



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Deployment Guide

cassandraEmbedded Section

12/22/2025

# cassandraEmbedded Section

**Note:** The options in this section are applicable only when `enabled = true`.

## Contents

- 1 **cassandraEmbedded Section**
  - 1.1 **enabled (Cluster Only)**
  - 1.2 **clusterName (Cluster Only)**
  - 1.3 **endpointSnitch (Cluster Only)**
  - 1.4 **partitioner (Cluster Only)**
  - 1.5 **dataDirectory**
  - 1.6 **commitLogDirectory**
  - 1.7 **savedCachesDirectory**
  - 1.8 **seedNodes (Cluster Only)**
  - 1.9 **rpcAddress (Node Only)**
  - 1.10 **listenAddress (Node Only)**
  - 1.11 **rpcPort**
  - 1.12 **nativeTransportPort**
  - 1.13 **storagePort**
  - 1.14 **sslStoragePort**
  - 1.15 **commitLogSync**
  - 1.16 **commitLogSyncPeriod**
  - 1.17 **numTokens**
  - 1.18 **authenticator**
  - 1.19 **authorizer**
  - 1.20 **writeTimeout**
  - 1.21 **readTimeout**
  - 1.22 **configFile**
  - 1.23 **encryption.server.internode**
  - 1.24 **encryption.server.keystore**
  - 1.25 **encryption.server.keystorePassword**
  - 1.26 **encryption.server.truststore**

- [1.27 encryption.server.truststorePassword](#)
- [1.28 encryption.server.clientAuth](#)
- [1.29 encryption.client.enabled](#)
- [1.30 encryption.client.keystore](#)
- [1.31 encryption.client.keystorePassword](#)
- [1.32 encryption.client.truststore](#)
- [1.33 encryption.client.truststorePassword](#)
- [1.34 encryption.client.clientAuth](#)

### enabled (Cluster Only)

**Description:** Indicates whether the Embedded Cassandra service is enabled.

**Mandatory:** No

**Default Value:** true

**Valid Values:** true, false

**Changes Take Effect:** After start/restart

### clusterName (Cluster Only)

**Description:** 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.

**Default Value:** Cluster

**Valid Values:** Valid string

**Mandatory:** No

**Changes Take Effect:** After start/restart

### endpointSnitch (Cluster Only)

**Description:** 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](http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architectureSnitchesAbout_c.html).

**Default Value:** GossipingPropertyFileSnitch

**Valid Values:** SimpleSnitch, GossipingPropertyFileSnitch, PropertyFileSnitch, Ec2Snitch, Ec2MultiRegionSnitch, RackInferringSnitch

**Mandatory:** No

**Changes Take Effect:** After start/restart

### partitioner (Cluster Only)

**Description:** 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](http://docs.datastax.com/en/cassandra/2.1/cassandra/architecture/architecturePartitionerAbout_c.html).

**Default Value:** org.apache.cassandra.dht.Murmur3Partitioner

**Valid Values:** org.apache.cassandra.dht.RandomPartitioner,  
org.apache.cassandra.dht.RandomPartitioner,  
org.apache.cassandra.dht.Murmur3Partitioner

**Mandatory:** No

**Changes Take Effect:** After start/restart

## dataDirectory

**Description:** 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.

**Default Value:** ./storage/data

**Valid Values:** Valid folder path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## commitLogDirectory

**Description:** The directory where the commit log is stored.

**Default Value:** ./storage/commitlog

**Valid Values:** Valid folder path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## savedCachesDirectory

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

**Default Value:** ./storage/saved\_caches

**Valid Values:** Valid folder path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## seedNodes (Cluster Only)

**Description:** 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](https://docs.datastax.com/en/cassandra/2.0/cassandra/architecture/architectureGossipAbout_c.html).

**Valid Values:** A single or comma-delimited list of IP addresses

**Mandatory:** Yes

**Changes Take Effect:** After start/restart

## rpcAddress (Node Only)

**Description:** The listen address for thrift client connections.

**Valid Values:** Valid IP address or hostname of the host where the Web Engagement Server is running

**Mandatory:** Yes

**Changes Take Effect:** After start/restart

## listenAddress (Node Only)

**Description:** The IP address or hostname that Cassandra binds to for connecting to other Cassandra nodes.

**Valid Values:** Valid IP address or hostname of the host where the Web Engagement Server is running

**Mandatory:** Yes

**Changes Take Effect:** After start/restart

## rpcPort

**Description:** Thrift port for client connections.

**Default Value:** 9160

**Valid Values:** Valid port number

**Mandatory:** No

**Changes Take Effect:** After start/restart

## nativeTransportPort

**Description:** Port on which the CQL native transport listens for clients.

**Default Value:** 9042

**Valid Values:** Valid port number

**Mandatory:** No

**Changes Take Effect:** After start/restart

## storagePort

**Description:** The port for inter-node communication.

**Default Value:** 7000

**Valid Values:** Valid port number

**Mandatory:** No

**Changes Take Effect:** After start/restart

## sslStoragePort

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

**Default Value:** 7001

**Valid Values:** Valid port number

**Mandatory:** No

**Changes Take Effect:** After start/restart

## commitLogSync

**Description:** 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](http://docs.datastax.com/en/cassandra/2.1/cassandra/dml/dml_durability_c.html).

**Default Value:** periodic

**Valid Values:** periodic, batch

**Mandatory:** No

**Changes Take Effect:** After start/restart

## commitLogSyncPeriod

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

**Default Value:** 10000

**Valid Values:** Valid integer

**Mandatory:** No

**Changes Take Effect:** After start/restart

## numTokens

**Description:** 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.

**Default Value:** 256

**Valid Values:** Valid integer

**Mandatory:** No

**Changes Take Effect:** After start/restart

## authenticator

**Description:** The authentication backend, as described at [http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure\\_about\\_native\\_authenticate\\_c.html](http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authenticate_c.html).

**Default Value:** AllowAllAuthenticator

**Valid Values:** AllowAllAuthenticator, PasswordAuthenticator

**Mandatory:** No

**Changes Take Effect:** After start/restart

## authorizer

**Description:** The authorization backend, as described at [http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure\\_about\\_native\\_authorize\\_c.html](http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secure_about_native_authorize_c.html).

**Default Value:** AllowAllAuthorizer

**Valid Values:** AllowAllAuthorizer, CassandraAuthorizer

**Mandatory:** No

**Changes Take Effect:** After start/restart

## writeTimeout

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

**Default Value:** 2000

**Valid Values:** Valid long

**Mandatory:** No

**Changes Take Effect:** After start/restart

## readTimeout

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

**Default Value:** 5000

**Valid Values:** Valid long

**Mandatory:** No

**Changes Take Effect:** After start/restart

## configFile

**Description:** Embedded Cassandra external configuration YAML file path. Overrides all Cassandra settings.

**Valid Values:** Valid YAML file path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.internode

**Description:** 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](http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLNodeToNode_t.html).

**Default Value:** none

**Valid Values:** none, all, dc, rack

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.keystore

**Description:** 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.

**Default Value:** conf/.keystore

**Valid Values:** Valid path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.keystorePassword

**Description:** Password for the server-side keystore.

**Default Value:** cassandra



**Valid Values:** Valid string

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.truststore

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

**Default Value:** conf/.truststore

**Valid Values:** Valid path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.truststorePassword

**Description:** Password for the truststore.

**Default Value:** cassandra

**Valid Values:** Valid string

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.server.clientAuth

**Description:** Enables or disables certificate authentication.

**Default Value:** false

**Valid Values:** true, false

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.enabled

**Description:** 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](http://docs.datastax.com/en/cassandra/2.1/cassandra/security/secureSSLClientToNode_t.html).

**Default Value:** false

**Valid Values:** true, false

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.keystore

**Description:** 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.

**Default Value:** conf/.keystore

**Valid Values:** Valid path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.keystorePassword

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

**Default Value:** cassandra

**Valid Values:**

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.truststore

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

**Default Value:** conf/.truststore

**Valid Values:** Valid path

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.truststorePassword

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

**Default Value:** *truststore\_password*

**Valid Values:** Valid string

**Mandatory:** No

**Changes Take Effect:** After start/restart

## encryption.client.clientAuth

**Description:** Enables or disables certificate authentication.

**Default Value:** false

**Valid Values:** true, false

**Mandatory:** No

**Changes Take Effect:** After start/restart