key, typically by hashing. Each row of data is then distributed across the cluster by the value of the token, as described at http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architecturePartitionerAbout_c.html.

readTimeout

Default Value: 5000
Valid Values: Valid long
Changes Take Effect: After start or restart

The time (in milliseconds) that the coordinator waits for read operations to complete.

rpcPort

Default Value: 9160
Valid Values: Valid port number
Changes Take Effect: After start or restart

Thrift port for client connections.

savedCachesDirectory

Default Value: ./storage/saved_caches
Valid Values: Valid folder path
Changes Take Effect: After start or restart

The directory location where table key and row caches are stored.

seedNodes

Default Value:
Valid Values: A single or comma-delimited list of IP addresses
Changes Take Effect: After start or restart

A comma-delimited list of IP addresses used by gossip for bootstrapping new nodes joining a cluster. In multiple data-center clusters, the seed list should include at least one node from each data center (replication group). More than a single seed node per data center is recommended for fault tolerance. Otherwise, gossip has to communicate with another data center when bootstrapping a node. Making every node a seed node is **not** recommended because of increased maintenance and reduced gossip performance. Gossip optimization is not critical, but Genesys recommends that you use a small seed list. For more information, refer to https://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureGossipAbout_c.html.

sslStoragePort

Default Value: 7001
Valid Values: Valid port number

Changes Take Effect: After start or restart

The SSL port for encrypted communication. Not used unless enabled in the **encryption.server.internode** option.

storagePort

Default Value: 7000
Valid Values: Valid port number
Changes Take Effect: After start or restart

The port for inter-node communication.

writeTimeout

Default Value: 2000
Valid Values: Valid long
Changes Take Effect: After start or restart

The time (in milliseconds) that the coordinator waits for write operations to complete.