



DataStax Distribution of Apache Cassandra™ 3.x for Windows Documentation

August 11, 2016

Apache, Apache Cassandra, Apache Hadoop, Hadoop and the eye logo are trademarks of the Apache Software Foundation

© 2016 DataStax, Inc. All rights reserved.

Contents

About Apache Cassandra.....	7
What's new?.....	9
Understanding the architecture.....	11
Architecture in brief.....	11
Internode communications (gossip).....	13
Failure detection and recovery.....	13
Data distribution and replication.....	14
Consistent hashing.....	14
Virtual nodes.....	15
Data replication.....	17
Partitioners.....	18
Murmur3Partitioner.....	18
RandomPartitioner.....	18
ByteOrderedPartitioner.....	19
Snitches.....	19
Dynamic snitching.....	19
SimpleSnitch.....	20
RackInferringSnitch.....	20
PropertyFileSnitch.....	20
GossipingPropertyFileSnitch.....	21
Ec2Snitch.....	22
Ec2MultiRegionSnitch.....	22
GoogleCloudSnitch.....	24
CloudstackSnitch.....	24
Database internals.....	25
Storage engine.....	25
How Cassandra reads and writes data.....	25
How is data written?.....	25
How is data maintained?.....	27
How is data updated?.....	32
How is data deleted?.....	33
How are indexes stored and updated?.....	34
How is data read?.....	35
How do write patterns affect reads?.....	38
Data consistency.....	38
How are consistent read and write operations handled?.....	38
How are Cassandra transactions different from RDBMS transactions?.....	40
How do I accomplish lightweight transactions with linearizable consistency?.....	40
How do I discover consistency level performance?.....	41
How is the consistency level configured?.....	42
How is the serial consistency level configured?.....	44
How are read requests accomplished?.....	45
How are write requests accomplished?.....	55

Planning a cluster deployment.....	58
Installing.....	58
Installing DataStax Distribution of Apache Cassandra 3.x for Windows.....	58
Windows troubleshooting.....	59
Installing earlier releases of DataStax Distribution of Apache Cassandra 3.x for Windows.....	60
Uninstalling DataStax Distribution of Apache Cassandra 3.x for Windows.....	60
Installing on cloud providers.....	61
Recommended production settings for Linux and Windows.....	61
Windows installation directories.....	61
Configuration.....	62
cassandra.yaml configuration file.....	63
Cassandra include file.....	82
Security.....	82
Securing Cassandra.....	82
SSL encryption.....	82
Internal authentication.....	87
Internal authorization.....	89
Enabling JMX authentication.....	91
Configuring gossip settings.....	92
Configuring the heap dump directory.....	93
Configuring virtual nodes.....	94
Enabling virtual nodes on a new cluster.....	94
Enabling virtual nodes on an existing production cluster.....	94
Using multiple network interfaces.....	95
Configuring logging.....	97
Commit log archive configuration.....	99
Generating tokens.....	100
Hadoop support.....	100
Initializing a cluster.....	102
Initializing a multiple node cluster (single data center).....	102
Initializing a multiple node cluster (multiple data centers).....	105
Starting or stopping Cassandra.....	107
Clearing the data from Windows.....	108
Operations.....	108
Adding or removing nodes, data centers, or clusters.....	108
Adding nodes to an existing cluster.....	108
Adding a data center to a cluster.....	110
Replacing a dead node or dead seed node.....	111
Replacing a running node.....	112
Moving a node from one rack to another.....	113
Decommissioning a data center.....	113
Removing a node.....	114
Switching snitches.....	114
Changing keyspace replication strategy.....	116
Edge cases for transitioning or migrating a cluster.....	116
Adding or replacing single-token nodes.....	117
Backing up and restoring data.....	120

About snapshots.....	120
Taking a snapshot.....	120
Deleting snapshot files.....	121
Enabling incremental backups.....	121
Restoring from a snapshot.....	122
Restoring a snapshot into a new cluster.....	123
Recovering from a single disk failure using JBOD.....	123
Repairing nodes.....	125
Hinted Handoff: repair during write path.....	125
Read Repair: repair during read path.....	127
Manual repair: Anti-entropy repair.....	127
Migrating to incremental repairs.....	132
Monitoring Cassandra.....	133
Monitoring a Cassandra cluster.....	133
Tuning Java resources.....	138
Data caching.....	141
Configuring data caches.....	141
Monitoring and adjusting caching.....	143
Configuring memtable thresholds.....	144
Configuring compaction.....	144
Compression.....	145
When to compress data.....	145
Configuring compression.....	146
Testing compaction and compression.....	147
Tuning Bloom filters.....	147
Moving data to or from other databases.....	148
Purging gossip state on a node.....	148
Cassandra tools.....	149
The nodetool utility.....	149
assassinate.....	150
bootstrap.....	151
cfhistograms.....	152
cfstats.....	152
cleanup.....	152
clearsnapshot.....	153
compact.....	153
compactionhistory.....	155
compactionstats.....	157
decommission.....	157
describecluster.....	158
describing.....	159
disableautocompaction.....	160
disablebackup.....	161
disablebinary.....	161
disablegossip.....	162
disablehandoff.....	162
disablehintsfordc.....	162
disablethrift.....	163
drain.....	164
enableautocompaction.....	165
enablebackup.....	165
enablebinary.....	166
enablegossip.....	166
enablehandoff.....	167

enablehintsfordc.....	167
enablethrift.....	168
flush.....	169
gcstats.....	169
getcompactionthreshold.....	170
getcompactionthroughput.....	170
getendpoints.....	171
getlogginglevels.....	172
getsstables.....	173
getstreamthroughput.....	173
gettimeout.....	174
gettraceprobability.....	175
gossipinfo.....	175
help.....	176
info.....	177
invalidatecountercache.....	177
invalidatekeycache.....	178
invalidaterowcache.....	178
join.....	179
listsnapshots.....	179
move.....	180
netstats.....	181
pausehandoff.....	182
proxyhistograms.....	182
rangekeysample.....	183
rebuild.....	183
rebuild_index.....	184
refresh.....	185
refreshsizeestimates.....	185
reloadtriggers.....	186
relocatesstables.....	186
removenode.....	187
repair.....	188
replaybatchlog.....	191
resetlocalschema.....	191
resumehandoff.....	192
ring.....	193
scrub.....	194
setcachecapacity.....	194
setcachekeystosave.....	195
setcompactionthreshold.....	196
setcompactionthroughput.....	197
sethintedhandoffthrottlekb.....	197
setlogginglevel.....	198
setstreamthroughput.....	199
settimeout.....	199
settraceprobability.....	200
snapshot.....	201
status.....	204
statusbackup.....	205
statusbinary.....	205
statusgossip.....	206
statushandoff.....	206
statusthrift.....	207
stop.....	207
stopdaemon.....	208

tablehistograms.....	208
tablestats.....	210
toppartitions.....	214
tpstats.....	216
truncatehints.....	220
upgradesstables.....	221
verify.....	221
version.....	222
The cassandra utility.....	223
The cassandra-stress tool.....	225
Interpreting the output of cassandra-stress.....	233
SSTable utilities.....	235
sstabledump.....	235
sstableexpiredblockers.....	236
sstablekeys.....	236
sstablelevelreset.....	237
sstableloader (Cassandra bulk loader).....	237
sstablemetadata.....	240
sstableofflinerelevel.....	243
sstablerepairedset.....	243
sstablescrub.....	244
sstablesplit.....	245
sstableupgrade.....	245
sstableutil.....	246
sstableverify.....	246
 Troubleshooting.....	 246
 Release notes.....	 247

About Apache Cassandra

About this document

Welcome to the Cassandra documentation provided by DataStax. To ensure that you get the best experience in using this document, take a moment to look at the [Tips for using DataStax documentation](#).

The [landing pages](#) provide information about supported platforms, product compatibility, planning and testing cluster deployments, recommended production settings, troubleshooting, third-party software, resources for additional information, administrator and developer topics, and earlier documentation.

Overview of Apache Cassandra

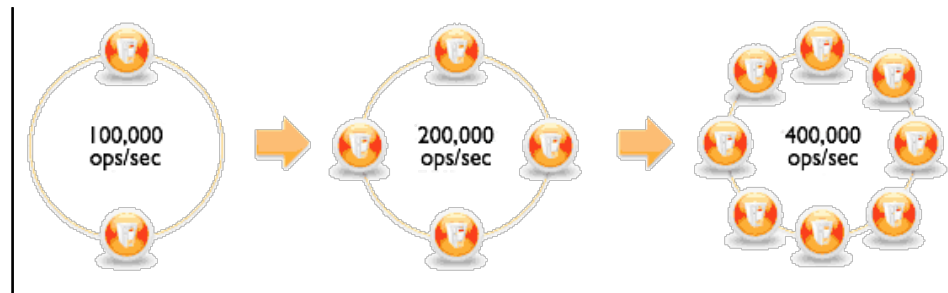
Apache Cassandra™ is a massively scalable open source NoSQL database. Cassandra is perfect for managing large amounts of structured, semi-structured, and unstructured data across multiple data centers and the cloud. Cassandra delivers continuous availability, linear scalability, and operational simplicity across many commodity servers with no single point of failure, along with a powerful dynamic data model designed for maximum flexibility and fast response times.

The latest version of DataStax Distribution of Apache Cassandra 3.x for Windows is 3.6.

How does Cassandra work?

Cassandra's built-for-scale architecture means that it is capable of handling petabytes of information and thousands of concurrent users/operations per second.

Cassandra is a partitioned row store database	Cassandra's architecture allows any authorized user to connect to any node in any data center and access data using the CQL language. For ease of use, CQL uses a similar syntax to SQL. The most basic way to interact with Cassandra is using the CQL shell, cqlsh . Using cqlsh , you can create keyspaces and tables, insert and query tables, plus much more. This Cassandra release works with CQL for Cassandra 2.2 and later . If you prefer a graphical tool, you can use DataStax DevCenter . For production, DataStax supplies a number drivers so that CQL statements can be passed from client to cluster and back.
Automatic data distribution	Cassandra provides automatic data distribution across all nodes that participate in a <i>ring</i> or database cluster. There is nothing programmatic that a developer or administrator needs to do or code to distribute data across a cluster because data is transparently partitioned across all nodes in a cluster.
Built-in and customizable replication	Cassandra also provides built-in and customizable replication, which stores redundant copies of data across nodes that participate in a Cassandra ring. This means that if any node in a cluster goes down, one or more copies of that node's data is available on other machines in the cluster. Replication can be configured to work across one data center, many data centers, and multiple cloud availability zones.
Cassandra supplies linear scalability	Cassandra supplies linear scalability, meaning that capacity may be easily added simply by adding new nodes online. For example, if 2 nodes can handle 100,000 transactions per second, 4 nodes will support 200,000 transactions/sec and 8 nodes will tackle 400,000 transactions/sec:



How is Cassandra different from relational databases?

Cassandra is designed from the ground up as a distributed database with peer-to-peer communication. As a best practice, queries should be one per table. Data is denormalized to make this possible. For this reason, the concept of JOINS between tables does not exist, although client-side joins can be used in applications.

What is NoSQL?

Most common translation is "Not only SQL", meaning a database that uses a method of storage different from a relational, or SQL, database. There are many different types of NoSQL databases, so a direct comparison of even the most used types is not useful. Database administrators today must be polyglot-friendly, meaning they must know how to work with many different RDBMS and NoSQL databases.

What is CQL?

[Cassandra Query Language \(CQL\)](#) is the primary interface into the Cassandra DBMS. Using CQL is similar to using SQL (Structured Query Language). CQL and SQL share the same abstract idea of a table constructed of columns and rows. The main difference from SQL is that Cassandra does not support joins or subqueries. Instead, Cassandra emphasizes denormalization through CQL features like collections and clustering specified at the schema level.

CQL is the recommended way to interact with Cassandra. Performance and the simplicity of reading and using CQL is an advantage of modern Cassandra over older Cassandra APIs.

The [CQL documentation](#) contains a [data modeling topic](#), examples, and command reference.

How do I interact with Cassandra?

The most basic way to interact with Cassandra is using the CQL shell, `cqlsh`. [Using cqlsh](#), you can create keyspaces and tables, insert and query tables, plus much more. If you prefer a graphical tool, you can use [DevCenter](#). For production, DataStax supplies a number of [drivers](#) in various programming languages, so that CQL statements can be passed from client to cluster and back.

How can I move data to/from Cassandra?

Data is inserted using the CQL INSERT command, the CQL COPY command and CSV files, or [sstableloader](#). But in reality, you need to consider how your client application will query the tables, and do data modeling first. The paradigm shift between relational and NoSQL means that a straight move of data from an RDBMS database to Cassandra will be doomed to failure.

What other tools come with Cassandra?

Cassandra automatically installs [nodetool](#), a useful command-line management tool for Cassandra. A tool for load-stressing and basic benchmarking, [cassandra-stress](#), is also installed by default.

What kind of hardware/cloud environment do I need to run Cassandra?

Cassandra is designed to run on [commodity hardware](#) with common specifications. In the [cloud](#), Cassandra is adapted for most common offerings.

What's new in DataStax Distribution of Apache Cassandra 3.x for Windows

Note: Cassandra is now releasing on a tick-tock schedule. For more information, see [Cassandra 2.2, 3.0, and beyond](#).

The latest version of DataStax Distribution of Apache Cassandra 3.x for Windows is 3.6.

The [CHANGES.txt](#) describes the changes in detail. You can view all version changes by branch or tag in the drop-down list on the changes page.

New features in Cassandra 3.2 and later

-graph option for cassandra-stress	cassandra-stress results can be automatically graphed for data visualization.
TTL for COPY FROM	A TTL value can be specified when copying from CSV files.
bulkloader can use third party authentication	The bulkloader has an option <code>-ap</code> for third party authentication.
CREATE TABLE WITH ID	If a table is accidentally dropped, it can be recreated with its ID and the commitlog replayed to regain data.
jvm.options file for GC and some JVM options	Some JVM options have been moved from the cassandra-env.sh file into a new file, jvm.options. The cassandra utility on page 223.
Static columns can be indexed	In Cassandra 3.4 and later, static columns can be indexed.
New option for nodetool compact	In Cassandra 3.4 and later, addition of <code>--user-defined</code> to <code>nodetool compact</code> to allow user to submit a list of files compact . Handy for dealing with low disk space or tombstone purging.
nodetool gettimeout and nodetool settimeout	In Cassandra 3.4 and later, two nodetool commands, nodetool gettimeout and nodetool settimeout to print out or set the value of a timeout in milliseconds.
SSTable Attached Secondary Indexes (SASI)	In Cassandra 3.4 and later, SSTable Attached Secondary Indexes (SASI) have been introduced that improve on the existing secondary index implementation with superior performance for queries that previously required the use of <code>ALLOW FILTERING</code>

New features released in Cassandra 3.0

Storage engine refactored	The Storage Engine has been refactored.
Materialized Views	Materialized views handle automated server-side denormalization, with consistency between base and view data.
Support for Windows	Support for Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012. See DataStax Cassandra 3.0 Windows Documentation .
Operations improvements	
Addition of MAX_WINDOW_SIZE_SECONDS to DTCS compaction settings	Allow DTCS compaction governance based on maximum window size rather than Table age.
File-based Hint Storage and Improved Replay	Hints are now stored in files and replay is improved.
Default garbage collector is changed to G1	Default garbage collector is changed from Concurrent-Mark-Sweep (CMS) to G1. G1 performance is better for nodes with heap size of 4GB or greater.
Changed syntax for CREATE TABLE compression options	Made the compression options more consistent for <code>CREATE TABLE</code> .
Add nodetool command to force blocking batchlog replay	BatchlogManager can force batchlog replay using nodetool.
Nodetool over SSL	Nodetool can connect using SSL like <code>cqlsh</code> .
New nodetool options for hinted handoffs	Nodetool options <code>disablehintsfordc</code> and <code>enablehintsfordc</code> added. to selectively disable or enable hinted handoffs for a data center.
nodetool stop	Nodetool option added to stop compactions.
Other notable changes	
Requires Java 8	Java 8 is now required.
nodetool cfstats and nodetool cfhistograms renamed	Renamed <code>nodetool cfstats</code> to <code>nodetool tablestats</code> . Renamed <code>nodetool cfhistograms</code> to <code>nodetool tablehistograms</code> .
Native protocol v1 and v2 are dropped	Native protocol v1 and v2 are dropped in Cassandra 3.0.
DataStax AMI does not install Cassandra 3.0 or 3.x	You can install Cassandra 2.1 and earlier versions on Amazon EC2 using the DataStax AMI (Amazon Machine Image) as described in the AMI documentation for Cassandra 2.1.

To install Cassandra 3.0 and later on Amazon EC2, use a [trusted AMI](#) for your platform and the appropriate [install method](#) for that platform.

Understanding the architecture

Architecture in brief

Cassandra is designed to handle big data workloads across multiple nodes with no single point of failure. Its architecture is based on the understanding that system and hardware failures can and do occur. Cassandra addresses the problem of failures by employing a peer-to-peer distributed system across homogeneous nodes where data is distributed among all nodes in the cluster. Each node frequently exchanges state information about itself and other nodes across the cluster using peer-to-peer [gossip](#) communication protocol. A sequentially written [commit log](#) on each node captures write activity to ensure data durability. Data is then indexed and written to an in-memory structure, called a [memtable](#), which resembles a write-back cache. Each time the memory structure is full, the data is written to disk in an [SSTables](#) data file. All writes are automatically partitioned and replicated throughout the cluster. Cassandra periodically consolidates SSTables using a process called [compaction](#), discarding obsolete data marked for deletion with a [tombstone](#). To ensure all data across the cluster stays consistent, various [repair](#) mechanisms are employed.

Cassandra is a partitioned row store database, where rows are organized into tables with a required primary key. Cassandra's architecture allows any [authorized user](#) to connect to any node in any data center and access data using the CQL language. For ease of use, CQL uses a similar syntax to SQL and works with table data. Developers can access CQL through [cqlsh](#), [DevCenter](#), and via [drivers](#) for application languages. Typically, a cluster has one [keyspace](#) per application composed of many different tables.

Client read or write requests can be sent to any node in the cluster. When a client connects to a node with a request, that node serves as the [coordinator](#) for that particular client operation. The coordinator acts as a proxy between the client application and the nodes that own the data being requested. The coordinator determines which nodes in the ring should get the request based on how the cluster is configured.

Key structures

- Node

Where you store your data. It is the basic infrastructure component of Cassandra.

- Data center

A collection of related nodes. A data center can be a physical data center or virtual data center. Different workloads should use separate data centers, either physical or virtual. Replication is set by data center. Using separate data centers prevents Cassandra transactions from being impacted by other workloads and keeps requests close to each other for lower latency. Depending on the replication factor, data can be written to multiple data centers. Data centers must never span physical locations.

- Cluster

A cluster contains one or more data centers. It can span physical locations.

- Commit log

All data is written first to the commit log for durability. After all its data has been flushed to SSTables, it can be archived, deleted, or recycled.

- SSTable

A sorted string table (SSTable) is an immutable data file to which Cassandra writes memtables periodically. SSTables are append only and stored on disk sequentially and maintained for each Cassandra table.

- CQL Table

A collection of ordered columns fetched by table row. A table consists of columns and has a primary key.

Key components for configuring Cassandra

- [Gossip](#)

A peer-to-peer communication protocol to discover and share location and state information about the other nodes in a Cassandra cluster. Gossip information is also persisted locally by each node to use immediately when a node restarts.

- [Partitioner](#)

A partitioner determines which node will receive the first replica of a piece of data, and how to distribute other replicas across other nodes in the cluster. Each row of data is uniquely identified by a primary key, which may be the same as its partition key, but which may also include other clustering columns. A partitioner is a hash function that derives a token from the primary key of a row. The partitioner uses the token value to determine which nodes in the cluster receive the replicas of that row. The [Murmur3Partitioner](#) is the default partitioning strategy for new Cassandra clusters and the right choice for new clusters in almost all cases.

You must set the partitioner and assign the node a [num_tokens](#) value for each node. The number of tokens you assign depends on the [hardware capabilities](#) of the system. If not using virtual nodes (vnodes), use the [initial_token](#) setting instead.

- [Replication factor](#)

The total number of replicas across the cluster. A replication factor of 1 means that there is only one copy of each row on one node. A replication factor of 2 means two copies of each row, where each copy is on a different node. All replicas are equally important; there is no primary or master replica. You define the replication factor for each data center. Generally you should set the replication strategy greater than one, but no more than the number of nodes in the cluster.

- [Replica placement strategy](#)

Cassandra stores copies (replicas) of data on multiple nodes to ensure reliability and fault tolerance. A replication strategy determines which nodes to place replicas on. The first replica of data is simply the first copy; it is not unique in any sense. The [NetworkTopologyStrategy](#) is highly recommended for most deployments because it is much easier to expand to multiple data centers when required by future expansion.

When creating a keyspace, you must define the replica placement strategy and the number of replicas you want.

- [Snitch](#)

A snitch defines groups of machines into data centers and racks (the topology) that the replication strategy uses to place replicas.

You must configure a [snitch](#) when you create a cluster. All snitches use a dynamic snitch layer, which monitors performance and chooses the best replica for reading. It is enabled by default and recommended for use in most deployments. Configure dynamic snitch thresholds for each node in the `cassandra.yaml` configuration file.

The default [SimpleSnitch](#) does not recognize data center or rack information. Use it for single-data center deployments or single-zone in public clouds. The [GossipingPropertyFileSnitch](#) is recommended for production. It defines a node's data center and rack and uses [gossip](#) for propagating this information to other nodes.

- [The `cassandra.yaml` configuration file](#)

The main configuration file for setting the initialization properties for a cluster, caching parameters for tables, properties for tuning and resource utilization, timeout settings, client connections, backups, and security.

By default, a node is configured to store the data it manages in a directory set in the `cassandra.yaml` file.

In a production cluster deployment, you can change the `commitlog-directory` to a different disk drive from the `data_file_directories`.

- [System keyspace table properties](#)

You set storage configuration attributes on a per-keyspace or per-table basis programmatically or using a client application, such as CQL.

Related reference

[cassandra.yaml configuration file](#) on page 63

[Installation locations](#) on page 61

Internode communications (gossip)

Gossip is a peer-to-peer communication protocol in which nodes periodically exchange state information about themselves and about other nodes they know about. The gossip process runs every second and exchanges state messages with up to three other nodes in the cluster. The nodes exchange information about themselves and about the other nodes that they have gossiped about, so all nodes quickly learn about all other nodes in the cluster. A gossip message has a version associated with it, so that during a gossip exchange, older information is overwritten with the most current state for a particular node.

To prevent problems in gossip communications, use the same list of seed nodes for all nodes in a cluster. This is most critical the first time a node starts up. By default, a node remembers other nodes it has gossiped with between subsequent restarts. The seed node designation has no purpose other than bootstrapping the gossip process for new nodes joining the cluster. Seed nodes are *not* a single point of failure, nor do they have any other special purpose in cluster operations beyond the bootstrapping of nodes.

Attention: In multiple data-center clusters, it is a good idea to include at least one node from each data center (replication group) in the seed list. Designating 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 it is recommended to use a small seed list (approximately three nodes per data center).

Failure detection and recovery

Failure detection is a method for locally determining from gossip state and history if another node in the system is down or has come back up. Cassandra uses this information to avoid routing client requests to unreachable nodes whenever possible. (Cassandra can also avoid routing requests to nodes that are alive, but performing poorly, through the [dynamic snitch](#).)

The gossip process tracks state from other nodes both directly (nodes gossiping directly to it) and indirectly (nodes communicated about secondhand, third-hand, and so on). Rather than have a fixed threshold for marking failing nodes, Cassandra uses an accrual detection mechanism to calculate a per-node threshold that takes into account network performance, workload, and historical conditions. During gossip exchanges, every node maintains a sliding window of inter-arrival times of gossip messages from other nodes in the cluster. Configuring the `phi_convict_threshold` property adjusts the sensitivity of the failure detector. Lower values increase the likelihood that an unresponsive node will be marked as down, while higher values decrease the likelihood that transient failures causing node failure. Use the default value

Understanding the architecture

for most situations, but increase it to 10 or 12 for Amazon EC2 (due to frequently encountered network congestion). In unstable network environments (such as EC2 at times), raising the value to 10 or 12 helps prevent false failures. Values higher than 12 and lower than 5 are not recommended.

Node failures can result from various causes such as hardware failures and network outages. Node outages are often transient but can last for extended periods. Because a node outage rarely signifies a permanent departure from the cluster it does not automatically result in permanent removal of the node from the ring. Other nodes will periodically try to re-establish contact with failed nodes to see if they are back up. To permanently change a node's membership in a cluster, administrators must explicitly add or remove nodes from a Cassandra cluster using the [nodetool utility](#).

When a node comes back online after an outage, it may have missed writes for the replica data it maintains. [Repair mechanisms](#) exist to recover missed data, such as hinted handoffs and manual repair with [nodetool repair](#). The length of the outage will determine which repair mechanism is used to make the data consistent.

Data distribution and replication

In Cassandra, data distribution and replication go together. Data is organized by table and identified by a primary key, which determines which node the data is stored on. Replicas are copies of rows. When data is first written, it is also referred to as a replica.

Factors influencing replication include:

- [Virtual nodes](#): assigns data ownership to physical machines.
- [Partitioner](#): partitions the data across the cluster.
- [Replication strategy](#): determines the replicas for each row of data.
- [Snitch](#): defines the topology information that the replication strategy uses to place replicas.

Consistent hashing

Consistent hashing allows distribution of data across a cluster to minimize reorganization when nodes are added or removed. Consistent hashing partitions data based on the partition key. (For an explanation of partition keys and primary keys, see the [Data modeling example](#) in *CQL for Cassandra 2.2 and later*.)

For example, if you have the following data:

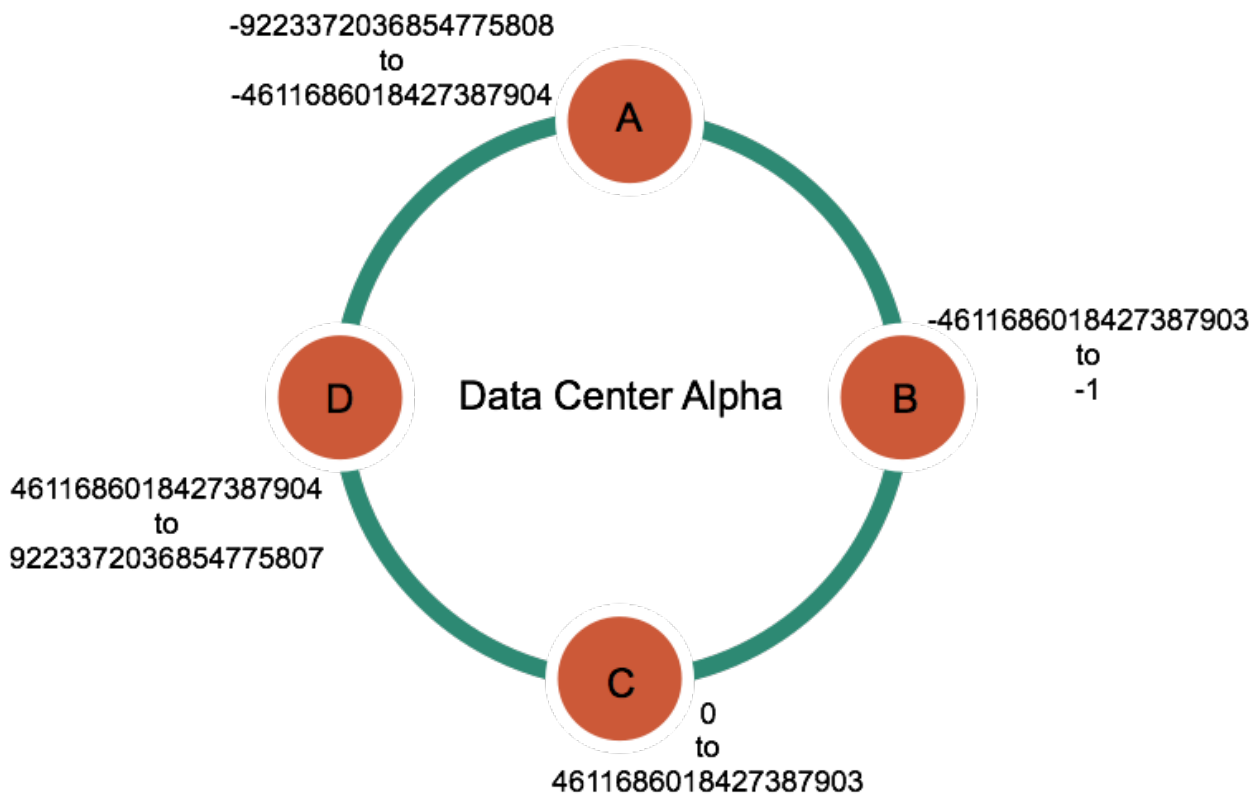
name	age	car	gender
jim	36	camaro	M
carol	37	bmw	F
johnny	12		M
suzy	10		F

Cassandra assigns a hash value to each partition key:

Partition key	Murmur3 hash value
jim	-2245462676723223822
carol	7723358927203680754
johnny	-6723372854036780875
suzy	1168604627387940318

Each node in the cluster is responsible for a range of data based on the hash value.

Figure: Hash values in a four node cluster



Cassandra places the data on each node according to the value of the partition key and the range that the node is responsible for. For example, in a four node cluster, the data in this example is distributed as follows:

Node	Start range	End range	Partition key	Hash value
A	-9223372036854775808	-4611686018427387904	johnny	-6723372854036780875
B	-4611686018427387903	-1	jim	-2245462676723223822
C	0	4611686018427387903	suzy	1168604627387940318
D	4611686018427387904	9223372036854775807	carol	7723358927203680754

Virtual nodes

Virtual nodes, known as Vnodes, distribute data across nodes at a finer granularity than can be easily achieved if calculated tokens are used. Vnodes simplify many tasks in Cassandra:

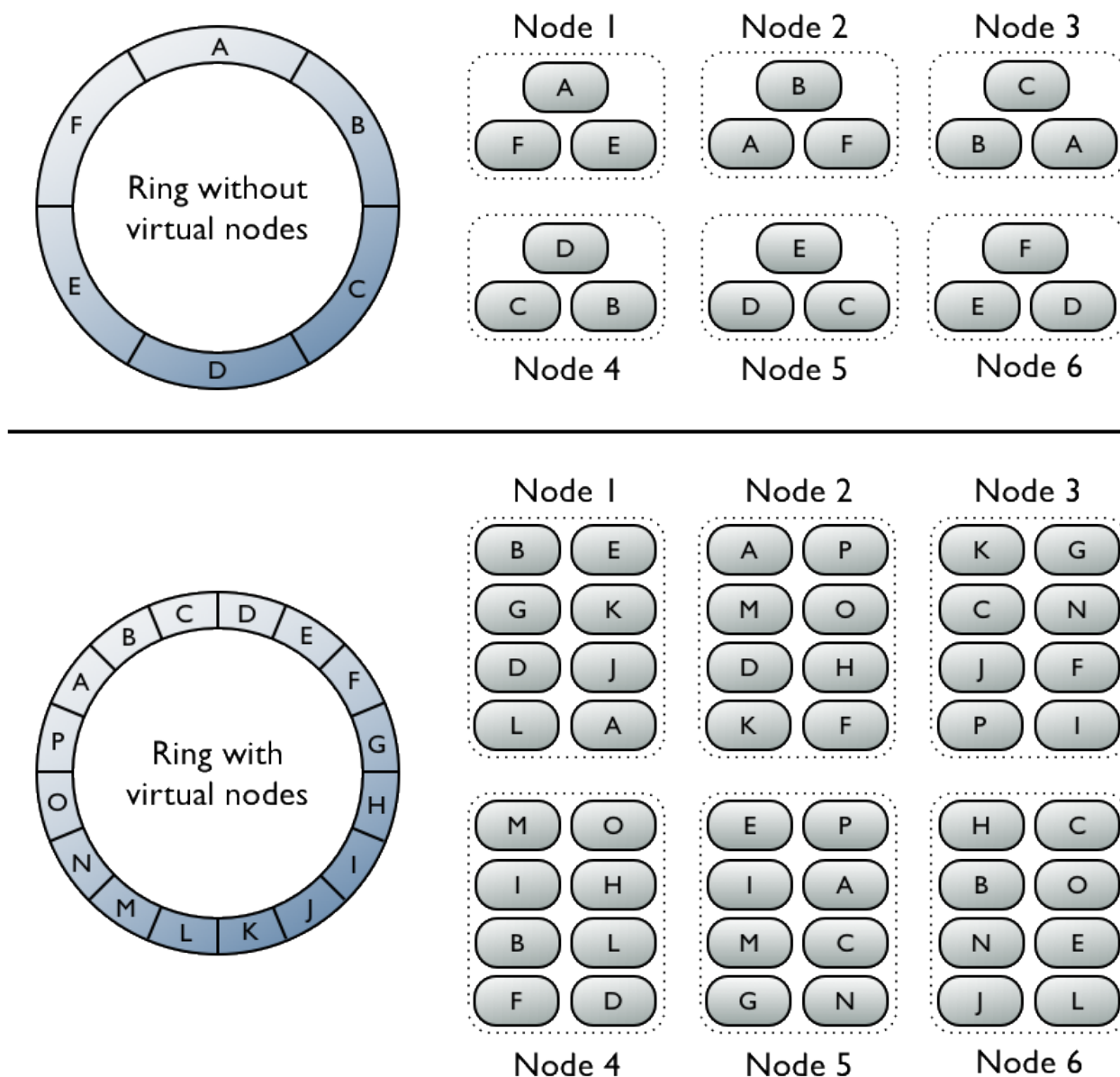
- Tokens are automatically calculated and assigned to each node.
- Rebalancing a cluster is automatically accomplished when adding or removing nodes. When a node joins the cluster, it assumes responsibility for an even portion of data from the other nodes in the cluster. If a node fails, the load is spread evenly across other nodes in the cluster.
- Rebuilding a dead node is faster because it involves every other node in the cluster.
- The proportion of vnodes assigned to each machine in a cluster can be assigned, so smaller and larger computers can be used in building a cluster.

For more information, see the article [Virtual nodes in Cassandra 1.2](#). To convert an existing cluster to vnodes, see [Enabling virtual nodes on an existing production cluster](#) on page 94.

How data is distributed across a cluster (using virtual nodes)

Prior to Cassandra 1.2, you had to calculate and assign a single [token](#) to each node in a cluster. Each token determined the node's position in the ring and its portion of data according to its hash value. In Cassandra 1.2 and later, each node is allowed many tokens. The new paradigm is called virtual nodes (vnodes). Vnodes allow each node to own a large number of small [partition ranges](#) distributed throughout the cluster. Vnodes also use consistent hashing to distribute data but using them doesn't require token generation and assignment.

Figure: Virtual vs single-token architecture



The top portion of the graphic shows a cluster without vnodes. In this paradigm, each node is assigned a single token that represents a location in the ring. Each node stores data determined by mapping the [partition key](#) to a token value within a range from the previous node to its assigned value. Each node also contains copies of each row from other nodes in the cluster. For example, if the replication factor is 3,

range E replicates to nodes 5, 6, and 1. Notice that a node owns exactly one contiguous partition range in the ring space.

The bottom portion of the graphic shows a ring with vnodes. Within a cluster, virtual nodes are randomly selected and non-contiguous. The placement of a row is determined by the hash of the partition key within many smaller partition ranges belonging to each node.

Data replication

Cassandra stores replicas on multiple nodes to ensure reliability and fault tolerance. A replication strategy determines the nodes where replicas are placed. The total number of replicas across the cluster is referred to as the replication factor. A replication factor of 1 means that there is only one copy of each row in the cluster. If the node containing the row goes down, the row cannot be retrieved. A replication factor of 2 means two copies of each row, where each copy is on a different node. All replicas are equally important; there is no primary or master replica. As a general rule, the replication factor should not exceed the number of nodes in the cluster. However, you can increase the replication factor and then add the desired number of nodes later.

Two replication strategies are available:

- `SimpleStrategy`: Use only for a single [data center](#) and one rack. If you ever intend more than one data center, use the `NetworkTopologyStrategy`.
- `NetworkTopologyStrategy`: Highly recommended for most deployments because it is much easier to expand to multiple data centers when required by future expansion.

SimpleStrategy

Use only for a single data center and one rack. `SimpleStrategy` places the first replica on a node determined by the partitioner. Additional replicas are placed on the next nodes clockwise in the ring without considering topology (rack or data center location).

NetworkTopologyStrategy

Use `NetworkTopologyStrategy` when you have (or plan to have) your cluster deployed across multiple data centers. This strategy specifies how many replicas you want in each data center.

`NetworkTopologyStrategy` places replicas in the same data center by walking the ring clockwise until reaching the first node in another rack. `NetworkTopologyStrategy` attempts to place replicas on distinct racks because nodes in the same rack (or similar physical grouping) often fail at the same time due to power, cooling, or network issues.

When deciding how many replicas to configure in each data center, the two primary considerations are (1) being able to satisfy reads locally, without incurring cross data-center latency, and (2) failure scenarios. The two most common ways to configure multiple data center clusters are:

- Two replicas in each data center: This configuration tolerates the failure of a single node per replication group and still allows local reads at a consistency level of `ONE`.
- Three replicas in each data center: This configuration tolerates either the failure of one node per replication group at a strong consistency level of `LOCAL_QUORUM` or multiple node failures per data center using consistency level `ONE`.

Asymmetrical replication groupings are also possible. For example, you can have three replicas in one data center to serve real-time application requests and use a single replica elsewhere for running analytics.

Replication strategy is defined per keyspace, and is set during keyspace creation. To set up a keyspace, see [creating a keyspace](#).

For more about replication strategy options, see [Changing keyspace replication strategy](#) on page 116.

Partitioners

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.

Both the `Murmur3Partitioner` and `RandomPartitioner` use tokens to help assign equal portions of data to each node and evenly distribute data from all the tables throughout the ring or other grouping, such as a keyspace. This is true even if the tables use different [partition keys](#), such as usernames or timestamps. Moreover, the read and write requests to the cluster are also evenly distributed and load balancing is simplified because each part of the hash range receives an equal number of rows on average. For more detailed information, see [Consistent hashing](#) on page 14.

The main difference between the two partitioners is how each generates the token hash values. The `RandomPartitioner` uses a cryptographic hash that takes longer to generate than the `Murmur3Partitioner`. Cassandra doesn't really need a cryptographic hash, so using the `Murmur3Partitioner` results in a 3-5 times improvement in performance.

Cassandra offers the following partitioners that can be set in the [cassandra.yaml](#) file.

- `Murmur3Partitioner` (default): uniformly distributes data across the cluster based on `MurmurHash` hash values.
- `RandomPartitioner`: uniformly distributes data across the cluster based on MD5 hash values.
- `ByteOrderedPartitioner`: keeps an ordered distribution of data lexically by key bytes

The `Murmur3Partitioner` is the default partitioning strategy for Cassandra 1.2 and later new clusters and the right choice for new clusters in almost all cases. However, the partitioners are not compatible and data partitioned with one partitioner cannot be easily converted to the other partitioner.

Note: If using virtual nodes (vnodes), you do **not** need to calculate the tokens. If not using vnodes, you **must** calculate the tokens to assign to the [initial_token](#) parameter in the `cassandra.yaml` file. See [Generating tokens](#) on page 100 and use the method for the type of partitioner you are using.

Related reference

[Installation locations](#) on page 61

Murmur3Partitioner

The `Murmur3Partitioner` is the default partitioner. The `Murmur3Partitioner` provides faster hashing and improved performance than the `RandomPartitioner`. The `Murmur3Partitioner` can be used with vnodes. However, if you don't use vnodes, you must calculate the tokens, as described in [Generating tokens](#).

Use `Murmur3Partitioner` for new clusters; you cannot change the partitioner in existing clusters that use a different partitioner. The `Murmur3Partitioner` uses the `MurmurHash` function. This hashing function creates a 64-bit hash value of the partition key. The possible range of hash values is from -2^{63} to $+2^{63}-1$.

When using the `Murmur3Partitioner`, you can page through all rows using the [token function](#) in a CQL query.

RandomPartitioner

The `RandomPartitioner` was the default partitioner prior to Cassandra 1.2. It is included for backwards compatibility. The `RandomPartitioner` can be used with virtual nodes (vnodes). However, if you don't use vnodes, you must calculate the tokens, as described in [Generating tokens](#). The `RandomPartitioner` distributes data evenly across the nodes using an MD5 hash value of the row key. The possible range of hash values is from 0 to $2^{127}-1$.

When using the `RandomPartitioner`, you can page through all rows using the [token function](#) in a CQL query.

ByteOrderedPartitioner

Cassandra provides the `ByteOrderedPartitioner` for ordered partitioning. It is included for backwards compatibility. This partitioner orders rows lexically by key bytes. You calculate tokens by looking at the actual values of your partition key data and using a hexadecimal representation of the leading character(s) in a key. For example, if you wanted to partition rows alphabetically, you could assign an A token using its hexadecimal representation of 41.

Using the ordered partitioner allows ordered scans by primary key. This means you can scan rows as though you were moving a cursor through a traditional index. For example, if your application has user names as the partition key, you can scan rows for users whose names fall between Jake and Joe. This type of query is not possible using randomly partitioned partition keys because the keys are stored in the order of their MD5 hash (not sequentially).

Although having the capability to do range scans on rows sounds like a desirable feature of ordered partitioners, there are ways to achieve the same functionality using [table indexes](#).

Using an ordered partitioner is not recommended for the following reasons:

Difficult load balancing

More administrative overhead is required to load balance the cluster. An ordered partitioner requires administrators to manually calculate [partition ranges](#) based on their estimates of the partition key distribution. In practice, this requires actively moving node tokens around to accommodate the actual distribution of data once it is loaded.

Sequential writes can cause hot spots

If your application tends to write or update a sequential block of rows at a time, then the writes are not be distributed across the cluster; they all go to one node. This is frequently a problem for applications dealing with timestamped data.

Uneven load balancing for multiple tables

If your application has multiple tables, chances are that those tables have different row keys and different distributions of data. An ordered partitioner that is balanced for one table may cause hot spots and uneven distribution for another table in the same cluster.

Snitches

A snitch determines which data centers and racks nodes belong to. They inform Cassandra about the network topology so that requests are routed efficiently and allows 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. All nodes must return to the same rack and data center. Cassandra does its best not to have more than one replica on the same rack (which is not necessarily a physical location).

Note: If you change snitches, you may need to perform additional steps because the snitch affects where replicas are placed. See [Switching snitches](#) on page 114.

Dynamic snitching

By default, all snitches also use a dynamic snitch layer that monitors read latency and, when possible, routes requests away from poorly-performing nodes. The dynamic snitch is enabled by default and is recommended for use in most deployments. For information on how this works, see [Dynamic snitching in Cassandra: past, present, and future](#). Configure dynamic snitch thresholds for each node in the `cassandra.yaml` configuration file.

For more information, see the properties listed under [Failure detection and recovery](#) on page 13.

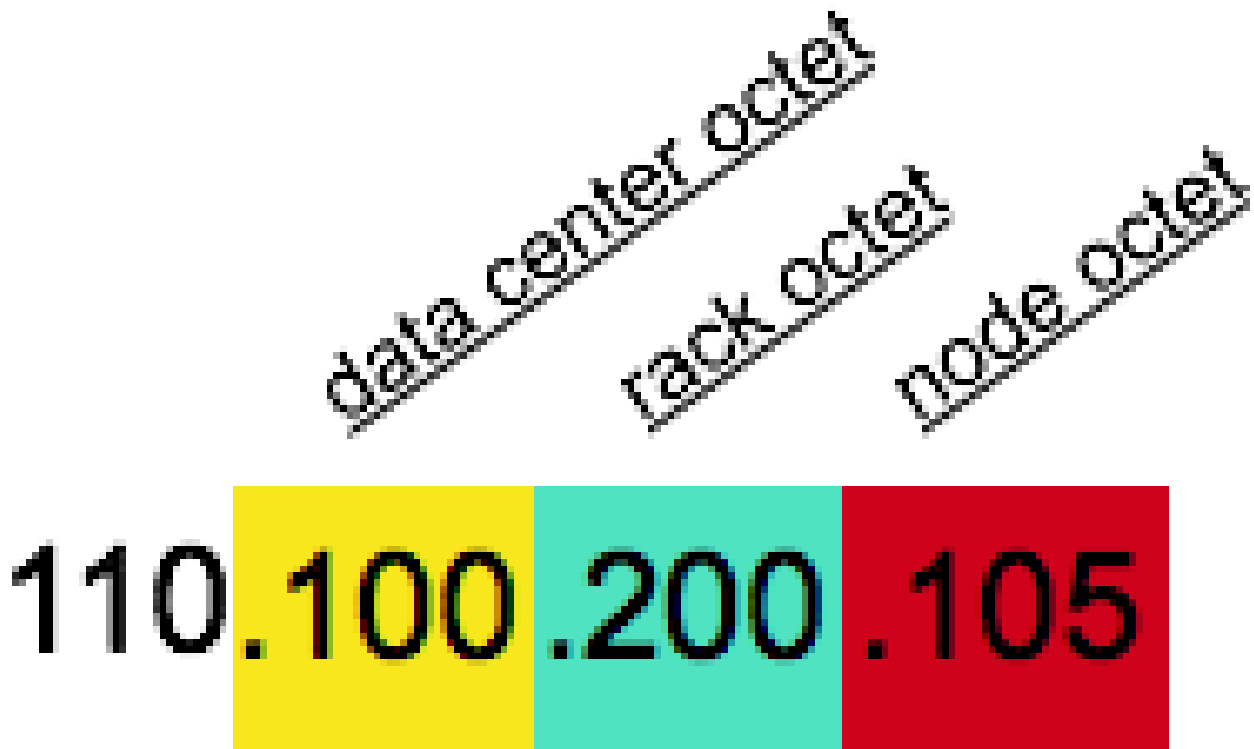
SimpleSnitch

The SimpleSnitch (default) is used only for single-data center deployments. It does not recognize data center or rack information and can be used only for single-data center deployments or single-zone in public clouds. It treats strategy order as proximity, which can improve cache locality when disabling read repair.

Using a SimpleSnitch, you [define the keyspace](#) to use SimpleStrategy and specify a replication factor.

RackInferringSnitch

The RackInferringSnitch determines the proximity of nodes by rack and data center, which are assumed to correspond to the 3rd and 2nd octet of the node's IP address, respectively. This snitch is best used as an example for writing a custom snitch class (unless this happens to match your deployment conventions).



PropertyFileSnitch

This snitch determines proximity as determined by rack and data center. It uses the network details located in the `cassandra-topology.properties` file. When using this snitch, you can define your data center names to be whatever you want. Make sure that the data center names correlate to the name of your data centers in the [keyspace definition](#). Every node in the cluster should be described in the `cassandra-topology.properties` file, and this file should be exactly the same on every node in the cluster.

Procedure

If you had non-uniform IPs and two physical data centers with two racks in each, and a third logical data center for replicating analytics data, the `cassandra-topology.properties` file might look like this:

Note: Data center and rack names are case-sensitive.

```
# Data Center One

175.56.12.105=DC1:RAC1
175.50.13.200=DC1:RAC1
175.54.35.197=DC1:RAC1

120.53.24.101=DC1:RAC2
120.55.16.200=DC1:RAC2
120.57.102.103=DC1:RAC2

# Data Center Two

110.56.12.120=DC2:RAC1
110.50.13.201=DC2:RAC1
110.54.35.184=DC2:RAC1

50.33.23.120=DC2:RAC2
50.45.14.220=DC2:RAC2
50.17.10.203=DC2:RAC2

# Analytics Replication Group

172.106.12.120=DC3:RAC1
172.106.12.121=DC3:RAC1
172.106.12.122=DC3:RAC1

# default for unknown nodes
default =DC3:RAC1
```

GossipingPropertyFileSnitch

This snitch is recommended for production. It uses rack and data center information for the local node defined in the `cassandra-rackdc.properties` file and propagates this information to other nodes via gossip.

The configuration for the `GossipingPropertyFileSnitch` is contained in the `cassandra-rackdc.properties` file.

To configure a node to use `GossipingPropertyFileSnitch`, edit the `cassandra-rackdc.properties` file as follows:

- Define the Data Center and Rack that include this node. The default settings:

```
dc=DC1
rack=RAC1
```

Note: Data center and rack names are case-sensitive.

- To save bandwidth, add the `prefer_local=true` option. This option tells Cassandra to use the local IP address when communication is not across different data centers.

Migrating from the `PropertyFileSnitch` to the `GossipingPropertyFileSnitch`

To allow migration from the `PropertyFileSnitch`, the `GossipingPropertyFileSnitch` uses the `cassandra-topology.properties` file when present. Delete the file after the migration is complete. For more information about migration, see [Switching snitches](#) on page 114.

Note: The `GossipingPropertyFileSnitch` always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the `PropertyFileSnitch`.

Ec2Snitch

Use the Ec2Snitch for simple cluster deployments on Amazon EC2 where all nodes in the cluster are within a single region.

In EC2 deployments, the region name is treated as the data center name and availability zones are treated as racks within a data center. For example, if a node is in the us-east-1 region, us-east is the data center name and 1 is the rack location. (Racks are important for distributing replicas, but not for data center naming.) Because private IPs are used, this snitch does not work across multiple regions.

If you are using only a single data center, you do not need to specify any properties.

If you need multiple data centers, set the `dc_suffix` options in the `cassandra-rackdc.properties` file. Any other lines are ignored.

For example, for each node within the us-east region, specify the data center in its `cassandra-rackdc.properties` file:

Note: Data center names are case-sensitive.

- **node0**
`dc_suffix=_1_cassandra`
- **node1**
`dc_suffix=_1_cassandra`
- **node2**
`dc_suffix=_1_cassandra`
- **node3**
`dc_suffix=_1_cassandra`
- **node4**
`dc_suffix=_1_analytics`
- **node5**
`dc_suffix=_1_search`

This results in three data centers for the region:

```
us-east_1_cassandra
us-east_1_analytics
us-east_1_search
```

Note: The data center naming convention in this example is based on the workload. You can use other conventions, such as DC1, DC2 or 100, 200.

Keyspace strategy options

When defining your [keyspace strategy options](#), use the EC2 region name, such as ``us-east``, as your data center name.

Ec2MultiRegionSnitch

Use the Ec2MultiRegionSnitch for deployments on Amazon EC2 where the cluster spans multiple regions.

You must configure settings in both the `cassandra.yaml` file and the property file (`cassandra-rackdc.properties`) used by the Ec2MultiRegionSnitch.

Configuring cassandra.yaml for cross-region communication

The Ec2MultiRegionSnitch uses public IP designated in the broadcast_address to allow cross-region connectivity. Configure each node as follows:

1. In the cassandra.yaml, set the listen_address to the private IP address of the node, and the broadcast_address to the public IP address of the node.

This allows Cassandra nodes in one EC2 region to bind to nodes in another region, thus enabling multiple data center support. For intra-region traffic, Cassandra switches to the private IP after establishing a connection.

2. Set the addresses of the seed nodes in the cassandra.yaml file to that of the public IP. Private IP are not routable between networks. For example:

```
seeds: 50.34.16.33, 60.247.70.52
```

To find the public IP address, from each of the seed nodes in EC2:

```
$ curl http://instance-data/latest/meta-data/public-ipv4
```

Note: Do not make all nodes seeds, see [Internode communications \(gossip\)](#) on page 13.

3. Be sure that the storage_port or ssl_storage_port is open on the public IP firewall.

Configuring the snitch for cross-region communication

In EC2 deployments, the region name is treated as the data center name and availability zones are treated as racks within a data center. For example, if a node is in the us-east-1 region, us-east is the data center name and 1 is the rack location. (Racks are important for distributing replicas, but not for data center naming.)

For each node, specify its data center in the cassandra-rackdc.properties. The dc_suffix option defines the data centers used by the snitch. Any other lines are ignored.

In the example below, there are two cassandra data centers and each data center is named for its workload. The data center naming convention in this example is based on the workload. You can use other conventions, such as DC1, DC2 or 100, 200. (Data center names are case-sensitive.)

Region: us-east	Region: us-west
Node and data center: <ul style="list-style-type: none">• node0 dc_suffix=_1_cassandra• node1 dc_suffix=_1_cassandra• node2 dc_suffix=_2_cassandra• node3 dc_suffix=_2_cassandra• node4 dc_suffix=_1_analytics• node5 dc_suffix=_1_search This results in four us-east data centers:	Node and data center: <ul style="list-style-type: none">• node0 dc_suffix=_1_cassandra• node1 dc_suffix=_1_cassandra• node2 dc_suffix=_2_cassandra• node3 dc_suffix=_2_cassandra• node4 dc_suffix=_1_analytics• node5 dc_suffix=_1_search This results in four us-west data centers:
us-east_1_cassandra	us-west_1_cassandra

Region: us-east	Region: us-west
us-east_2_cassandra us-east_1_analytics us-east_1_search	us-west_2_cassandra us-west_1_analytics us-west_1_search

Keyspace strategy options

When defining your [keyspace strategy options](#), use the EC2 region name, such as ``us-east``, as your data center name.

Related reference

[Installation locations](#) on page 61

GoogleCloudSnitch

Use the GoogleCloudSnitch for Cassandra deployments on [Google Cloud Platform](#) across one or more regions. The region is treated as a data center and the availability zones are treated as racks within the data center. All communication occurs over private IP addresses within the same logical network.

The region name is treated as the data center name and zones are treated as racks within a data center. For example, if a node is in the us-central1-a region, us-central1 is the data center name and a is the rack location. (Racks are important for distributing replicas, but not for data center naming.) This snitch can work across multiple regions without additional configuration.

If you are using only a single data center, you do not need to specify any properties.

If you need multiple data centers, set the `dc_suffix` options in the `cassandra-rackdc.properties` file. Any other lines are ignored.

For example, for each node within the us-central1 region, specify the data center in its `cassandra-rackdc.properties` file:

Note: Data center names are case-sensitive.

- **node0**
`dc_suffix=_a_cassandra`
- **node1**
`dc_suffix=_a_cassandra`
- **node2**
`dc_suffix=_a_cassandra`
- **node3**
`dc_suffix=_a_cassandra`
- **node4**
`dc_suffix=_a_analytics`
- **node5**
`dc_suffix=_a_search`

Note: Data center and rack names are case-sensitive.

CloudstackSnitch

Use the CloudstackSnitch for [Apache Cloudstack](#) environments. Because zone naming is free-form in Apache Cloudstack, this snitch uses the widely-used <country> <location> <az> notation.

Database internals

Storage engine

Cassandra uses a storage structure similar to a [Log-Structured Merge Tree](#), unlike a typical relational database that uses a [B-Tree](#). Cassandra avoids reading before writing. Read-before-write, especially in a large distributed system, can result in large latencies in read performance and other problems. For example, two clients read at the same time; one overwrites the row to make update A, and the other overwrites the row to make update B, removing update A. This race condition will result in ambiguous query results - which update is correct?

To avoid using read-before-write for most writes in Cassandra, the storage engine groups inserts and updates in memory, and at intervals, sequentially writes the data to disk in append mode. Once written to disk, the data is immutable and is never overwritten. Reading data involves combining this immutable sequentially-written data to discover the correct query results. You can use [Lightweight transactions \(LWT\)](#) to check the state of the data before writing. However, this feature is recommended only for limited use.

A log-structured engine that avoids overwrites and uses sequential I/O to update data is essential for writing to solid-state disks (SSD) and hard disks (HDD). On HDD, writing randomly involves a higher number of seek operations than sequential writing. The seek penalty incurred can be substantial. Because Cassandra sequentially writes immutable files, thereby avoiding [write amplification](#) and disk failure, the database accommodates inexpensive, consumer SSDs extremely well. For many other databases, write amplification is a problem on SSDs.

How Cassandra reads and writes data

To manage and access data in Cassandra, it is important to understand how Cassandra stores data. The hinted handoff feature plus Cassandra conformance and non-conformance to the ACID (atomic, consistent, isolated, durable) database properties are key concepts to understand reads and writes. In Cassandra, consistency refers to how up-to-date and synchronized a row of data is on all of its replicas.

Client utilities and application programming interfaces (APIs) for developing applications for data storage and retrieval are [available](#).

How is data written?

Cassandra processes data at several stages on the write path, starting with the immediate logging of a write and ending in with a write of data to disk:

- Logging data in the commit log
- Writing data to the memtable
- Flushing data from the memtable
- Storing data on disk in SSTables

Logging writes and memtable storage

When a write occurs, Cassandra stores the data in a memory structure called memtable, and to provide [configurable durability](#), it also appends writes to the commit log on disk. The commit log receives every write made to a Cassandra node, and these durable writes survive permanently even if power fails on

a node. The memtable is a write-back cache of data partitions that Cassandra looks up by key. The memtable stores writes in sorted order until reaching a configurable limit, and then is flushed.

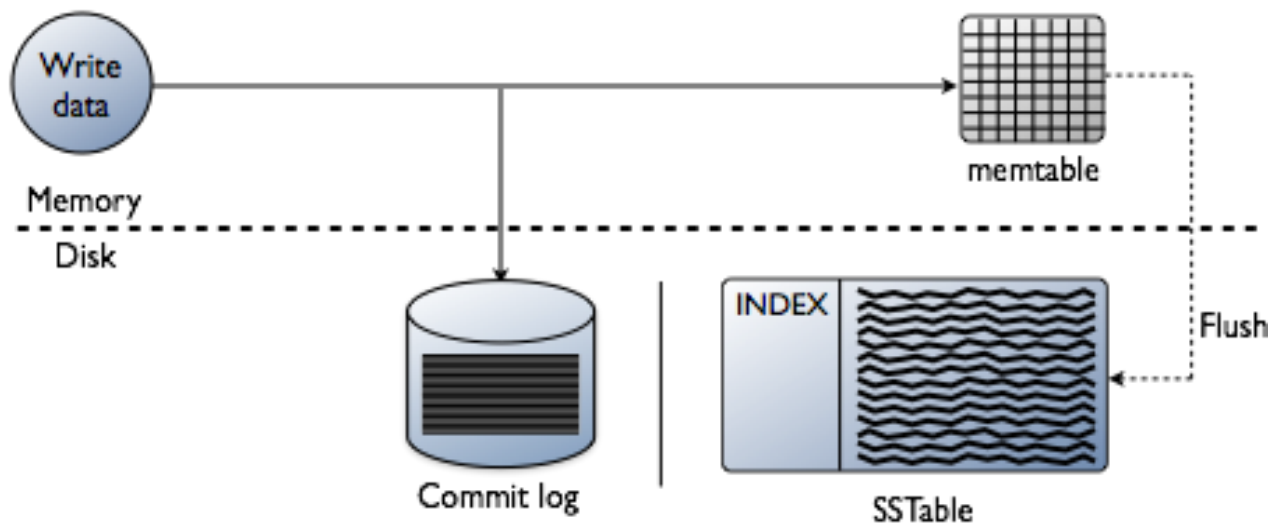
Flushing data from the memtable

To flush the data, Cassandra writes the data to disk, in the memtable-sorted order.. A partition index is also created on the disk that maps the tokens to a location on disk. When the memtable content exceeds the [configurable threshold](#) or the commitlog space exceeds the `commitlog_total_space_in_mb`, the memtable is put in a queue that is flushed to disk. The queue can be configured with the `memtable_heap_space_in_mb` or `memtable_offheap_space_in_mb` setting in the `cassandra.yaml` file. If the data to be flushed exceeds the `memtable_cleanup_threshold`, Cassandra blocks writes until the next flush succeeds. You can manually flush a table using [nodetool flush](#) or [nodetool drain](#) (flushes memtables without listening for connections to other nodes). To reduce the commit log replay time, the recommended best practice is to flush the memtable before you restart the nodes. If a node stops working, replaying the commit log restores to the memtable the writes that were there before it stopped.

Data in the commit log is purged after its corresponding data in the memtable is flushed to an SSTable on disk.

Storing data on disk in SSTables

Memtables and SSTables are maintained per table. The commit log is shared among tables. SSTables are immutable, not written to again after the memtable is flushed. Consequently, a partition is typically stored across multiple SSTable files. A number of other SSTable structures exist to assist read operations:



For each SSTable, Cassandra creates these structures:

Data (Data.db)

The SSTable data

Primary Index (Index.db)

Index of the row keys with pointers to their positions in the data file

Bloom filter (Filter.db)

A structure stored in memory that checks if row data exists in the memtable before accessing SSTables on disk

Compression Information (CompressionInfo.db)

A file holding information about uncompressed data length, chunk offsets and other compression information

Statistics (Statistics.db)

Statistical metadata about the content of the SSTable

Digest (Digest.crc32, Digest.adler32, Digest.sha1)

A file holding adler32 checksum of the data file

CRC (CRC.db)

A file holding the CRC32 for chunks in an a uncompressed file.

SSTable Index Summary (SUMMARY.db)

A sample of the partition index stored in memory

SSTable Table of Contents (TOC.txt)

A file that stores the list of all components for the sstable TOC

Secondary Index (SI_*.db)

Built-in secondary index. Multiple SIs may exist per SSTable

The SSTables are files stored on disk. The naming convention for SSTable files has changed with Cassandra 2.2 and later to shorten the file path. The data files are stored in a data directory that varies with installation. For each keyspace, a directory within the data directory stores each table. For example, `/data/data/ks1/cf1-5be396077b811e3a3ab9dc4b9ac088d/1a-1-big-Data.db` represents a data file. `ks1` represents the keyspace name to distinguish the keyspace for streaming or bulk loading data. A hexadecimal string, `5be396077b811e3a3ab9dc4b9ac088d` in this example, is appended to table names to represent unique table IDs.

Cassandra creates a subdirectory for each table, which allows you to symlink a table to a chosen physical drive or data volume. This provides the capability to move very active tables to faster media, such as SSDs for better performance, and also divides tables across all attached storage devices for better I/O balance at the storage layer.

How is data maintained?

The Cassandra write process stores data in structures called SSTables. SSTables are immutable. Instead of overwriting existing rows with inserts or updates, Cassandra writes new timestamped versions of the inserted or updated data in new SSTables. Also, Cassandra also does not delete in place: instead, Cassandra marks data to be deleted with a [tombstone](#).

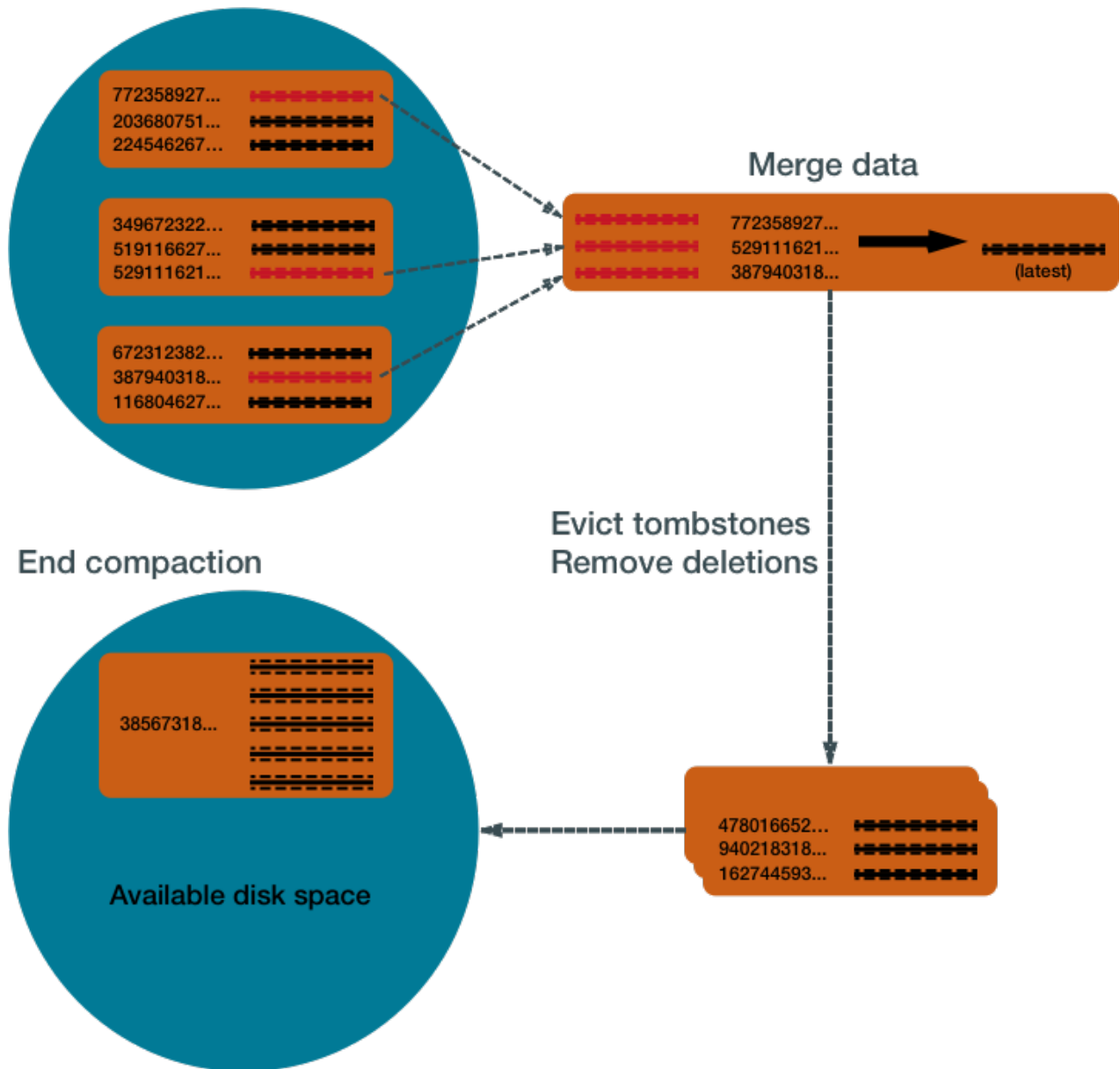
Over time, Cassandra may write many versions of a row, each in a different SSTable. Each version may have a unique set of columns stored, with a different timestamp. This means that Cassandra must access more and more SSTables to retrieve an entire row of data.

To keep the database healthy, Cassandra periodically merges SSTables and discards old data. This process is called compaction.

Compaction

Compaction merges the data in each SSTable by [partition key](#), selecting the version of the data with the latest timestamp. The merge process is performant. Because rows are sorted by partition key within each SSTable, the merge process does not use random I/O. After removing deleted columns and rows, the compaction process consolidates SSTables into a new single SSTable. The old SSTable files are deleted as soon as pending reads finish using the files.

Start compaction



Compaction causes a temporary spike in disk space usage and disk I/O while old and new SSTables co-exist. As it completes, compaction frees up disk space that was occupied by old SSTables. It improves read performance by incrementally replacing old SSTables with compacted SSTables. Cassandra can read data directly from the new SSTable even before it finishes writing, instead of waiting for the entire compaction process to finish.

As Cassandra processes writes and reads, it replaces the old SSTables with new SSTables in the page cache. The process of caching the new SSTable, while directing reads away from the old one, is incremental – it does not cause a the dramatic cache miss. Cassandra provides predictable high performance even under heavy load.

Compaction strategies

Cassandra supports different compaction strategies. Each has its own strengths. Understanding how each strategy works is vital to choosing the right one for your application workload. Although each of the following sections starts with a generalized recommendation, there are many factors that complicate

the choice of a compaction strategy. For more in-depth information about the relative strengths of each strategy and discussions of specific use cases, see [Which compaction strategy is best?](#).

SizeTieredCompactionStrategy (STCS)

Recommended for write-intensive workloads.

The SizeTieredCompactionStrategy (STCS) initiates compaction when a set number (default is 4) of similar-sized SSTables has accumulated. This compaction strategy merges these SSTables into one larger SSTable. Then the larger SSTables are in turn merged into even larger SSTables. At any given time, several SSTables of varying sizes are present.

Figure: Size tiered compaction after many inserts



While this strategy works well to compact a write-intensive workload, it makes reads slower, because the merge-by-size process does not tend to group data by rows. For this reason, it is more likely that the data for a particular row may be spread over many SSTables. Also, the eviction of deleted data does not occur predictably, because SSTable size is the trigger for compaction, and SSTables might not grow quickly enough to merge and evict old data. As the largest SSTables grow in size, the amount of disk space needed for compaction to hold both the new and old SSTables simultaneously can outstrip a typical amount of disk space on a node.

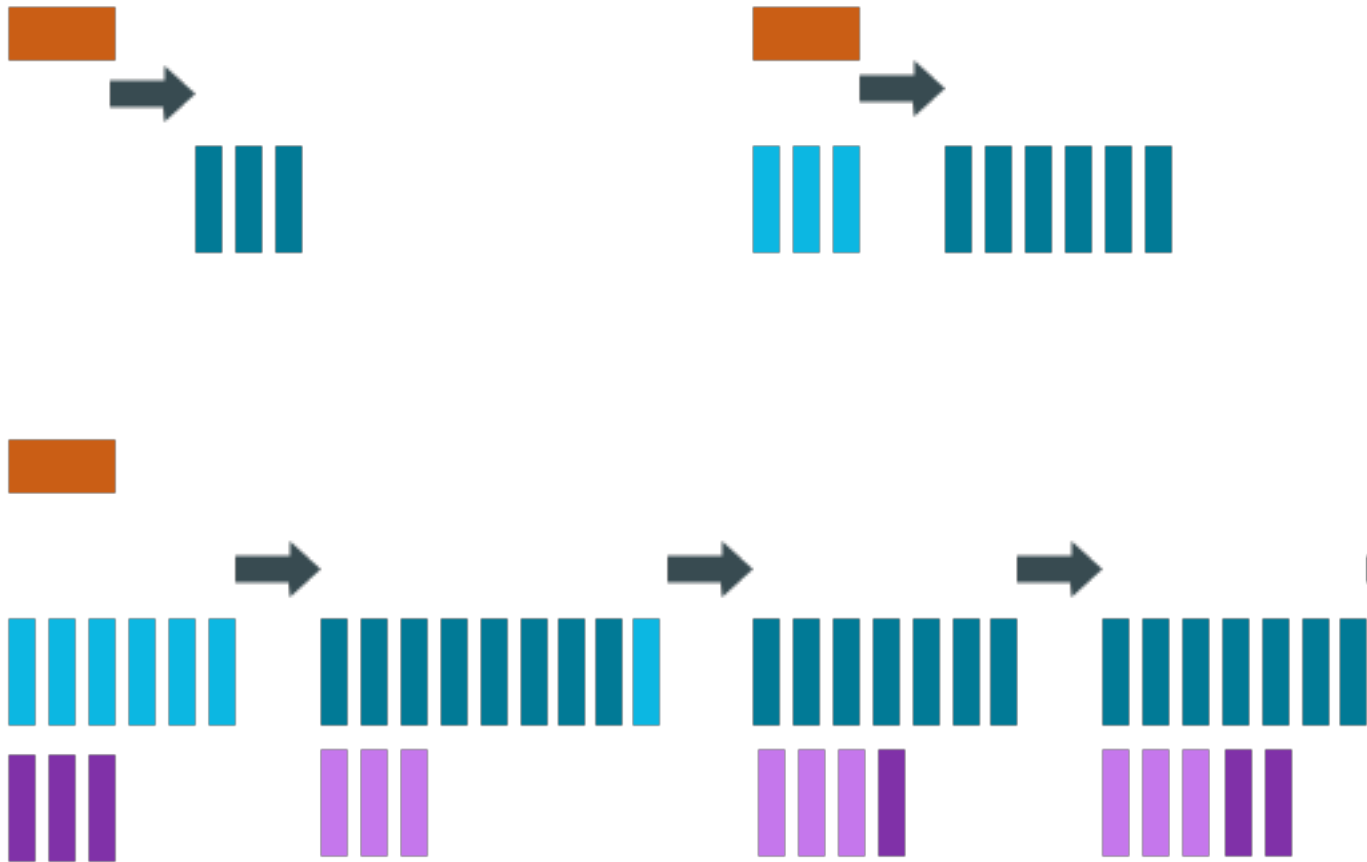
- **Pros:** Compacts write-intensive workload very well.
- **Cons:** Can hold onto stale data too long. Amount of memory needed increases over time.

LeveledCompactionStrategy (LCS)

Recommended for read-intensive workloads.

The LeveledCompactionStrategy (LCS) works to alleviate some of the read operation issues with STCS. This strategy works with a series of levels. First, memtables are first flushed to SSTables in the first level (L0). Then compaction merges these SSTables with larger SSTables in level L1.

Figure: Leveled compaction — adding SSTables



The SSTables in levels greater than L1 are merged into SSTables with a size greater than or equal to `sstable_size_in_mb` (default: 160 MB). If a L1 SStable stores data of a partition that is larger than L2, LCS moves the SStable past L2 to the next level up.

Figure: Leveled compaction after many inserts



In each of the levels above L0, LCS creates SSTables that are about the same size. Each level is 10X the size of the last level, so level L1 has 10X as many SSTables as L0, and level L2 has 100X as many. If the result of the compaction is more than 10 SSTables in level L1, the excess SSTables are moved to level L2.

The LCS compaction process guarantees that the SSTables within each level starting with L1 have non-overlapping data. For many reads, this guarantee enables Cassandra to retrieve all the required data from only one or two SSTables. In fact, 90% of all reads can be satisfied from one SStable. Since LCS does not compact L0 tables, however, resource-intensive reads involving many L0 SSTables may still occur.

At levels beyond L0, LCS requires less disk space for compacting — generally, 10X the fixed size of the SSTable. Obsolete data is evicted more often, so deleted data uses smaller portions of the SSTables on disk. However, LCS compaction operations take place more often and place more I/O burden on the node. For write-intensive workloads, the payoff of using this strategy is generally not worth the performance loss to I/O operations. In many cases, tests of LCS-configured tables reveal I/O saturation on writes and compactions.

Note: Performance improvements in Cassandra 2.2 and later bypass compaction operations when bootstrapping a new node using LCS into a cluster. The original data is moved directly to the correct level because there is no existing data, so no partition overlap per level is present. For more information, see [Apache Cassandra 2.2 - Bootstrapping Performance Improvements for Leveled Compaction](#).

- **Pros:** Disk requirements are easier to predict. Read operation latency is more predictable. Stale data is evicted more frequently.
- **Cons:** Much higher I/O utilization impacting operation latency

DateTieredCompactionStrategy (DTCS)

Recommended for time series and expiring TTL workloads.

The DateTieredCompactionStrategy (DTCS) is similar to STCS. But instead of compacting based on SSTable size, DTCS compacts based on SSTable age. Configuring the time window ensures that new and old data is not mixed in merged SSTables. In fact, using Time-To-Live (TTL) timestamps, DTCS can eject whole SSTables containing expired data. This strategy often generates similar-sized SSTables, if time series data is ingested at a steady rate.

DTCS merges SSTables when the system reaches a certain minimum threshold of number of SSTables within a configurable time interval. DTCS merges SSTables into larger tables, as in STC, when the required number of SSTables falls within the time interval. However, DTCS skips compacting SSTables that reach a configurable age. This reduces the number of times data is rewritten. Queries that ask for the *last hour's worth of data* (or some other time interval that is well coordinated with the configured time interval) can be executed very efficiently on DTCS-compacted SSTables.

One case that can cause difficulty with this strategy is out-of-order writing – for example, an operation that writes a timestamped record with a past timestamp. Read repairs can inject an out-of-order timestamping, so be sure to turn off read repairs when using DTCS.

- **Pros:** Specifically designed for time series data.
- **Cons:** Out of order data injections can cause errors. Read repair must be turned off for DTCS, and `TIMESTAMP` options must not be used with the `BATCH`, `DELETE`, `INSERT` and `UPDATE` CQL commands.

Which compaction strategy is best?

To implement the best compaction strategy:

1. Review your application's requirements.
2. Configure the table to use the most appropriate strategy.
3. Test the compaction strategies against your data.

The following questions are based on the experiences of Cassandra developers and users with the strategies described above.

Does your table process time series data?

If so, DTCS is probably your best choice. To avoid problems, review the description above.

If your table is not focused on time series data, the choice becomes more complicated. The following questions introduce other considerations that may guide your choice.

Does your table handle more reads than writes, or more writes than reads?

LCS is a good choice if your table processes twice as many reads as writes or more – especially randomized reads. If the proportion of reads to writes is closer, the performance hit exacted by LCS may not be worth the benefit. Be aware that LCS can be quickly overwhelmed by a high volume of writes.

Does the data in your table change often?

One advantage of LCS is that it keeps related data in a small set of SSTables. If your data is *immutable* or not subject to frequent [upserts](#), STCS accomplishes the same type of grouping without the LCS performance hit.

Do you require predictable levels of read and write activity?

LCS keeps the SSTables within predictable sizes and numbers. For example, if your table's read/write ratio is small, and it is expected to conform to a Service Level agreements (SLAs) for reads, it may be worth taking the write performance penalty of LCS in order to keep read rates and latency at predictable levels. And you may be able to overcome this write penalty through *horizontal scaling* — adding more nodes.

Will your table be populated by a batch process?

On both batch reads and batch writes, STCS performs better than LCS. The batch process causes little or no fragmentation, so the benefits of LCS are not realized. And batch processes can overwhelm LCS-configured tables.

Does your system have limited disk space?

LCS handles disk space more efficiently than STCS: it requires about 10% *headroom* in addition to the space occupied by the data it handles. STCS and DTCS generally require more — in some cases, 50% more than the data space.

Is your system reaching its limits for I/O?

LCS is significantly more I/O intensive than DTCS or STCS. Switching to LCS may introduce extra I/O load that offsets the advantages.

Testing compaction strategies

Suggestions for determining which compaction strategy is best for your system:

- Create a three-node cluster using one of the compaction strategies, stress test the cluster using `cassandra-stress`, and measure the results.
- Set up a node on your existing cluster and use Cassandra's write survey mode to sample live data. See [What's new in Cassandra 1.1: live traffic sampling](#).

Configuring and running compaction

Set the compaction strategy for a table in the parameters for the `CREATE TABLE` or `ALTER TABLE` command. For details, see [Table properties](#).

You can start compaction manually using the `nodetool compact` command.

More information about compaction

The following blog posts provide more information from developers that have tested compaction strategies:

- [When to Use Leveled Compaction](#)
- [Leveled compaction in Apache Cassandra](#)
- [DateTieredCompactionStrategy: Notes from the Field](#)
- [Date-Tiered Compaction in Cassandra](#)
- [DateTieredCompactionStrategy: Compaction for Time Series Data](#)
- [What delays a tombstone purge when using LCS in Cassandra](#)

How is data updated?

Inserting a duplicate primary key is treated as an [upsert](#). An upsert writes a new record to the database if the data didn't exist before. If the data for that primary key already exists, a new record is written with a more recent timestamp. If the data is retrieved during a read, only the most recent is retrieved; older timestamped data will be marked for deletion. The net effect is similar to swapping overwriting the old value with the new value, even though Cassandra does not overwrite data. Eventually, the updates are streamed

to disk using sequential I/O and stored in a new SSTable. During an update, Cassandra timestamps and writes columns to disk using the [write path](#). If a user writes the same data several times, only the latest version is stored in the memtable and flushed to disk, as described in the [Compaction](#) section.

Inserting a duplicate primary key is treated as an [upsert](#). An upsert writes a new record to the database if the data didn't exist before. If the data for that primary key already exists, a new record is written with a more recent timestamp. If the data is retrieved during a read, only the most recent is retrieved; older timestamped data will be marked for deletion. The net effect is similar to swapping overwriting the old value with the new value, even though Cassandra does not overwrite data. Eventually, the updates are streamed to disk using sequential I/O and stored in a new SSTable. During an update, Cassandra timestamps and writes columns to disk using the [write path](#). If multiple versions of the column exist in the memtable, Cassandra flushes only the newer version of the column to disk, as described in the [Compaction](#) section.

How is data deleted?

Cassandra's processes for deleting data are designed to improve performance, and to work with Cassandra's built-in properties for data distribution and fault-tolerance.

Cassandra treats a delete as an insert or [upsert](#). The data being added to the record in the [DELETE](#) command is a deletion marker called a [tombstone](#). The tombstone goes through Cassandra's write path, and are written to SSTables on one or more nodes. The key difference: the tombstone has a built-in expiration date/time. At the end of its expiration period (for details see below) the tombstone is eligible for deletion as part of Cassandra's normal [compaction](#) process.

You can also mark a Cassandra record (row or column) with a [time-to-live](#) value. After this amount of time has ended, Cassandra marks the record with a tombstone, and handles it like other tombstoned records.

Deletion in a distributed system

In a multi-node cluster, Cassandra stores replicas of the same data on two or more nodes. This helps prevent data loss, but it complicates the delete process. If a node receives a delete for data it stores locally, the node tombstones the specified record and tries to pass the tombstone to other nodes containing replicas of that record. But if one replica node is unresponsive at that time, it does not receive the tombstone immediately, so it still contains the pre-delete version of the record. If the tombstoned record has already been deleted from the rest of the cluster by the time that node recovers, Cassandra treats the record on the recovered node as new data, and propagates it to the rest of the cluster. This kind of deleted but persistent record is called a [zombie](#).

To prevent the reappearance of zombies, Cassandra gives each tombstone a *grace period*. Its purpose is to give unresponsive nodes time to recover and process tombstones normally. If a client writes a new update to the tombstoned record during the grace period, Cassandra overwrites the tombstone. If a client sends a read for that record during the grace period, Cassandra disregards the tombstone, and retrieves the record from other replicas if possible.

When an unresponsive node recovers, Cassandra uses [hinted handoff](#) to replay the database mutations the node missed while it was down. Cassandra will not replay a mutation for a tombstone during its grace period. But if the node does not recover until after the grace period ends, Cassandra may miss the deletion.

After the tombstone's grace period ends, Cassandra deletes the tombstone during compaction.

The `gc_grace_period` property can be set individually for each table. Its default value is 86400 seconds (24 hours).

More about Cassandra deletes

Details:

- The expiration date/time for a tombstone is the date/time of its creation plus the value of the [table property](#) `gc_grace_seconds`.
- Cassandra also supports [Batching data insertion and updates](#). This procedure introduces the same danger of replaying a record insertion after that record has been removed from the rest of the cluster.

Cassandra does not replay a batched mutation for a tombstoned record that is still within its grace period.

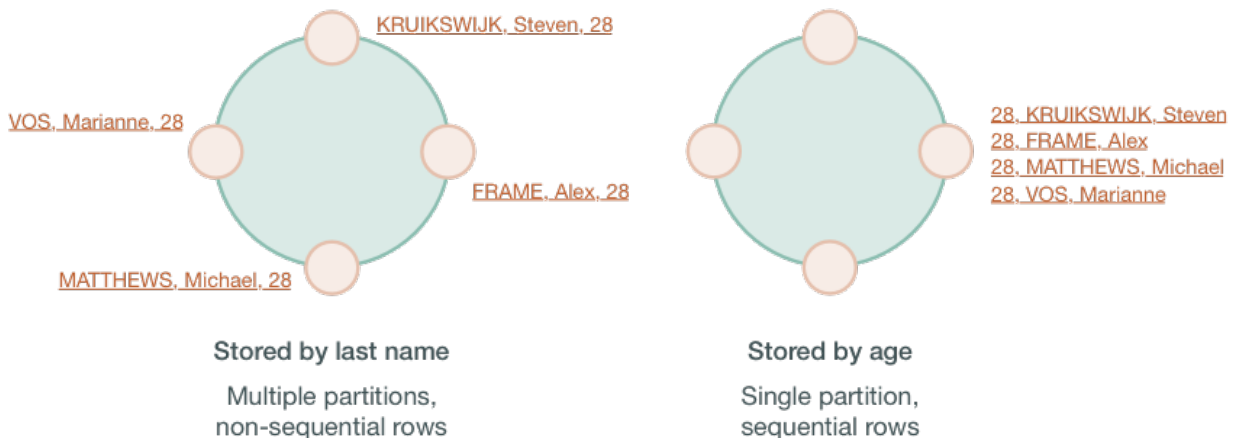
- On a single-node cluster, you can set `gc_grace_seconds` to 0 (zero).
- To completely prevent the reappearance of zombie records, run `nodetool repair` on a node after it recovers, and on each table every `gc_grace_seconds`.
- If all records in a table are given a TTL at creation, and all are allowed to expire and not deleted manually, it is not necessary to run `nodetool repair` for that table on a regular basis.
- If you use the `SizeTieredCompactionStrategy` or `DateTieredCompactionStrategy`, you can delete tombstones immediately by manually starting the compaction process.

CAUTION: If you force compaction, Cassandra may create one very large SSTable from all the data. Cassandra will not trigger another compaction for a long time. The data in the SSTable created during the forced compaction can grow very stale during this long period of non-compaction.

- Cassandra allows you to set a `default_time_to_live` property for an entire table. Columns and rows marked with regular TTLs are processed as described above; but when a record exceeds the table-level TTL, Cassandra deletes it immediately, without tombstoning or compaction.
- Cassandra supports immediate deletion through the `DROP KEYSPACE` and `DROP TABLE` statements.

How are indexes stored and updated?

Secondary indexes are used to filter a table for data stored in non-primary key columns. For example, a table storing cyclist names and ages using the last name of the cyclist as the primary key might have a secondary index on the age to allow queries by age. Querying to match a non-primary key column is an anti-pattern, as querying should always result in a continuous slice of data retrieved from the table.



If the table rows are stored based on last names, the table may be spread across several partitions stored on different nodes. Queries based on a particular range of last names, such as all cyclists with the last name `Matthews` will retrieve sequential rows from the table, but a query based on the age, such as all cyclists who are 28, will require all nodes to be queried for a value. Non-primary keys play no role in ordering the data in storage, thus querying for a particular value of a non-primary key column results in scanning all partitions. Scanning all partitions generally results in a prohibitive read latency, and is not allowed.

Secondary indexes can be built for a column in a table. These indexes are stored locally on each node in a hidden table and built in a background process. If a secondary index is used in a query that is not restricted to a particular partition key, the query will have prohibitive read latency because all nodes will be queried. A query with these parameters is only allowed if the query option `ALLOW FILTERING` is used. This option is not appropriate for production environments. If a query includes both a partition key condition and a secondary index column condition, the query will be successful because the query can be directed to a single node partition.

This technique, however, does not guarantee trouble-free indexing, so know [when and when not to use an index](#). In the example shown above, an index on the age could be used, but a better solution is to create a materialized view or additional table that is ordered by age.

As with relational databases, keeping indexes up to date uses processing time and resources, so unnecessary indexes should be avoided. When a column is updated, the index is updated as well. If the old column value still exists in the memtable, which typically occurs when updating a small set of rows repeatedly, Cassandra removes the corresponding obsolete index entry; otherwise, the old entry remains to be purged by compaction. If a read sees a stale index entry before compaction purges it, the reader thread invalidates it.

How is data read?

To satisfy a read, Cassandra must combine results from the active memtable and potentially multiple SSTables.

Cassandra processes data at several stages on the read path to discover where the data is stored, starting with the data in the memtable and finishing with SSTables:

- Check the memtable
- Check row cache, if enabled
- Checks Bloom filter
- Checks partition key cache, if enabled
- Goes directly to the compression offset map if a partition key is found in the partition key cache, or checks the partition summary if not

If the partition summary is checked, then the partition index is accessed

- Locates the data on disk using the compression offset map
- Fetches the data from the SSTable on disk

Figure: Read request flow

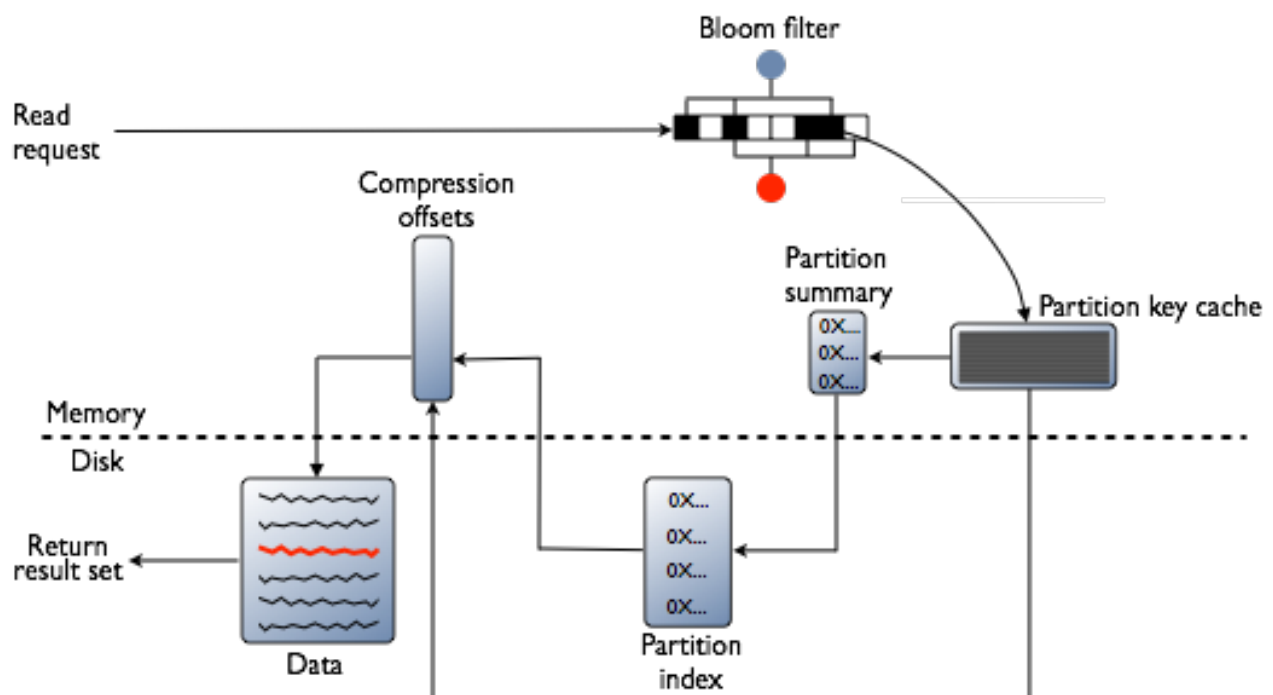
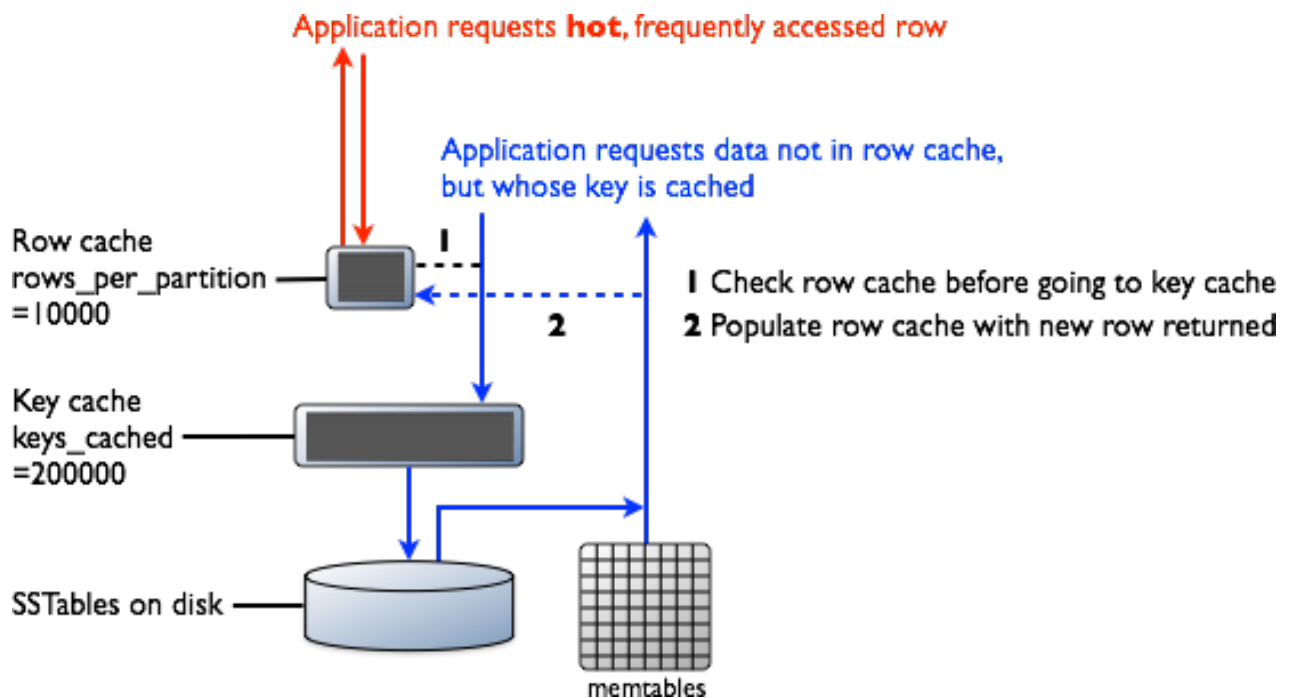


Figure: Row cache and Key cache request flow



Memtable

If the memtable has the desired partition data, then the data is read and then merged with the data from the SSTables. The SSTable data is accessed as shown in the following steps.

Row Cache

Typical of any database, reads are fastest when the most in-demand data fits into memory. The operating system page cache is best at improving performance, although the row cache can provide some improvement for very read-intensive operations, where read operations are 95% of the load. Row cache is contra-indicated for write-intensive operations. The row cache, if enabled, stores a subset of the partition data stored on disk in the SSTables in memory. In Cassandra 2.2 and later, it is stored in fully off-heap memory using a new implementation that relieves garbage collection pressure in the JVM. The subset stored in the row cache use a configurable amount of memory for a specified period of time. The row cache uses LRU (least-recently-used) eviction to reclaim memory when the cache has filled up.

The row cache size is configurable, as is the number of rows to store. Configuring the number of rows to be stored is a useful feature, making a "Last 10 Items" query very fast to read. If row cache is enabled, desired partition data is read from the row cache, potentially saving two seeks to disk for the data. The rows stored in row cache are frequently accessed rows that are merged and saved to the row cache from the SSTables as they are accessed. After storage, the data is available to later queries. The row cache is not write-through. If a write comes in for the row, the cache for that row is invalidated and is not cached again until the row is read. Similarly, if a partition is updated, the entire partition is evicted from the cache. When the desired partition data is not found in the row cache, then the [Bloom filter](#) is checked.

Bloom Filter

First, Cassandra checks the Bloom filter to discover which SSTables are likely to have the request partition data. The Bloom filter is stored in off-heap memory. Each SSTable has a Bloom filter associated with it. A Bloom filter can establish that a SSTable does not contain certain partition data. A Bloom filter can also find the likelihood that partition data is stored in a SSTable. It speeds up the process of partition key lookup by narrowing the pool of keys. However, because the Bloom filter is a probabilistic function, it can result in false positives. Not all SSTables identified by the Bloom filter will have data. If the Bloom filter does not rule out an SSTable, Cassandra checks the [partition key cache](#)

The Bloom filter grows to approximately 1-2 GB per billion partitions. In the extreme case, you can have one partition per row, so you can easily have billions of these entries on a single machine. The Bloom filter is tunable if you want to trade memory for performance.

Partition Key Cache

The partition key cache, if enabled, stores a cache of the partition index in off-heap memory. The key cache uses a small, configurable amount of memory, and each "hit" saves one seek during the read operation. If a partition key is found in the key cache can go directly to the compression offset map to find the compressed block on disk that has the data. The partition key cache functions better once warmed, and can greatly improve over the performance of cold-start reads, where the key cache doesn't yet have or has purged the keys stored in the key cache. It is possible to limit the number of partition keys saved in the key cache, if memory is very limited on a node. If a partition key is not found in the key cache, then the [partition summary](#) is searched.

The partition key cache size is configurable, as are the number of partition keys to store in the key cache.

Partition Summary

The partition summary is an off-heap in-memory structure that stores a sampling of the partition index. A partition index contains all partition keys, whereas a partition summary samples every X keys, and maps the location of every Xth key's location in the index file. For example, if the partition summary is set to sample every 20 keys, it will store the location of the first key as the beginning of the SSTable file, the 20th key and its location in the file, and so on. While not as exact as knowing the location of the partition key, the partition summary can shorten the scan to find the partition data location. After finding the range of possible partition key values, the [partition index](#) is searched.

By configuring the sample frequency, you can trade memory for performance, as the more granularity the partition summary has, the more memory it will use. The sample frequency is changed using the [index interval](#) property in the table definition. A fixed amount of memory is configurable using the [index_summary_capacity_in_mb](#) property, and defaults to 5% of the heap size.

Partition Index

The partition index resides on disk and stores an index of all partition keys mapped to their offset. If the partition summary has been checked for a range of partition keys, now the search passes to the partition index to seek the location of the desired partition key. A single seek and sequential read of the columns over the passed-in range is performed. Using the information found, the partition index now goes to the compression offset map to find the compressed block on disk that has the data. If the partition index must be searched, two seeks to disk will be required to find the desired data.

Compression offset map

The compression offset map stores pointers to the exact location on disk that the desired partition data will be found. It is stored in off-heap memory and is accessed by either the partition key cache or the partition index. The desired compressed partition data is fetched from the correct SSTable(s) once the compression offset map identifies the disk location. The query receives the result set.

Note: Within a partition, all rows are not equally expensive to query. The very beginning of the partition (the first rows, clustered by your key definition) is slightly less expensive to query because there is no need to consult the partition-level index.

The compression offset map grows to 1-3 GB per terabyte compressed. The more you compress data, the greater number of compressed blocks you have and the larger the compression offset table. Compression is enabled by default even though going through the compression offset map consumes CPU resources. Having compression enabled makes the page cache more effective, and typically, almost always pays off.

How do write patterns affect reads?

It is important to consider how the write operations will affect the read operations in the cluster. The type of [compaction strategy](#) Cassandra performs on your data is configurable and can significantly affect read performance. Using the `SizeTieredCompactionStrategy` or `DateTieredCompactionStrategy` tends to cause data fragmentation when rows are frequently updated. The `LeveledCompactionStrategy` (LCS) was designed to prevent fragmentation under this condition.

Data consistency

How are consistent read and write operations handled?

Consistency refers to how up-to-date and synchronized all replicas of a row of Cassandra data are at any given moment. Ongoing [repair operations](#) in Cassandra ensure that all replicas of a row will eventually be consistent. Repairs work to decrease the variability in replica data, but constant data traffic through a widely distributed system can lead to inconsistency (stale data) at any given time. Cassandra is a AP system according to the [CAP theorem](#), providing high availability and partition tolerance. Cassandra does have flexibility in its configuration, though, and can perform more like a CP (consistent and partition tolerant) system according to the CAP theorem, depending on the application requirements. Two consistency features are tunable consistency and linearizable consistency.

Tunable consistency

To ensure that Cassandra can provide the proper levels of consistency for its reads and writes, Cassandra extends the concept of [eventual consistency](#) by offering tunable consistency. You can tune Cassandra's consistency level per-operation, or set it globally for a cluster or data center. You can vary the consistency for individual read or write operations so that the data returned is more or less consistent, as required by the client application. This allows you to make Cassandra act more like a CP (consistent and partition tolerant) or AP (highly available and partition tolerant) system according to the CAP theorem, depending on the application requirements.

Note: It is not possible to "tune" Cassandra into a completely CA system. See [You Can't Sacrifice Partition Tolerance](#) for a more detailed discussion.

There is a tradeoff between operation latency and consistency: higher consistency incurs higher latency, lower consistency permits lower latency. You can control latency by tuning consistency.

The consistency level determines the number of replicas that need to acknowledge the read or write operation success to the client application. For read operations, the read consistency level specifies how many replicas must respond to a read request before returning data to the client application. If a read operation reveals inconsistency among replicas, Cassandra initiates a [read repair](#) to update the inconsistent data.

For write operations, the write consistency level specified how many replicas must respond to a write request before the write is considered successful. Even at low consistency levels, Cassandra writes to all replicas of the partition key, including replicas in other data centers. The write consistency level just specifies when the coordinator can report to the client application that the write operation is considered completed. Write operations will use [hinted handoffs](#) to ensure the writes are completed when replicas are down or otherwise not responsive to the write request.

Typically, a client specifies a consistency level that is less than the replication factor specified by the keyspace. Another common practice is to write at a consistency level of QUORUM and read at a consistency level of QUORUM. The choices made depend on the client application's needs, and Cassandra provides maximum flexibility for application design.

Linearizable consistency

In ACID terms, linearizable consistency (or serial consistency) is a serial (immediate) isolation level for [lightweight transactions](#). Cassandra does not use employ traditional mechanisms like locking or transactional dependencies when concurrently updating multiple rows or tables.

However, some operations must be performed in sequence and not interrupted by other operations. For example, duplications or overwrites in user account creation can have serious consequences. Situations like race conditions (two clients updating the same record) can introduce inconsistency across replicas. Writing with high consistency does nothing to reduce this. You can apply linearizable consistency to a unique identifier, like the userID or email address, although is not required for all aspects of the user's account. Serial operations for these elements can be implemented in Cassandra with the Paxos consensus protocol, which uses a quorum-based algorithm. Lightweight transactions can be implemented without the need for a master database or two-phase commit process.

Lightweight transaction write operations use the serial consistency level for Paxos consensus and the regular consistency level for the write to the table. For more information, see [Lightweight Transactions](#).

Calculating consistency

Reliability of read and write operations depends on the consistency used to verify the operation. Strong consistency can be guaranteed when the following condition is true:

$$R + W > N$$

where

- R is the consistency level of read operations
- W is the consistency level of write operations
- N is the number of replicas

If the replication factor is 3, then the consistency level of the reads and writes combined must be at least 4. For example, read operations using 2 out of 3 replicas to verify the value, and write operations using 2 out of 3 replicas to verify the value will result in strong consistency. If fast write operations are required, but strong consistency is still desired, the write consistency level is lowered to 1, but now read operations have to verify a matched value on all 3 replicas. Writes will be fast, but reads will be slower.

Eventual consistency occurs if the following condition is true:

$$R + W \leq N$$

where

- R is the consistency level of read operations
- W is the consistency level of write operations
- N is the number of replicas

If the replication factor is 3, then the consistency level of the reads and writes combined are 3 or less. For example, read operations using [QUORUM](#) (2 out of 3 replicas) to verify the value, and write operations using [ONE](#) (1 out of 3 replicas) to do fast writes will result in eventual consistency. All replicas will receive the data, but read operations are more vulnerable to selecting data before all replicas write the data.

Additional consistency examples:

- You do a write at [ONE](#), the replica crashes one second later. The other messages are not delivered. The data is lost.
- You do a write at [ONE](#), and the operation times out. Future reads can return the old or the new value. You will not know the data is incorrect.
- You do a write at [ONE](#), and one of the other replicas is down. The node comes back online. The application will get old data from that node until the node gets the correct data or a read repair occurs.

- You do a write at QUORUM, and then a read at QUORUM. One of the replicas dies. You will always get the correct data.

How are Cassandra transactions different from RDBMS transactions?

Cassandra does not use RDBMS ACID transactions with rollback or locking mechanisms, but instead offers atomic, isolated, and durable transactions with eventual/tunable consistency that lets the user decide how strong or eventual they want each transaction's consistency to be.

As a non-relational database, Cassandra does not support joins or foreign keys, and consequently does not offer consistency in the ACID sense. For example, when moving money from account A to B the total in the accounts does not change. Cassandra supports atomicity and isolation at the row-level, but trades transactional isolation and atomicity for high availability and fast write performance. Cassandra writes are durable.

Atomicity

In Cassandra, a write operation is atomic at the partition level, meaning the insertions or updates of two or more rows in the same partition are treated as one write operation. A delete operation is also atomic at the partition level.

For example, if using a write consistency level of QUORUM with a replication factor of 3, Cassandra will replicate the write to all nodes in the cluster and wait for acknowledgement from two nodes. If the write fails on one of the nodes but succeeds on the other, Cassandra reports a failure to replicate the write on that node. However, the replicated write that succeeds on the other node is not automatically rolled back.

Cassandra uses client-side timestamps to determine the most recent update to a column. The latest timestamp always wins when requesting data, so if multiple client sessions update the same columns in a row concurrently, the most recent update is the one seen by readers.

Isolation

Cassandra write and delete operations are performed with full row-level isolation. This means that a write to a row within a single partition on a single node is only visible to the client performing the operation – the operation is restricted to this scope until it is complete. All updates in a batch operation belonging to a given partition key have the same restriction. However, a Batch operation is not isolated if it includes changes to more than one partition.

Durability

Writes in Cassandra are durable. All writes to a replica node are recorded both in memory and in a commit log on disk before they are acknowledged as a success. If a crash or server failure occurs before the memtables are flushed to disk, the commit log is replayed on restart to recover any lost writes. In addition to the local durability (data immediately written to disk), the replication of data on other nodes strengthens durability.

You can manage the local durability to suit your needs for consistency using the `commitlog_sync` option in the `cassandra.yaml` file. Set the option to either `periodic` or `batch`.

How do I accomplish lightweight transactions with linearizable consistency?

Distributed databases present a unique challenge when data must be strictly read and written in sequential order. In transactions for creating user accounts or transferring money, race conditions between two potential writes must be regulated to ensure that one write precedes the other. In Cassandra, the Paxos consensus protocol is used to implement lightweight transactions that can handle concurrent operations.

The Paxos protocol is implemented in Cassandra with linearizable consistency, that is sequential consistency with real-time constraints. Linearizable consistency ensures transaction isolation at a level similar to the serializable level offered by RDBMSs. This type of transaction is known as compare and set (CAS); replica data is compared and any data found to be out of date is set to the most consistent value. In Cassandra, the process combines the Paxos protocol with normal read and write operations to accomplish the compare and set operation.

The Paxos protocol is implemented as a series of phases:

1. Prepare/Promise
2. Read/Results
3. Propose/Accept
4. Commit/Acknowledge

These phases are actions that take place between a proposer and acceptors. Any node can be a proposer, and multiple proposers can be operating at the same time. For simplicity, this description will use only one proposer. A proposer prepares by sending a message to a quorum of acceptors that includes a proposal number. Each acceptor promises to accept the proposal if the proposal number is the highest they have received. Once the proposer receives a quorum of acceptors who promise, the value for the proposal is read from each acceptor and sent back to the proposer. The proposer figures out which value to use and proposes the value to a quorum of the acceptors along with the proposal number. Each acceptor accepts the proposal with a certain number if and only if the acceptor is not already promised to a proposal with a high number. The value is committed and acknowledged as a Cassandra write operation if all the conditions are met.

These four phases require four round trips between a node proposing a lightweight transaction and any cluster replicas involved in the transaction. Performance will be affected. Consequently, reserve lightweight transactions for situations where concurrency must be considered.

Lightweight transactions will block other lightweight transactions from occurring, but will not stop normal read and write operations from occurring. Lightweight transactions use a timestamping mechanism different than for normal operations and mixing LWTs and normal operations can result in errors. If lightweight transactions are used to write to a row within a partition, only lightweight transactions for both read and write operations should be used. This caution applies to all operations, whether individual or batched. For example, the following series of operations can fail:

```
DELETE ...
INSERT .... IF NOT EXISTS
SELECT .....
```

The following series of operations will work:

```
DELETE ... IF EXISTS
INSERT .... IF NOT EXISTS
SELECT .....
```

Reads with linearizable consistency

A [SERIAL consistency level](#) allows reading the current (and possibly uncommitted) state of data without proposing a new addition or update. If a SERIAL read finds an uncommitted transaction in progress, Cassandra performs a [read repair](#) as part of the commit.

How do I discover consistency level performance?

Before changing the consistency level on read and write operations, discover how your CQL commands are performing using the `TRACING` command in CQL. Using `cqlsh`, you can vary the consistency level and trace read and write operations. The tracing output includes latency times for the operations.

The CQL documentation includes a [tutorial](#) comparing consistency levels.

How is the consistency level configured?

Consistency levels in Cassandra can be configured to manage availability versus data accuracy. You can configure consistency on a cluster, data center, or per individual read or write operation. Consistency among participating nodes can be set globally and also controlled on a per-operation basis. Within `cqlsh`, use `CONSISTENCY`, to set the consistency level for all queries in the current `cqlsh` session. For programming client applications, set the consistency level using an appropriate driver. For example, using the Java driver, call `QueryBuilder.insertInto` with `setConsistencyLevel` to set a per-insert consistency level.

The consistency level defaults to `ONE` for all write and read operations.

Write consistency levels

This table describes the write consistency levels in strongest-to-weakest order.

Table: Write Consistency Levels

Level	Description	Usage
ALL	A write must be written to the commit log and memtable on all replica nodes in the cluster for that partition.	Provides the highest consistency and the lowest availability of any other level.
EACH_QUORUM	Strong consistency. A write must be written to the commit log and memtable on a quorum of replica nodes in each datacenter .	Used in multiple data center clusters to strictly maintain consistency at the same level in each data center. For example, choose this level if you want a read to fail when a data center is down and the <code>QUORUM</code> cannot be reached on that data center.
QUORUM	A write must be written to the commit log and memtable on a quorum of replica nodes across <i>all</i> data centers.	Used in either single or multiple data center clusters to maintain strong consistency across the cluster. Use if you can tolerate some level of failure.
LOCAL_QUORUM	Strong consistency. A write must be written to the commit log and memtable on a quorum of replica nodes in the same data center as the coordinator . Avoids latency of inter-data center communication.	Used in multiple data center clusters with a rack-aware replica placement strategy, such as NetworkTopologyStrategy , and a properly configured snitch. Use to maintain consistency locally (within the single data center). Can be used with SimpleStrategy .
ONE	A write must be written to the commit log and memtable of at least one replica node.	Satisfies the needs of most users because consistency requirements are not stringent.
TWO	A write must be written to the commit log and memtable of at least two replica nodes.	Similar to <code>ONE</code> .
THREE	A write must be written to the commit log and memtable of at least three replica nodes.	Similar to <code>TWO</code> .
LOCAL_ONE	A write must be sent to, and successfully acknowledged by, at least one replica node in the local data center.	In a multiple data center clusters, a consistency level of <code>ONE</code> is often desirable, but cross-DC traffic is not. <code>LOCAL_ONE</code> accomplishes this. For security and quality reasons, you can use this consistency level in an offline data center to prevent

Level	Description	Usage
		automatic connection to online nodes in other data centers if an offline node goes down.
ANY	A write must be written to at least one node. If all replica nodes for the given partition key are down, the write can still succeed after a hinted handoff has been written. If all replica nodes are down at write time, an ANY write is not readable until the replica nodes for that partition have recovered.	Provides low latency and a guarantee that a write never fails. Delivers the lowest consistency and highest availability.

Read consistency levels

This table describes read consistency levels in strongest-to-weakest order.

Table: Read Consistency Levels

Level	Description	Usage
ALL	Returns the record after all replicas have responded. The read operation will fail if a replica does not respond.	Provides the highest consistency of all levels and the lowest availability of all levels.
EACH_QUORUM	EACH_QUORUM is not supported for reads.	EACH_QUORUM is not supported for reads.
QUORUM	Returns the record after a quorum of replicas from all datacenters has responded.	Used in either single or multiple data center clusters to maintain strong consistency across the cluster. Ensures strong consistency if you can tolerate some level of failure.
LOCAL_QUORUM	Returns the record after a quorum of replicas in the current data center as the coordinator has reported. Avoids latency of inter-data center communication.	Used in multiple data center clusters with a rack-aware replica placement strategy (<code>NetworkTopologyStrategy</code>) and a properly configured snitch. Fails when using <code>SimpleStrategy</code> .
ONE	Returns a response from the closest replica, as determined by the snitch . By default, a read repair runs in the background to make the other replicas consistent.	Provides the highest availability of all the levels if you can tolerate a comparatively high probability of stale data being read. The replicas contacted for reads may not always have the most recent write.
TWO	Returns the most recent data from two of the closest replicas.	Similar to ONE.
THREE	Returns the most recent data from three of the closest replicas.	Similar to TWO.
LOCAL_ONE	Returns a response from the closest replica in the local data center.	Same usage as described in the table about write consistency levels.
SERIAL	Allows reading the current (and possibly uncommitted) state of data without proposing a new addition or update. If a SERIAL read finds an uncommitted transaction in progress, it will commit the	To read the latest value of a column after a user has invoked a lightweight transaction to write to the column, use SERIAL. Cassandra then checks the inflight

Level	Description	Usage
	transaction as part of the read. Similar to QUORUM.	lightweight transaction for updates and, if found, returns the latest data.
LOCAL_SERIAL	Same as SERIAL, but confined to the data center. Similar to LOCAL_QUORUM.	Used to achieve linearizable consistency for lightweight transactions.

How QUORUM is calculated

The QUORUM level writes to the number of nodes that make up a quorum. A quorum is calculated, and then rounded down to a whole number, as follows:

```
quorum = (sum_of_replication_factors / 2) + 1
```

The sum of all the `replication_factor` settings for each data center is the `sum_of_replication_factors`.

```
sum_of_replication_factors = datacenter1_RF + datacenter2_RF + . . . +
datacentern_RF
```

Examples:

- Using a replication factor of 3, a quorum is 2 nodes. The cluster can tolerate 1 replica down.
- Using a replication factor of 6, a quorum is 4. The cluster can tolerate 2 replicas down.
- In a two data center cluster where each data center has a replication factor of 3, a quorum is 4 nodes. The cluster can tolerate 2 replica nodes down.
- In a five data center cluster where two data centers have a replication factor of 3 and three data centers have a replication factor of 2, a quorum is 7 nodes.

The more data centers, the higher number of replica nodes need to respond for a successful operation.

Similar to QUORUM, the LOCAL_QUORUM level is calculated based on the replication factor of the same data center as the coordinator node. That is, even if the cluster has more than one data center, the quorum is calculated only with local replica nodes.

In EACH_QUORUM, every data center in the cluster must reach a quorum based on that data center's replication factor in order for the read or write request to succeed. That is, for every data center in the cluster a quorum of replica nodes must respond to the coordinator node in order for the read or write request to succeed.

Configuring client consistency levels

You can use a `cqlsh` command, [CONSISTENCY](#), to set the consistency level for queries in the current `cqlsh` session. For programming client applications, set the consistency level using an appropriate driver. For example, call `QueryBuilder.insertInto` with a `setConsistencyLevel` argument using the Java driver.

How is the serial consistency level configured?

Serial consistency levels in Cassandra can be configured to manage lightweight transaction isolation. Lightweight transactions have two consistency levels defined. The serial consistency level defines the consistency level of the serial phase, or Paxos phase, of lightweight transactions. The learn phase, which defines what read operations will be guaranteed to complete immediately if lightweight writes are occurring uses a normal consistency level. The serial consistency level is ignored for any query that is not a conditional update.

Serial consistency levels

Table: Serial Consistency Levels

Level	Description	Usage
SERIAL	Achieves linearizable consistency for lightweight transactions by preventing unconditional updates.	This consistency level is only for use with lightweight transaction. Equivalent to QUORUM.
LOCAL_SERIAL	Same as SERIAL but confined to the data center. A conditional write must be written to the commit log and memtable on a quorum of replica nodes in the same data center.	Same as SERIAL but used to maintain consistency locally (within the single data center). Equivalent to LOCAL_QUORUM.

How are read requests accomplished?

There are three types of read requests that a [coordinator](#) can send to a replica:

- A direct read request
- A digest request
- A background read repair request

The coordinator node contacts one replica node with a direct read request. Then the coordinator sends a digest request to a number of replicas determined by the [consistency level](#) specified by the client. The digest request checks the data in the replica node to make sure it is up to date. Then the coordinator sends a digest request to all remaining replicas. If any replica nodes have out of date data, a background [read repair](#) request is sent. Read repair requests ensure that the requested row is made consistent on all replicas.

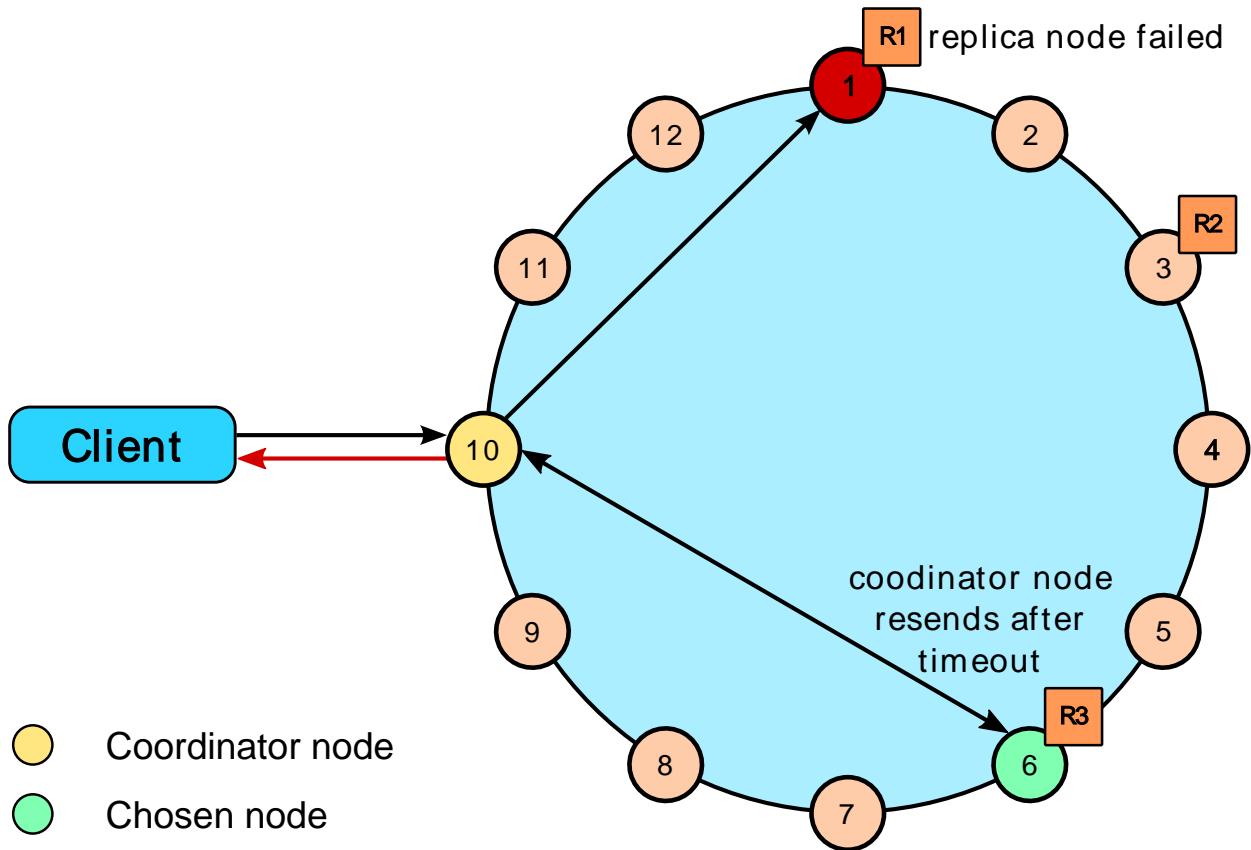
For a digest request the coordinator first contacts the replicas specified by the consistency level. The coordinator sends these requests to the replicas that are currently responding the fastest. The nodes contacted respond with a digest of the requested data; if multiple nodes are contacted, the rows from each replica are compared in memory to see if they are consistent. If they are not, then the replica that has the most recent data (based on the timestamp) is used by the coordinator to forward the result back to the client. To ensure that all replicas have the most recent version of the data, read repair is carried out to update out-of-date replicas.

For illustrated examples of read requests, see the [examples of read consistency levels](#).

Rapid read protection using speculative_retry

Rapid read protection allows Cassandra to still deliver read requests when the originally selected replica nodes are either down or taking too long to respond. If the table has been configured with the [speculative_retry](#) property, the coordinator node for the read request will retry the request with another replica node if the original replica node exceeds a configurable timeout value to complete the read request.

Figure: Recovering from replica node failure with rapid read protection



Examples of read consistency levels

The following diagrams show examples of read requests using these consistency levels:

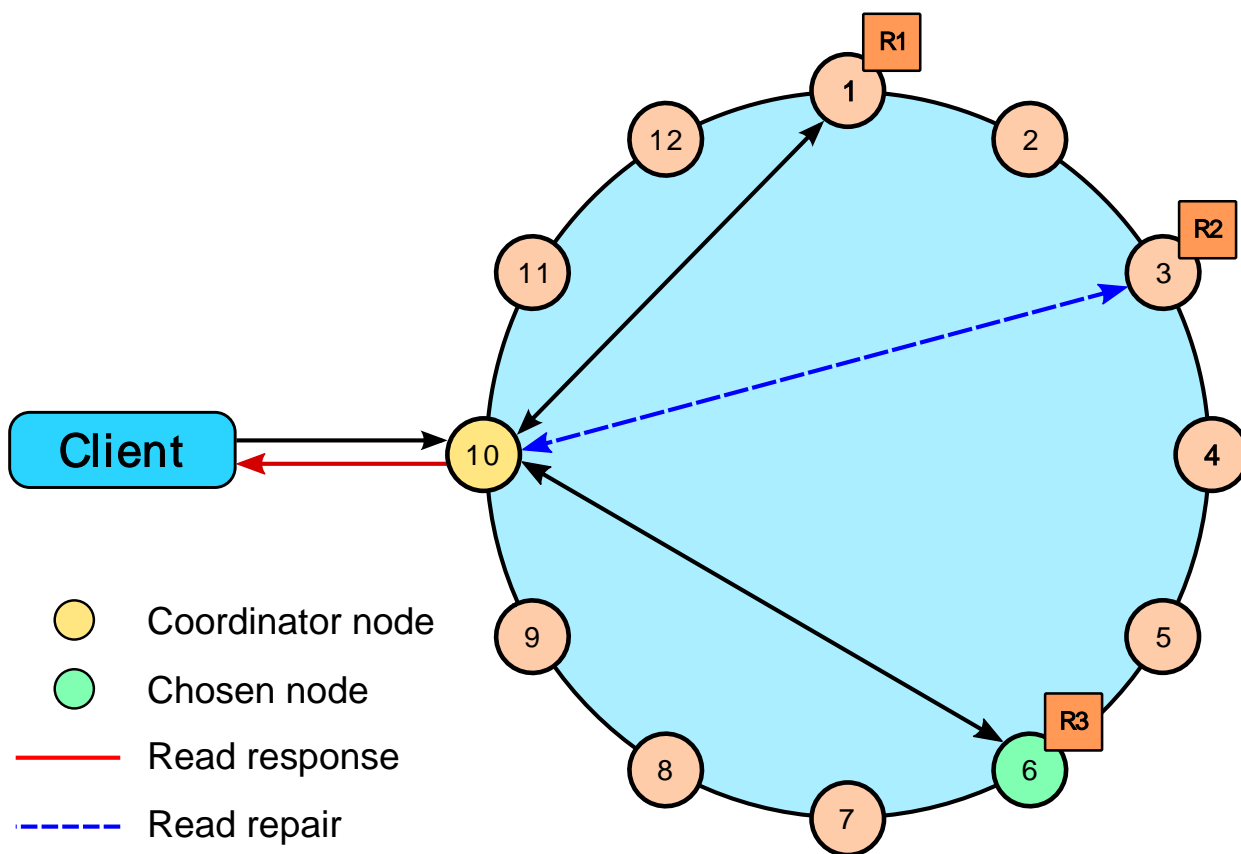
- QUORUM in a single data center
- ONE in a single data center
- QUORUM in two data centers
- LOCAL_QUORUM in two data centers
- ONE in two data centers
- LOCAL_ONE in two data centers

[Rapid read protection diagram](#) shows how the speculative retry table property affects consistency.

A single data center cluster with a consistency level of QUORUM

In a single data center cluster with a replication factor of 3, and a read consistency level of `QUORUM`, 2 of the 3 replicas for the given row must respond to fulfill the read request. If the contacted replicas have different versions of the row, the replica with the most recent version will return the requested data. In the background, the third replica is checked for consistency with the first two, and if needed, a read repair is initiated for the out-of-date replicas.

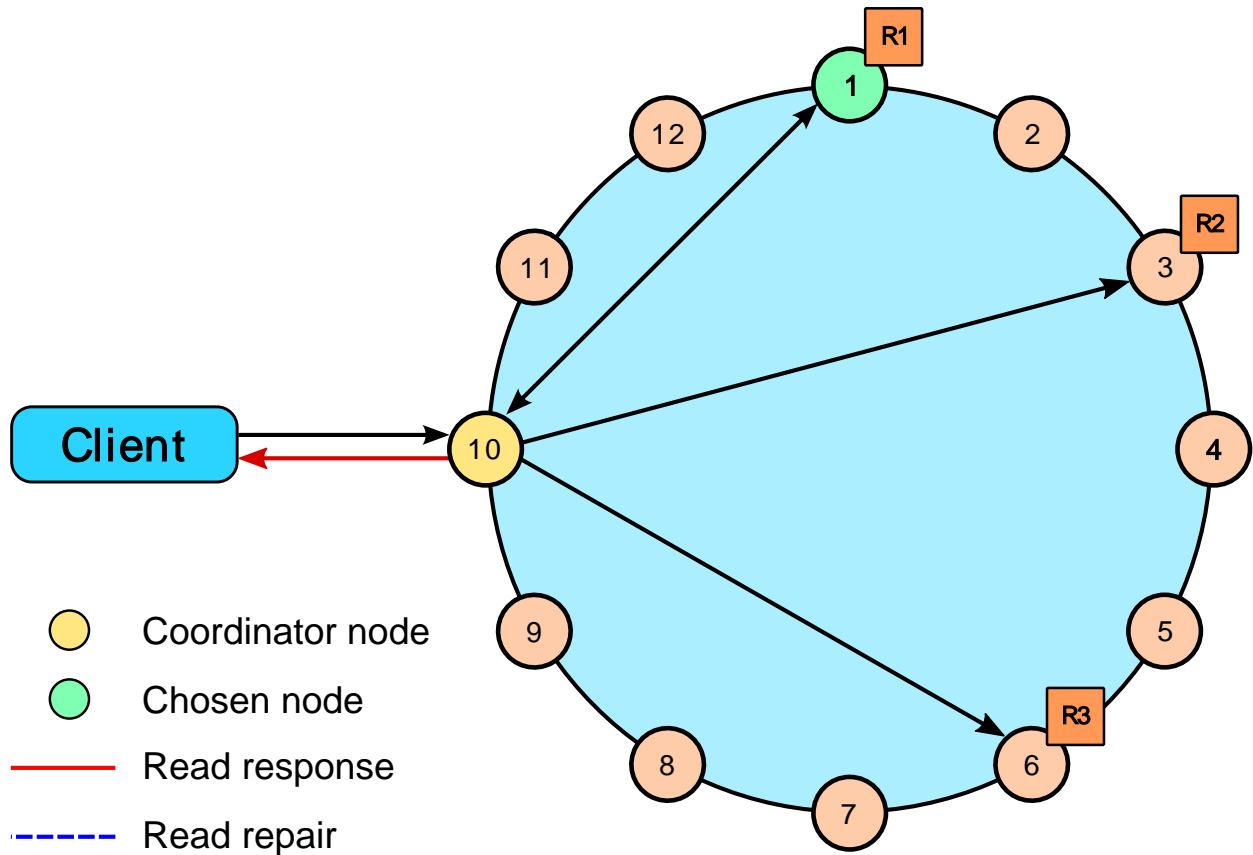
Figure: Single data center cluster with 3 replica nodes and consistency set to QUORUM



A single data center cluster with a consistency level of ONE

In a single data center cluster with a replication factor of 3, and a read consistency level of `ONE`, the closest replica for the given row is contacted to fulfill the read request. In the background a read repair is potentially initiated, based on the `read_repair_chance` setting of the table, for the other replicas.

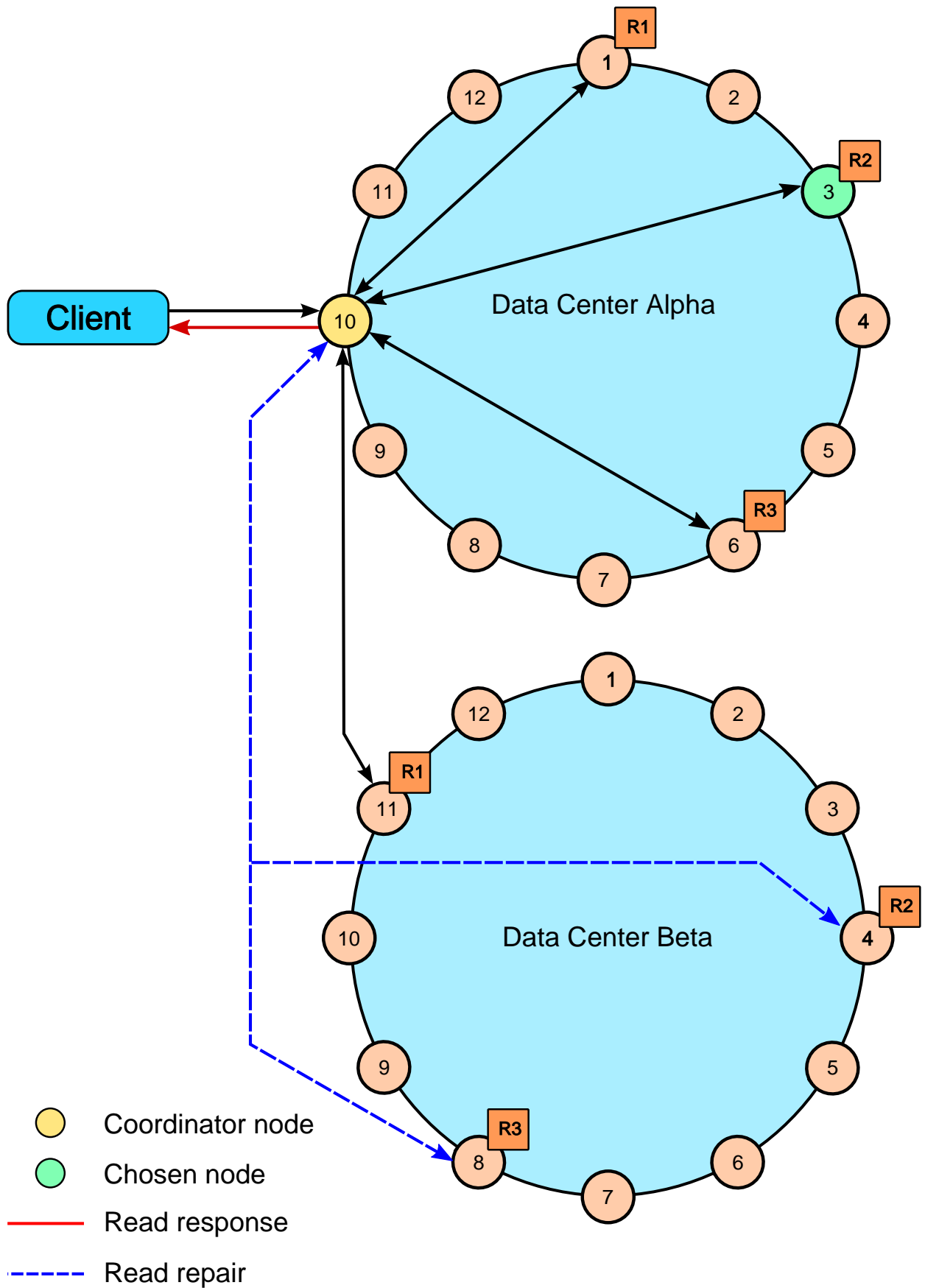
Figure: Single data center cluster with 3 replica nodes and consistency set to ONE



A two data center cluster with a consistency level of QUORUM

In a two data center cluster with a replication factor of 3, and a read consistency of `QUORUM`, 4 replicas for the given row must respond to fulfill the read request. The 4 replicas can be from any data center. In the background, the remaining replicas are checked for consistency with the first four, and if needed, a read repair is initiated for the out-of-date replicas.

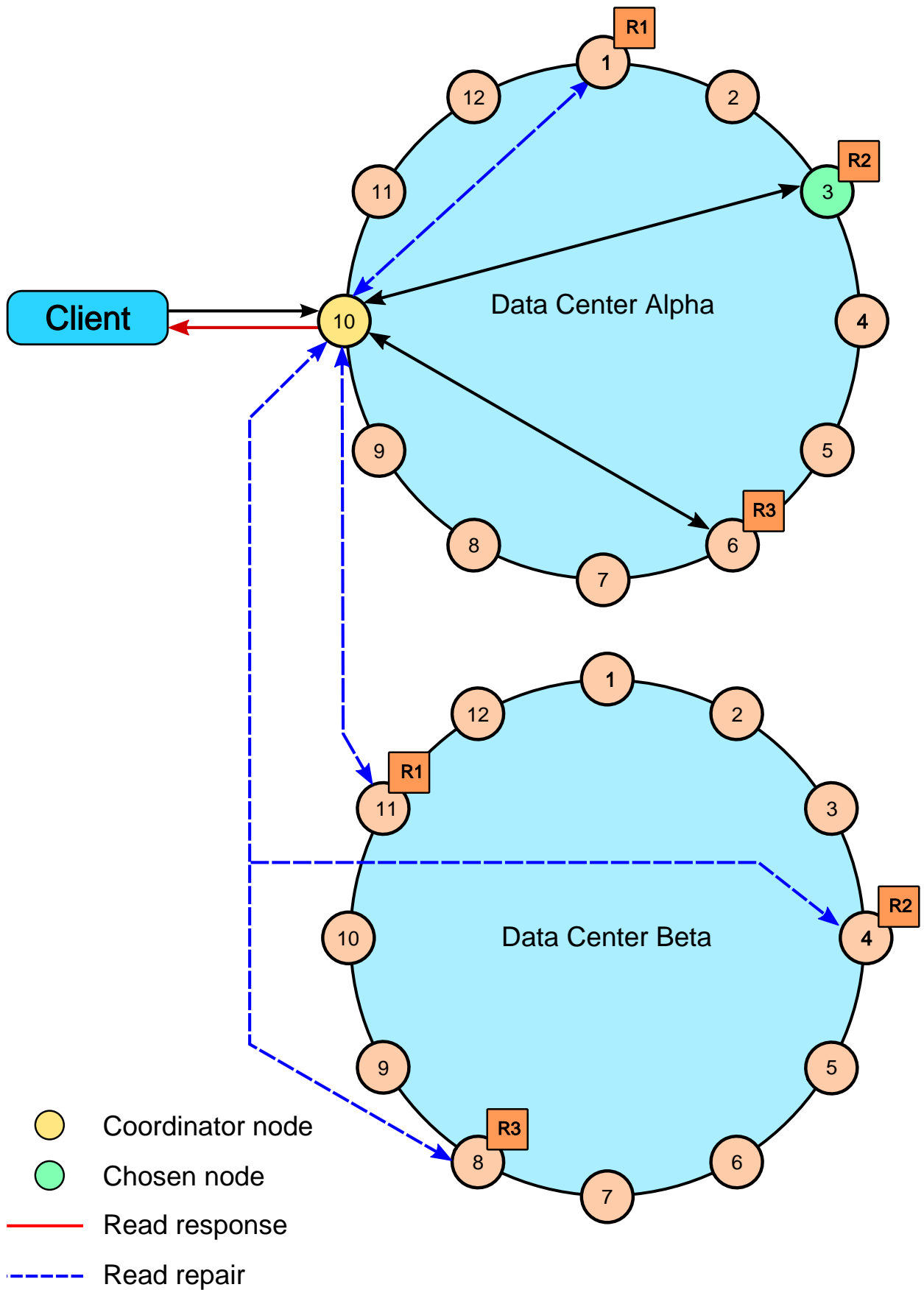
Figure: Multiple data center cluster with 3 replica nodes and consistency level set to QUORUM



A two data center cluster with a consistency level of LOCAL_QUORUM

In a multiple data center cluster with a replication factor of 3, and a read consistency of `LOCAL_QUORUM`, 2 replicas in the same data center as the coordinator node for the given row must respond to fulfill the read request. In the background, the remaining replicas are checked for consistency with the first 2, and if needed, a read repair is initiated for the out-of-date replicas.

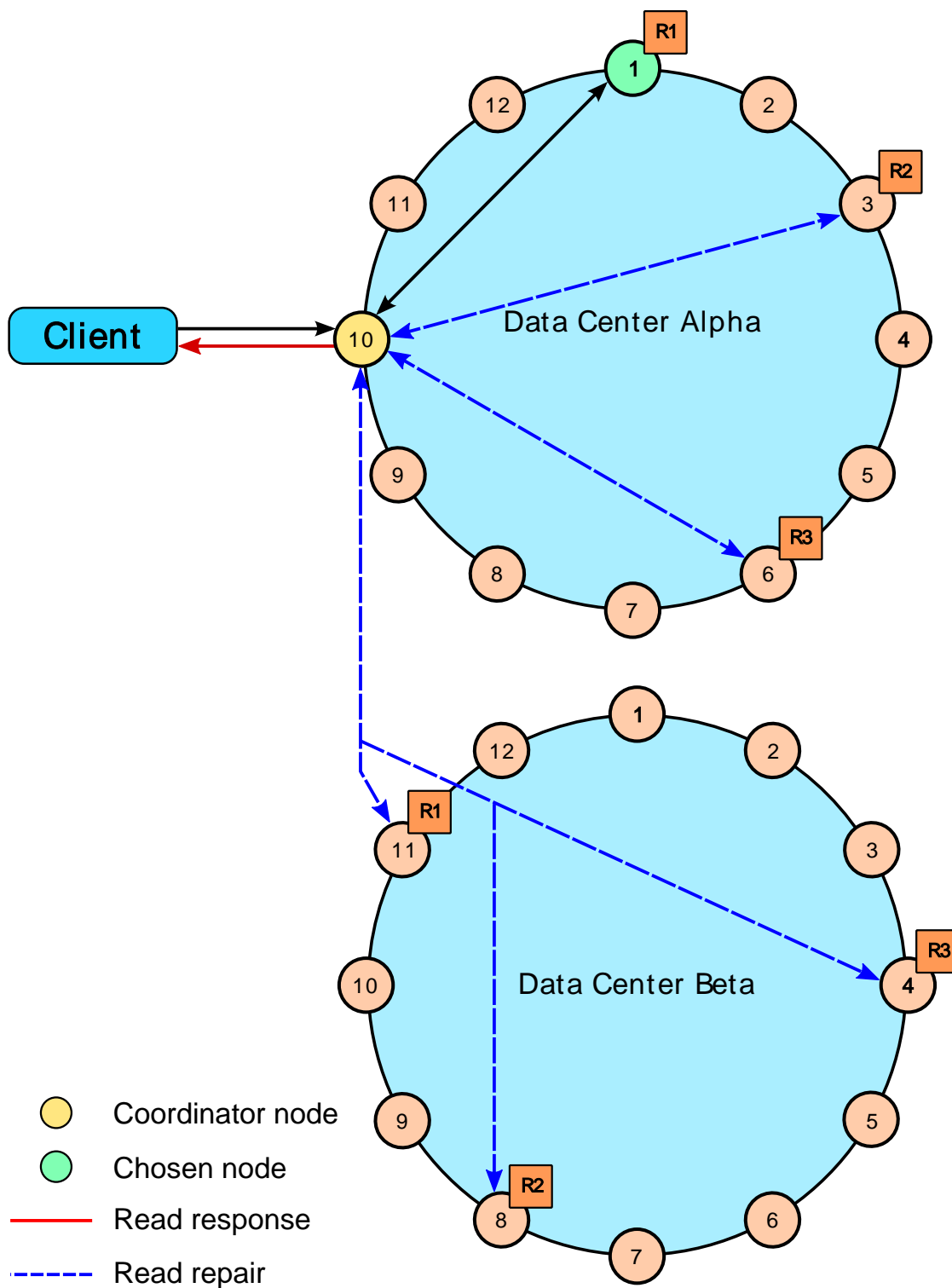
Figure: Multiple data center cluster with 3 replica nodes and consistency set to `LOCAL_QUORUM`



A two data center cluster with a consistency level of ONE

In a multiple data center cluster with a replication factor of 3, and a read consistency of ONE, the closest replica for the given row, regardless of data center, is contacted to fulfill the read request. In the background a read repair is potentially initiated, based on the `read_repair_chance` setting of the table, for the other replicas.

Figure: Multiple data center cluster with 3 replica nodes and consistency set to ONE

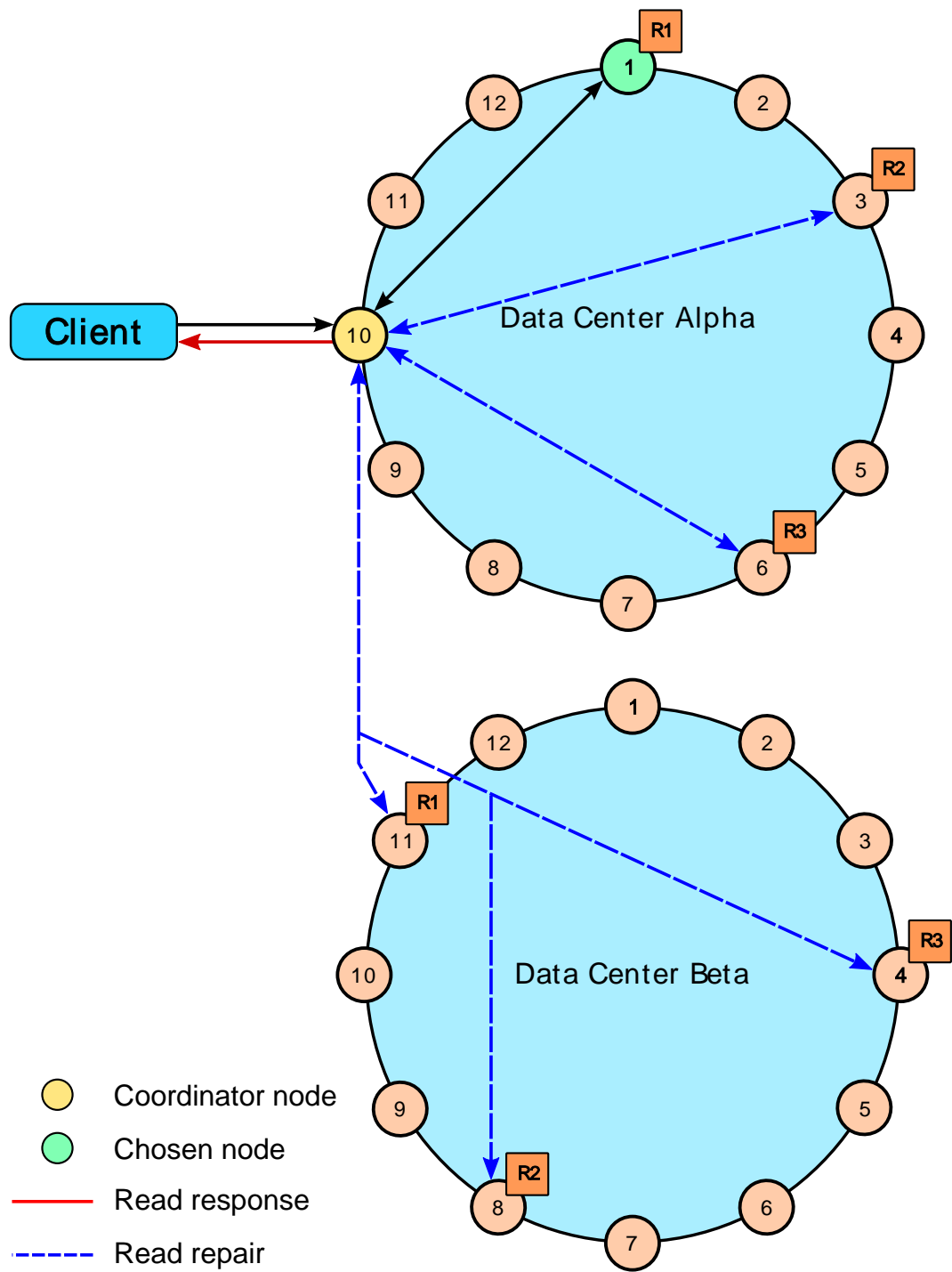


A two data center cluster with a consistency level of `LOCAL_ONE`

In a multiple data center cluster with a replication factor of 3, and a read consistency of `LOCAL_ONE`, the closest replica for the given row in the same data center as the coordinator node is contacted to fulfill the

read request. In the background a read repair is potentially initiated, based on the `read_repair_chance` setting of the table, for the other replicas.

Figure: Multiple data center cluster with 3 replica nodes and consistency set to LOCAL_ONE



How are write requests accomplished?

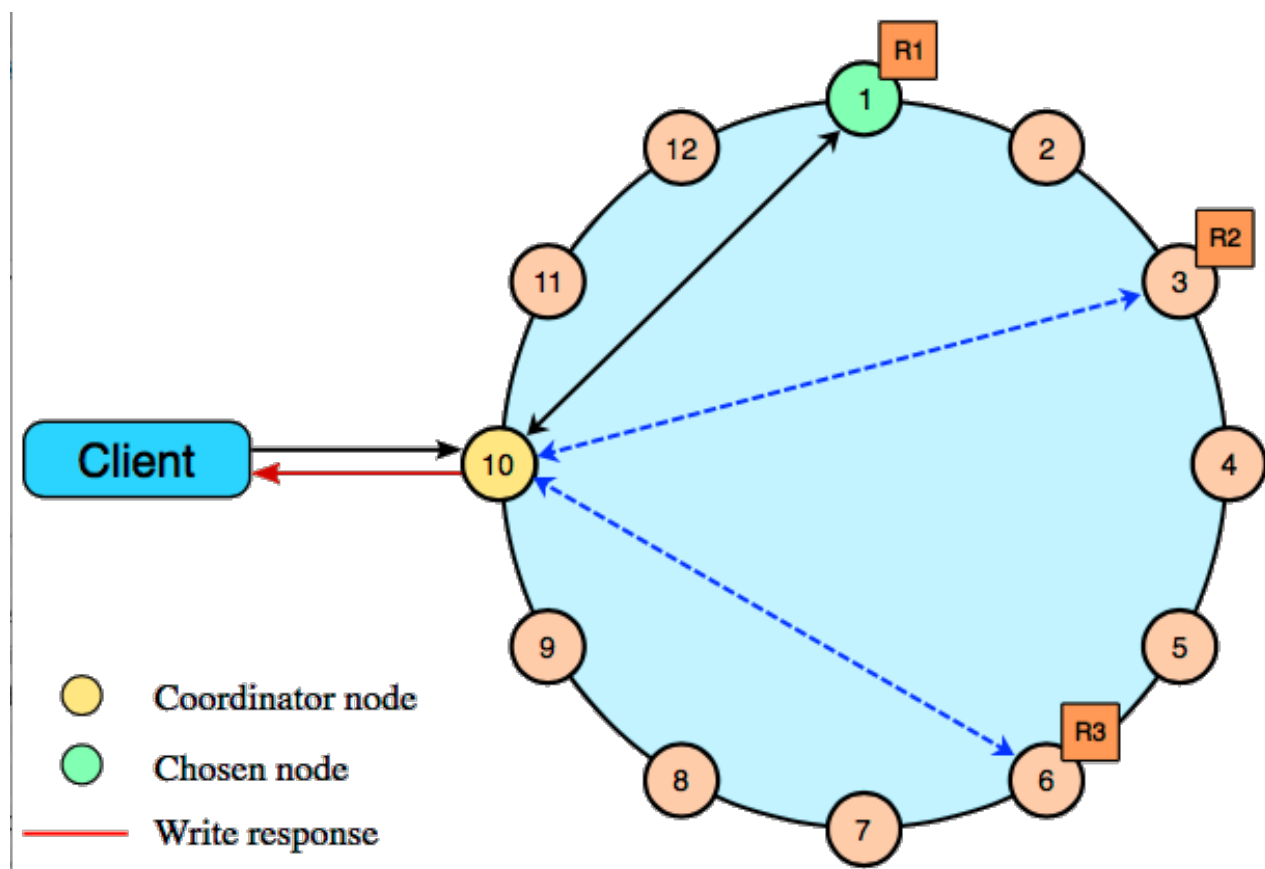
The coordinator sends a write request to *all* replicas that own the row being written. As long as all replica nodes are up and available, they will get the write regardless of the [consistency level](#) specified by the client. The write consistency level determines how many replica nodes must respond with a success acknowledgment in order for the write to be considered successful. Success means that the data was written to the commit log and the memtable as described in [how data is written](#).

For example, in a single data center 10 node cluster with a replication factor of 3, an incoming write will go to all 3 nodes that own the requested row. If the write consistency level specified by the client is ONE, the first node to complete the write responds back to the coordinator, which then proxies the success message back to the client. A consistency level of ONE means that it is possible that 2 of the 3 replicas could miss the write if they happened to be down at the time the request was made. If a replica misses a write, Cassandra will make the row consistent later using one of its [built-in repair mechanisms](#): hinted handoff, read repair, or anti-entropy node repair.

That node forwards the write to all replicas of that row. It responds to the client once it receives write acknowledgments from the number of nodes specified by the consistency level. Exceptions:

- If the coordinator cannot write to enough replicas to meet the requested Consistency level, it throws an `Unavailable` Exception and does not perform any writes.
- If there are enough replicas available but the required writes don't finish within the timeout window, the coordinator throws a `Timeout` Exception.

Figure: Single data center cluster with 3 replica nodes and consistency set to ONE

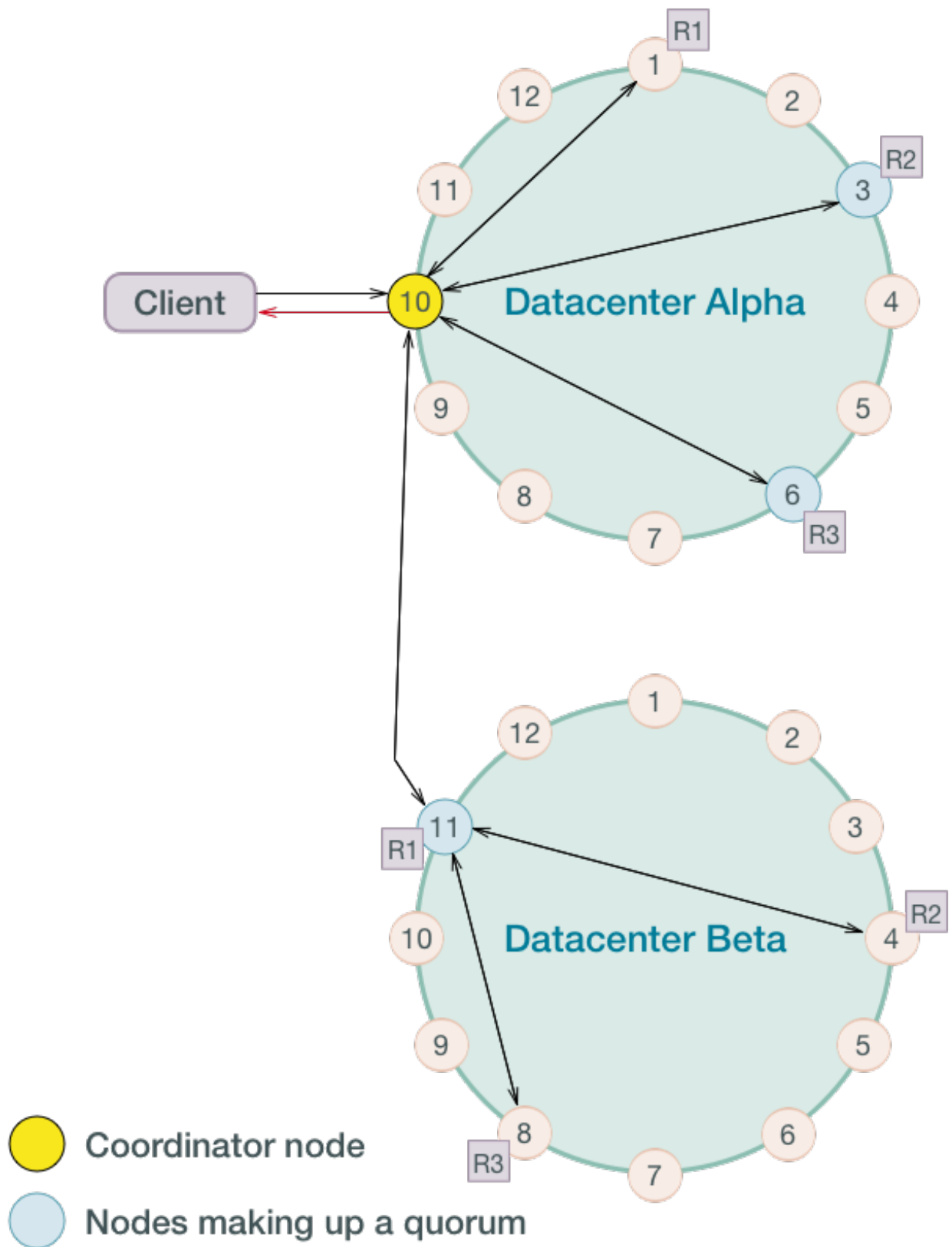


Multiple data center write requests

In multiple data center deployments, Cassandra optimizes write performance by choosing one coordinator node. The coordinator node contacted by the client application forwards the write request to one replica in each of the other DCs, with a special tag to forward the write to the other local replicas.

If the [consistency level](#) is `LOCAL_ONE` or `LOCAL_QUORUM`, only the nodes in the same data center as the coordinator node must respond to the client request in order for the request to succeed. This way, geographical latency does not impact client request response times.

Figure: Multiple data center cluster with 3 replica nodes and consistency set to QUORUM



Planning a cluster deployment

Planning has moved to [Planning and testing cluster deployments](#).

Installing DataStax Distribution of Apache Cassandra 3.x for Windows

Installing DataStax Distribution of Apache Cassandra 3.x for Windows

Attention: OpsCenter is not supported or installed with Apache Cassandra 3.0 2.2 and later.

Prerequisites

- Ensure that your platform is [supported](#).
- If you are using a 32-bit systems, make sure it has the Visual C++ 2008 runtime ([Microsoft Visual C++ 2008 Redistributable Package \(x86\)](#)) installed.
- Make sure it is running the latest version of [Java 8](#).

Note: From Windows PowerShell, set the execution policy to unrestricted from an elevated command-prompt:

```
Set-ExecutionPolicy Unrestricted
```

Procedure

1. Download the Windows MSI installer for your platform from [Planet Cassandra](#).

Note: 32-bit systems are for development only.

2. Follow the setup wizard to install.

The installation wizard lets you set up the Datastax services to start automatically when the installation completes, and whenever the computer reboots. If you select this option, the services start automatically – you can skip the next step.

3. If you did not elect to have Datastax services start automatically, start Cassandra by entering the following:

```
C:\> net start DataStax_DDC_Server
```

4. To verify that DataStax Distribution of Apache Cassandra 3.x for Windows is running, use the nodetool status command:
For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool status
```

```
Datacenter: datacenter1
=====
```

```
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load        Tokens      Owns    Host ID
   Rack
UN  127.0.0.1    133.97 KB   256         ?
    16e04c6b-5d43-4372-9e71-7acdcaa023bc rack1
```

What to do next

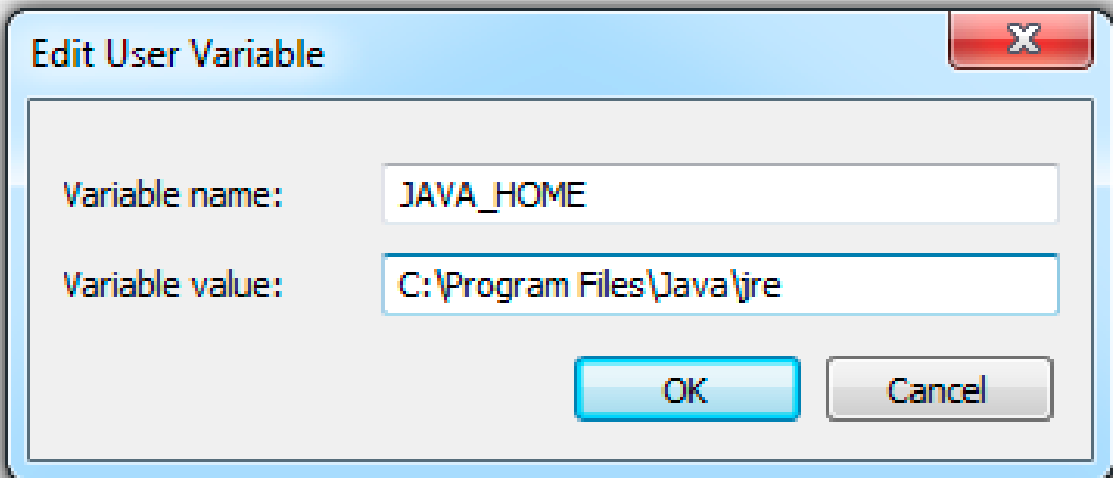
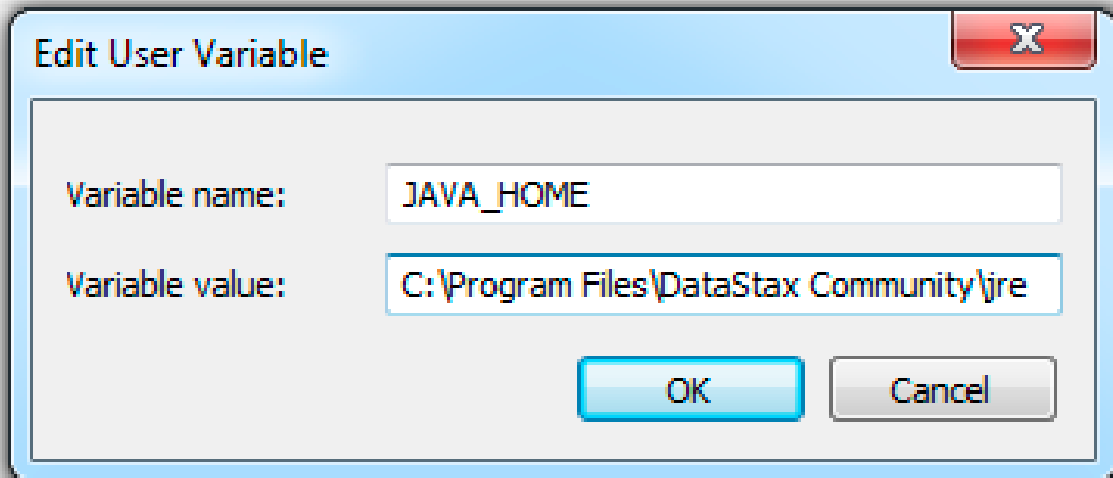
- [Configure the DataStax Distribution of Apache Cassandra](#)
- [Initializing a cluster](#) on page 102
- [Recommended production settings](#)
- [Key components for configuring Cassandra](#)
- [Installation locations](#)
- [Starting or stopping Cassandra](#)

Windows troubleshooting

What to do if Cassandra services do not start.

Procedure

- If Cassandra does not start, check that the `JAVA_HOME` environmental variable points to either of the following (Cassandra 3.0 and later requires Java 8):



Installing earlier releases of DataStax Distribution of Apache Cassandra 3.x for Windows

Download the previous version you want from [Planet Cassandra](#) and follow the install instructions for that version.

Uninstalling DataStax Distribution of Apache Cassandra 3.x for Windows

To uninstall:

1. Use either:
 - **Uninstall DataStax Distribution of Apache Cassandra** on the **Start** menu
 - **Windows Uninstall a program** on the **Control Panel**
2. To remove any remaining files, delete the C:\Program Files\DataStax-DDC folder.

```
C:\> rmdir /s "Program Files\DataStax-DDC"
```

Installing on cloud providers

You can install Cassandra on cloud providers that supply any of the [supported platforms](#).

You can install Cassandra 2.1 and earlier versions on Amazon EC2 using the DataStax AMI (Amazon Machine Image) as described in the [AMI documentation](#) for Cassandra 2.1.

To install Cassandra 2.2 and later on Amazon EC2, use a [trusted AMI](#) for your platform and the appropriate [install method](#) for that platform.

Recommended production settings for Linux and Windows

Recommendations for production environments have been moved to [Recommended production settings](#).

Windows installation directories

The configuration files are located in the following directories:

Configuration Files	Locations	Description
cassandra.yaml	Program Files\DataStax-DDC\apache-cassandra\conf\cassandra.yaml	Main configuration file.
cassandra-env.ps1	Program Files\DataStax-DDC\apache-cassandra\conf\cassandra-env.ps1	Windows settings for Java, some JVM, and JMX.
jvm.options	Program Files\DataStax-DDC\apache-cassandra\conf\jvm.options	Static JVM settings for heap, garbage collection, and Cassandra startup parameters.
cassandra-rackdc.properties	Program Files\DataStax-DDC\apache-cassandra\conf\cassandra-rackdc.properties	Defines the default data center and rack used by the GossipingPropertyFileSnitch, Ec2Snitch, Ec2MultiRegionSnitch, and GoogleCloudSnitch.
cassandra.in.bat	Program Files\DataStax-DDC\apache-cassandra\bin	Sets environment variables.
cassandra-topology.properties	Program Files\DataStax-DDC\apache-cassandra\conf\cassandra-topology.properties	Defines the default data center and rack used by the PropertyFileSnitch.

Configuration Files	Locations	Description
<code>commit_archiving.properties</code>	<code>Program Files\DataStax-DDC\apache-cassandra\conf\commitlog_archiving.properties</code>	Configures commitlog archiving.
<code>cqlshrc.sample</code>	<code>Program Files\DataStax-DDC\apache-cassandra\conf\cqlshrc.sample</code>	Example file for using cqlsh with SSL encryption.
<code>metrics-reporter-config-sample.yaml</code>	<code>Program Files\DataStax-DDC\apache-cassandra\conf\metrics-reporter-config-sample.yaml</code>	Example file for configuring metrics in Cassandra.
<code>logback.xml</code>	<code>Program Files\DataStax-DDC\apache-cassandra\conf\logback.xml</code>	Configuration file for logback.
<code>triggers</code>	<code>Program Files\DataStax-DDC\apache-cassandra\conf\triggers</code>	The default location for the trigger JARs.

The Windows releases install into these directories:

Directories	Description
<code>Program Files\DataStax-DDC\apache-cassandra\bin</code>	Utilities and start scripts.
<code>Program Files\DataStax-DDC\apache-cassandra\conf</code>	Configuration files and sample files.
<code>Program Files\DataStax-DDC\data</code>	Files for commitlog, data, and saved_caches (unless set in <code>cassandra.yaml</code>)
<code>Program Files\DataStax-DDC\apache-cassandra\interface</code>	Thrift.
<code>Program Files\DataStax-DDC\jre</code>	Run-time support files for Java.
<code>Program Files\DataStax-DDC\log</code>	Log files.
<code>Program Files\DataStax-DDC\python</code>	Run-time support for Python. Python is used for cqlsh.
<code>Program Files\DataStax-DDC\apache-cassandra\lib</code>	JAR and license files.
<code>Program Files\DataStax-DDC\utils</code>	Utilities and Java support classes for running Java applications as server processes.

For DataStax Enterprise installs, see the documentation for your DataStax Enterprise version.

Configuration

The cassandra.yaml configuration file

The `cassandra.yaml` file is the main configuration file for Cassandra.

Important: After changing properties in the `cassandra.yaml` file, you must restart the node for the changes to take effect. It is located in `C:\Program Files\DataStax-DDC\apache-cassandra\conf\cassandra.yaml`.

The configuration properties are grouped into the following sections:

- [Quick start](#)

The minimal properties needed for configuring a cluster.

- [Commonly used](#)

Properties most frequently used when configuring Cassandra.

- [Performance tuning](#)

Tuning performance and system resource utilization, including commit log, compaction, memory, disk I/O, CPU, reads, and writes.

- [Advanced](#)

Properties for advanced users or properties that are less commonly used.

- [Security](#)

Server and client security settings.

Note: Values with ^{note} indicate default values that are defined internally, missing, commented out, or implementation depends on other properties in the `cassandra.yaml` file. Additionally, some commented out values may not match the actual default value; these values are recommended when changing from the default.

Quick start properties

The minimal properties needed for configuring a cluster.

Related information: [Initializing a multiple node cluster \(single data center\)](#) on page 102 and [Initializing a multiple node cluster \(multiple data centers\)](#) on page 105.

cluster_name

(Default: Test Cluster) 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.

listen_address

(Default: localhost) The IP address or hostname that Cassandra binds to for connecting to other Cassandra nodes. Set this parameter or [listen_interface](#), not both. You must change the default setting for multiple nodes to communicate:

- Generally set to empty. If the node is properly configured (host name, name resolution, and so on), Cassandra uses `InetAddress.getLocalHost()` to get the local address from the system.
- For a single node cluster, you can use the default setting (localhost).
- If Cassandra can't find the correct address, you must specify the IP address or host name.
- Never specify 0.0.0.0; it is always wrong.
- If you use multiple physical network interfaces, set both `listen_address` and [listen_on_broadcast_address](#) to true.

listen_interface

(Default: eth0)^{note} The interface that Cassandra binds to for connecting to other Cassandra nodes. Interfaces must correspond to a single address, IP aliasing is not supported. See [listen_address](#).

listen_interface_prefer_ipv6

(Default: false) By default, if an interface has an ipv4 and an ipv6 address, the first ipv4 address will be used. If set to true, the first ipv6 address will be used.

Default directories

If you have changed any of the default directories during installation, make sure you have root access and set these properties:

commitlog_directory

The directory where the commit log is stored. Default locations:

For optimal write performance, place the commit log be on a separate disk partition, or (ideally) a separate physical device from the data file directories. Because the commit log is append only, an HDD is acceptable for this purpose.

data_file_directories

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

As a production best practice, use [RAID 0 and SSDs](#).

saved_caches_directory

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

- Windows 3.x installations: C:\Program Files\DataStax-DDC\data\saved_caches

Commonly used properties

Properties most frequently used when configuring Cassandra.

Before starting a node for the first time, you should carefully evaluate your requirements.

Common initialization properties

Note: Be sure to set the properties in the [Quick start section](#) as well.

commit_failure_policy

(Default: stop) Policy for commit disk failures:

- die
Shut down gossip and Thrift and kill the JVM, so the node can be replaced.
- stop
Shut down gossip and Thrift, leaving the node effectively dead, but can be inspected using JMX.
- stop_commit
Shut down the commit log, letting writes collect but continuing to service reads (as in pre-2.0.5 Cassandra).
- ignore
Ignore fatal errors and let the batches fail.

disk_optimization_strategy

(Default: ssd) The strategy for optimizing disk reads can be set to either ssd or spinning.

disk_failure_policy

(Default: stop) Sets how Cassandra responds to disk failure. Recommend settings are stop or best_effort.

- die
Shut down gossip and Thrift and kill the JVM for any file system errors or single SSTable errors, so the node can be replaced.
- stop_paranoid

Shut down gossip and Thrift even for single SSTable errors.

- stop

Shut down gossip and Thrift, leaving the node effectively dead, but available for inspection using JMX.

- best_effort

Stop using the failed disk and respond to requests based on the remaining available SSTables. This means you will see obsolete data at consistency level of ONE.

- ignore

Ignores fatal errors and lets the requests fail; all file system errors are logged but otherwise ignored. Cassandra acts as in versions prior to 1.2.

Related information: [Handling Disk Failures In Cassandra 1.2](#) blog and [Recovering from a single disk failure using JBOD](#) on page 123.

endpoint_snitch

(Default: `org.apache.cassandra.locator.SimpleSnitch`) Set to a class that implements the `IEndpointSnitch` interface. Cassandra uses snitches for locating nodes and routing requests.

- SimpleSnitch

Use for single-data center deployments or single-zone in public clouds. Does not recognize data center or rack information. It treats strategy order as proximity, which can improve cache locality when disabling read repair.

- GossipingPropertyFileSnitch

Recommended for production. The rack and data center for the local node are defined in the `cassandra-rackdc.properties` file and propagated to other nodes via gossip. To allow migration from the `PropertyFileSnitch`, it uses the `cassandra-topology.properties` file if it is present.

- PropertyFileSnitch

Determines proximity by rack and data center, which are explicitly configured in the `cassandra-topology.properties` file.

- Ec2Snitch

For EC2 deployments in a single region. Loads region and availability zone information from the Amazon EC2 API. The region is treated as the data center and the availability zone as the rack and uses only private IPs. Subsequently it does not work across multiple regions.

- Ec2MultiRegionSnitch

Uses public IPs as the [broadcast_address](#) to allow cross-region connectivity. This means you must also set [seed](#) addresses to the public IP and open the [storage_port](#) or [ssl_storage_port](#) on the public IP firewall. For intra-region traffic, Cassandra switches to the private IP after establishing a connection.

- RackInferringSnitch:

Proximity is determined by rack and data center, which are assumed to correspond to the 3rd and 2nd octet of each node's IP address, respectively. This snitch is best used as an example for writing a custom snitch class (unless this happens to match your deployment conventions).

- GoogleCloudSnitch:

Use the `GoogleCloudSnitch` for Cassandra deployments on [Google Cloud Platform](#) across one or more regions. The region is treated as a data center and the availability zones are treated as racks within the data center. All communication occurs over private IP addresses within the same logical network.

- CloudstackSnitch

Use the `CloudstackSnitch` for [Apache Cloudstack](#) environments.

Related information: [Snitches](#) on page 19

rpc_address

Configuration

(Default: localhost) The listen address for client connections (Thrift RPC service and native transport). Valid values are:

- unset:
Resolves the address using the hostname configuration of the node. If left unset, the hostname must resolve to the IP address of this node using `C:\WINDOWS\system32\drivers\etc\hosts`, or DNS.
- 0.0.0.0:
Listens on all configured interfaces, but you must set the [broadcast_rpc_address](#) to a value other than 0.0.0.0.
- IP address
- hostname

Related information: [Network](#)

rpc_interface

(Default: eth1)^{note} The listen address for client connections. Interfaces must correspond to a single address, IP aliasing is not supported. See [rpc_address](#).

rpc_interface_prefer_ipv6

(Default: false) By default, if an interface has an ipv4 and an ipv6 address, the first ipv4 address will be used. If set to true, the first ipv6 address will be used.

seed_provider

The addresses of hosts deemed contact points. Cassandra nodes use the -seeds list to find each other and learn the topology of the ring.

- class_name (Default: `org.apache.cassandra.locator.SimpleSeedProvider`)
The class within Cassandra that handles the seed logic. It can be customized, but this is typically not required.
- - seeds (Default: 127.0.0.1)
A comma-delimited list of IP addresses used by [gossip](#) for bootstrapping new nodes joining a cluster. When running multiple nodes, you must change the list from the default value. In multiple data-center clusters, it is a good idea to include at least one node from each data center (replication group) in the seed list. Designating 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 it is recommended to use a small seed list (approximately three nodes per data center).

Related information: [Initializing a multiple node cluster \(single data center\)](#) on page 102 and [Initializing a multiple node cluster \(multiple data centers\)](#) on page 105.

enable_user_defined_functions

(Default: false) User defined functions (UDFs) present a security risk, since they are executed on the server side. In Cassandra 3.0 and later, UDFs are executed in a sandbox to contain the execution of malicious code. They are disabled by default.

enable_scripted_user_defined_functions

(Default: false) Java UDFs are always enabled, if `enable_user_defined_functions` is true. Enable this option to use UDFs with language `javascript` or any custom JSR-223 provider. This option has no effect, if `enable_user_defined_functions` is false.

Common compaction settings

compaction_throughput_mb_per_sec

(Default: 16) Throttles compaction to the specified total throughput across the instance. The faster you insert data, the faster you need to compact in order to keep the SSTable count down. The recommended value

is 16 to 32 times the rate of write throughput (in Mb/second). Setting the value to 0 disables compaction throttling.

Related information: [Configuring compaction](#) on page 144

compaction_large_partition_warning_threshold_mb

(Default: 100) Logs a warning when compacting partitions larger than the set value.

Common memtable settings

memtable_heap_space_in_mb

(Default: 1/4 of heap size)^{note}

Sets the amount of on-heap memory allocated for memtables. Cassandra uses the total of this amount and the value of `memtable_offheap_space_in_mb` to determine when to flush memtables automatically. For details, see [memtable_cleanup_threshold](#).

Related information: [Tuning the Java heap](#)

memtable_offheap_space_in_mb

(Default: 1/4 of heap size)^{note}

Sets the total amount of off-heap memory allocated for memtables. Cassandra uses the total of this amount and the value of `memtable_heap_space_in_mb` to determine when to flush memtables automatically. For details, see [memtable_cleanup_threshold](#).

Related information: [Tuning the Java heap](#)

Common disk settings

concurrent_reads

(Default: 32)^{note} For workloads with more data than can fit in memory, the bottleneck is reads fetching data from disk. Setting to $(16 \times \text{number_of_drives})$ allows operations to queue low enough in the stack so that the OS and drives can reorder them. The default setting applies to both logical volume managed (LVM) and RAID drives.

concurrent_writes

(Default: 32)^{note} Writes in Cassandra are rarely I/O bound, so the ideal number of concurrent writes depends on the number of CPU cores in your system. The recommended value is $8 \times \text{number_of_cpu_cores}$.

concurrent_counter_writes

(Default: 32)^{note} Counter writes read the current values before incrementing and writing them back. The recommended value is $(16 \times \text{number_of_drives})$.

concurrent_batchlog_writes

(Default: 32) Limit the concurrent batchlog writes, similar to `concurrent_writes`.

concurrent_materialized_view_writes

(Default: 32) Limit the concurrent materialize view writes to the lesser of concurrent reads or concurrent writes, because there is a read involved in materialized view writes.

Common automatic backup settings

incremental_backups

(Default: false) Backs up data updated since the last snapshot was taken. When enabled, Cassandra creates a hard link to each SSTable flushed or streamed locally in a `backups/` subdirectory of the keyspace data. Removing these links is the operator's responsibility.

Related information: [Enabling incremental backups](#) on page 121

snapshot_before_compaction

(Default: false) Enable or disable taking a snapshot before each compaction. This option is useful to back up data when there is a data format change. Be careful using this option because Cassandra does not clean up older snapshots automatically.

Related information: [Configuring compaction](#) on page 144

Common fault detection setting

phi_convict_threshold

(Default: 8)^{note} Adjusts the sensitivity of the failure detector on an exponential scale. Generally this setting never needs adjusting.

Related information: [Failure detection and recovery](#) on page 13

Performance tuning properties

Tuning performance and system resource utilization, including commit log, compaction, memory, disk I/O, CPU, reads, and writes.

Commit log settings

commitlog_sync

(Default: periodic) The method that Cassandra uses to acknowledge writes in milliseconds:

- periodic: (Default: 10000 milliseconds [10 seconds])
Used with `commitlog_sync_period_in_ms` to control how often the commit log is synchronized to disk. Periodic syncs are acknowledged immediately.
- batch: (Default: disabled)^{note}
Used with `commitlog_sync_batch_window_in_ms` (Default: 2 ms) to control how long Cassandra waits for other writes before performing a sync. When using this method, writes are not acknowledged until fsynced to disk.

commitlog_segment_size_in_mb

(Default: 32MB) Sets the size of the individual commitlog file segments. A commitlog segment may be archived, deleted, or recycled after all its data has been flushed to SSTables. This amount of data can potentially include commitlog segments from every table in the system. The default size is usually suitable for most commitlog archiving, but if you want a finer granularity, 8 or 16 MB is reasonable.

This property determines the maximum mutation size, defined as half the segment size. If a mutation's size exceeds the maximum mutation size, the mutation is rejected. Before increasing the commitlog segment size of the commitlog segments, investigate why the mutations are larger than expected. Look for underlying issues with access patterns and data model, because increasing the commitlog segment size is a limited fix.

Related information: [Commit log archive configuration](#) on page 99

max_mutation_size_in_kb

This property is independently configurable. For more information, see [commitlog_segment_size_in_mb](#) above.

commitlog_compression

(Default: not enabled) Sets the compressor to use if commit log is compressed. Options are: LZ4, Snappy or Deflate. The commit log is written uncompressed if a compressor option is not set.

commitlog_total_space_in_mb

(Default: 32MB for 32-bit JVMs, 8192MB for 64-bit JVMs)^{note} Total space used for commit logs. If the used space goes above this value, Cassandra rounds up to the next nearest segment multiple and flushes memtables to disk for the oldest commitlog segments, removing those log segments. This reduces the amount of data to replay on start-up, and prevents infrequently-updated tables from indefinitely keeping commitlog segments. A small total commitlog space tends to cause more flush activity on less-active tables.

Related information: [Configuring memtable thresholds](#) on page 144

Compaction settings

Related information: [Configuring compaction](#) on page 144

concurrent_compactors

(Default: Smaller of number of disks or number of cores, with a minimum of 2 and a maximum of 8 per CPU core)^{note} Sets the number of concurrent compaction processes allowed to run simultaneously on a node, not including validation [compactions](#) for [anti-entropy](#) repair. Simultaneous compactions help preserve read performance in a mixed read-write workload by mitigating the tendency of small SSTables to accumulate during a single long-running compaction. If your data directories are backed by SSD, increase this value to the number of cores. If compaction running too slowly or too fast, adjust [compaction_throughput_mb_per_sec](#) first.

Note: Increasing concurrent compactors impacts the available disk storage because concurrent compactions happen in parallel, especially for STCS. Ensure that adequate disk space is available when increasing this configuration.

sstable_preemptive_open_interval_in_mb

(Default: 50MB) When compacting, the replacement opens SSTables before they are completely written and uses in place of the prior SSTables for any range previously written. This setting helps to smoothly transfer reads between the SSTables by reducing page cache churn and keeps hot rows hot.

*Memtable settings***memtable_allocation_type**

(Default: heap_buffers) Specifies the way Cassandra allocates and manages memtable memory. See [Off-heap memtables in Cassandra 2.1](#). In releases 3.2.0 and 3.2.1, the only option that works is: heap-buffers (On heap NIO (non-blocking I/O) buffers).

memtable_cleanup_threshold

(Default: $1/(\text{memtable_flush_writers} + 1)$)^{note}. Ratio used for automatic memtable flush. Cassandra adds [memtable_heap_space_in_mb](#) to [memtable_offheap_space_in_mb](#) and multiplies the total by [memtable_cleanup_threshold](#) to get a space amount in MB. When the total amount of memory being used by all non-flushing memtables exceeds this amount, Cassandra flushes the largest memtable to disk.

For example, consider a node on which the total of [memtable_heap_space_in_mb](#) and [memtable_offheap_space_in_mb](#) is 1000, and [memtable_cleanup_threshold](#) is 0.50. The "memtable_cleanup" amount is 500MB. This node has two memtables: Memtable A (150MB) and Memtable B (350MB). When either memtable increases, the total space they use exceeds 500MB. When this happens, Cassandra flushes the Memtable B to disk.

A larger value for [memtable_cleanup_threshold](#) means larger flushes, less frequent flushes and potentially less compaction activity, but also less concurrent flush activity, which can make it difficult to keep your disks saturated under heavy write load.

This section documents the formula used to calculate the ratio based on the number of [memtable_flush_writers](#). The default value in `cassandra.yaml` is 0.11, which works if the node has many disks or if you set the node's [memtable_flush_writers](#) to 8. As another example, if the node uses a single SSD, the value for [memtable_cleanup_threshold](#) computes to 0.33, based on the minimum [memtable_flush_writers](#) value of 2.

file_cache_size_in_mb

(Default: Smaller of 1/4 heap or 512) Total memory to use for SSTable-reading buffers.

buffer_pool_use_heap_if_exhausted

(Default: true)^{note} Indicates whether to allocate on or off heap when the SSTable buffer pool is exhausted (when the buffer pool has exceeded the maximum memory [file_cache_size_in_mb](#)), beyond which it will not cache buffers but allocate on request.

memtable_flush_writers

(Default: Smaller of number of disks or number of cores with a minimum of 2 and a maximum of 8)^{note} Sets the number of memtable flush writer threads. These threads are blocked by disk I/O, and each one holds a memtable in memory while blocked. If your data directories are backed by SSD, increase this setting to the number of cores.

Cache and index settings

column_index_size_in_kb

(Default: 64) Granularity of the index of rows within a partition. For huge rows, decrease this setting to improve seek time. If you use key cache, be careful not to make this setting too large because key cache will be overwhelmed. If you're unsure of the size of the rows, it's best to use the default setting.

index_summary_capacity_in_mb

(Default: 5% of the heap size [empty])^{note} Fixed memory pool size in MB for SSTable index summaries. If the memory usage of all index summaries exceeds this limit, any SSTables with low read rates shrink their index summaries to meet this limit. This is a best-effort process. In extreme conditions, Cassandra may need to use more than this amount of memory.

index_summary_resize_interval_in_minutes

(Default: 60 minutes) How frequently index summaries should be re-sampled. This is done periodically to redistribute memory from the fixed-size pool to SSTables proportional their recent read rates. To disable, set to -1. This leaves existing index summaries at their current sampling level.

Disks settings

stream_throughput_outbound_megabits_per_sec

(Default: 200 Mbps)^{note} Throttles all outbound streaming file transfers on a node to the specified throughput. Cassandra does mostly sequential I/O when streaming data during bootstrap or repair, which can lead to saturating the network connection and degrading client (RPC) performance.

inter_dc_stream_throughput_outbound_megabits_per_sec

(Default: unset)^{note} Throttles all streaming file transfer between the data centers. This setting allows throttles streaming throughput between data centers in addition to throttling all network stream traffic as configured with [stream_throughput_outbound_megabits_per_sec](#).

trickle_fsync

(Default: false) When doing sequential writing, enabling this option tells fsync to force the operating system to flush the dirty buffers at a set interval `trickle_fsync_interval_in_kb`. Enable this parameter to avoid sudden dirty buffer flushing from impacting read latencies. Recommended to use on SSDs, but not on HDDs.

trickle_fsync_interval_in_kb

(Default: 10240). Sets the size of the fsync in kilobytes.

windows_timer_interval

(Default: 1) The default Windows kernel timer and scheduling resolution is 15.6ms for power conservation. Lowering this value on Windows can provide much tighter latency and better throughput. However, some virtualized environments may see a negative performance impact from changing this setting below the system default. The sysinternals 'clockres' tool can confirm your system's default setting.

Advanced properties

Properties for advanced users or properties that are less commonly used.

Advanced initialization properties

auto_bootstrap

(Default: true) This setting has been removed from default configuration. It makes new (non-seed) nodes automatically migrate the right data to themselves. When initializing a fresh cluster *without* data, add `auto_bootstrap: false`.

Related information: [Initializing a multiple node cluster \(single data center\)](#) on page 102 and [Initializing a multiple node cluster \(multiple data centers\)](#) on page 105.

batch_size_warn_threshold_in_kb

(Default: 5KB per batch) Log WARN on any batch size exceeding this value in kilobytes. Caution should be taken on increasing the size of this threshold as it can lead to node instability.

batch_size_fail_threshold_in_kb

(Default: 50KB per batch) Fail any batch exceeding this setting. The default value is 10X the value of `batch_size_warn_threshold_in_kb`.

broadcast_address

(Default: `listen_address`)^{note} The IP address a node tells other nodes in the cluster to contact it by. It allows public and private address to be different. For example, use the `broadcast_address` parameter in topologies where not all nodes have access to other nodes by their private IP addresses.

If your Cassandra cluster is deployed across multiple Amazon EC2 regions and you use the `Ec2MultiRegionSnitch`, set the `broadcast_address` to public IP address of the node and the `listen_address` to the private IP.

listen_on_broadcast_address

(Default: false) If you use multiple physical network interfaces, set this both property and `listen_address` to true. This allows nodes to communicate on both interfaces.

Set this property to false if the network automatically routes between public and private networks, as Amazon EC2 does.

initial_token

(Default: disabled) Used in the single-node-per-token architecture, where a node owns exactly one contiguous range in the ring space. Setting this property overrides `num_tokens`.

If your Cassandra installation is not using vnodes or have `num_tokens` set it to 1 or unspecified (`#num_tokens`), you should always specify this parameter when setting up a production cluster for the first time and when adding capacity. For more information, see this parameter in the [Cassandra 1.1 Node and Cluster Configuration](#) documentation.

This parameter can be used with `num_tokens` (vnodes) in special cases such as [Restoring from a snapshot](#) on page 122.

num_tokens

(Default: 256)^{note} 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. Generally all nodes should have the same number of tokens assuming equal hardware capability. The recommended value is 256. If unspecified (`#num_tokens`), Cassandra uses 1 (equivalent to `#num_tokens : 1`) for legacy compatibility and uses the `initial_token` setting.

If not using vnodes, comment `#num_tokens : 256` or set `num_tokens : 1` and use `initial_token`. If you already have an existing cluster with one token per node and wish to migrate to vnodes, see [Enabling virtual nodes on an existing production cluster](#).

Note: If using DataStax Enterprise, the default setting of this property depends on the type of node and type of install.

allocate_tokens_keyspace

(Default: `KEYSPACE`) Automatic allocation of `num_tokens` tokens for this node is triggered. The allocation algorithm attempts to choose tokens in a way that optimizes replicated load over the nodes in the datacenter for the replication strategy used by the specified `KEYSPACE`. The load assigned to each node will be close to proportional to its number of vnodes.

partitioner

(Default: `org.apache.cassandra.dht.Murmur3Partitioner`) Distributes rows (by partition key) across all nodes in the cluster. Any `IPartitioner` may be used, including your own as long as it is in the class path. For new clusters use the default partitioner.

Cassandra provides the following partitioners for backwards compatibility:

- `RandomPartitioner`
- `ByteOrderedPartitioner` (deprecated)
- `OrderPreservingPartitioner` (deprecated)

Related information: [Partitioners](#) on page 18

storage_port

(Default: 7000) The port for inter-node communication.

tracetype_query_ttl

(Default: 86400) TTL for different trace types used during logging of the query process

tracetype_repair_ttl

(Default: 604800) TTL for different trace types used during logging of the repair process.

Advanced automatic backup setting

auto_snapshot

(Default: true) Enable or disable whether a snapshot is taken of the data before keyspace truncation or dropping of tables. To prevent data loss, using the default setting is strongly advised. If you set to false, you will lose data on truncation or drop.

Key caches and global row properties

When creating or modifying tables, you enable or disable the key cache (partition key cache) or row cache for that table by setting the caching parameter. Other row and key cache tuning and configuration options are set at the global (node) level. Cassandra uses these settings to automatically distribute memory for each table on the node based on the overall workload and specific table usage. You can also configure the save periods for these caches globally.

Related information: [Configuring caches](#)

key_cache_keys_to_save

(Default: disabled - all keys are saved)^{note} Number of keys from the key cache to save.

key_cache_save_period

(Default: 14400 seconds [4 hours]) Duration in seconds that keys are saved in cache. Caches are saved to [saved_caches_directory](#). Saved caches greatly improve cold-start speeds and has relatively little effect on I/O.

key_cache_size_in_mb

(Default: empty) A global cache setting for tables. It is the maximum size of the key cache in memory. When no value is set, the cache is set to the smaller of 5% of the available heap, or 100MB. To disable set to 0.

Related information: [setcachecapacity](#).

row_cache_class_name

(Default: disabled - row cache is not enabled)^{note} Specify which row cache provider to use, OHCTProvider or SerializingCacheProvider. OHCTProvider is fully off-heap, SerializingCacheProvider is partially off-heap.

row_cache_keys_to_save

(Default: disabled - all keys are saved)^{note} Number of keys from the row cache to save.

row_cache_size_in_mb

(Default: 0- disabled) Maximum size of the row cache in memory. Row cache can save more time than [key_cache_size_in_mb](#), but is space-intensive because it contains the entire row. Use the row cache only for hot rows or static rows. If you reduce the size, you may not get you hottest keys loaded on start up.

row_cache_save_period

(Default: 0- disabled) Duration in seconds that rows are saved in cache. Caches are saved to [saved_caches_directory](#). This setting has limited use as described in [row_cache_size_in_mb](#).

memory_allocator

(Default: NativeAllocator) The off-heap memory allocator. In addition to caches, this property affects storage engine meta data. Supported values:

- NativeAllocator
- JEMallocAllocator

Experiments show that jemalloc saves some memory compared to the native allocator because it is more fragmentation resistant. To use, install jemalloc as a library and modify `cassandra-env.ps1`.

CAUTION: JEMalloc version 3.6.0 or later should be used with option. Known errors occur with earlier versions.

Counter caches properties

Counter cache helps to reduce counter locks' contention for hot counter cells. In case of RF = 1 a counter cache hit will cause Cassandra to skip the read before write entirely. With RF > 1 a counter cache hit will still help to reduce the duration of the lock hold, helping with hot counter cell updates, but will not allow skipping the read entirely. Only the local (clock, count) tuple of a counter cell is kept in memory, not the whole counter, so it's relatively cheap.

Note: Reducing the size counter cache may result in not getting the hottest keys loaded on start-up.

counter_cache_size_in_mb

(Default value: empty)^{note} When no value is specified a minimum of 2.5% of Heap or 50MB. If you perform counter deletes and rely on low `gc_grace_seconds`, you should disable the counter cache. To disable, set to 0.

counter_cache_save_period

(Default: 7200 seconds [2 hours]) Duration after which Cassandra should save the counter cache (keys only). Caches are saved to `saved_caches_directory`.

counter_cache_keys_to_save

(Default value: disabled)^{note} Number of keys from the counter cache to save. When disabled all keys are saved.

Tombstone settings

When executing a scan, within or across a partition, tombstones must be kept in memory to allow returning them to the coordinator. The coordinator uses them to ensure other replicas know about the deleted rows. Workloads that generate numerous tombstones may cause performance problems and exhaust the server heap. See [Cassandra anti-patterns: Queues and queue-like datasets](#). Adjust these thresholds only if you understand the impact and want to scan more tombstones. Additionally, you can adjust these thresholds at runtime using the `StorageServiceMBean`.

Related information: [Cassandra anti-patterns: Queues and queue-like datasets](#)

tombstone_warn_threshold

(Default: 1000) The maximum number of tombstones a query can scan before warning.

tombstone_failure_threshold

(Default: 100000) The maximum number of tombstones a query can scan before aborting.

Network timeout settings

range_request_timeout_in_ms

(Default: 10000 milliseconds) The time that the coordinator waits for sequential or index scans to complete.

read_request_timeout_in_ms

(Default: 5000 milliseconds) The time that the coordinator waits for read operations to complete.

counter_write_request_timeout_in_ms

(Default: 5000 milliseconds) The time that the coordinator waits for counter writes to complete.

cas_contention_timeout_in_ms

(Default: 1000 milliseconds) The time that the coordinator continues to retry a CAS (compare and set) operation that contends with other proposals for the same row.

truncate_request_timeout_in_ms

(Default: 60000 milliseconds) The time that the coordinator waits for truncates (remove all data from a table) to complete. The long default value allows for a snapshot to be taken before removing the data. If [auto_snapshot](#) is disabled (not recommended), you can reduce this time.

write_request_timeout_in_ms

(Default: 2000 milliseconds) The time that the coordinator waits for write operations to complete.

Related information: [Hinted Handoff: repair during write path](#) on page 125

request_timeout_in_ms

(Default: 10000 milliseconds) The default time for other, miscellaneous operations.

Related information: [Hinted Handoff: repair during write path](#) on page 125

Inter-node settings

cross_node_timeout

(Default: false) Enable or disable operation timeout information exchange between nodes (to accurately measure request timeouts). If disabled Cassandra assumes the request are forwarded to the replica instantly by the coordinator, which means that under overload conditions extra time is required for processing already-timed-out requests..

CAUTION: Before enabling this property make sure NTP (network time protocol) is installed and the times are synchronized between the nodes.

internode_send_buff_size_in_bytes

(Default: N/A)^{note} Sets the sending socket buffer size in bytes for inter-node calls.

When setting this parameter and [internode_recv_buff_size_in_bytes](#), the buffer size is limited by `net.core.wmem_max`. When unset, buffer size is defined by `net.ipv4.tcp_wmem`. See `man tcp` and:

- `/proc/sys/net/core/wmem_max`
- `/proc/sys/net/core/rmem_max`
- `/proc/sys/net/ipv4/tcp_wmem`
- `/proc/sys/net/ipv4/tcp_wmem`

internode_recv_buff_size_in_bytes

(Default: N/A)^{note} Sets the receiving socket buffer size in bytes for inter-node calls.

internode_compression

(Default: all) Controls whether traffic between nodes is compressed. The valid values are:

- `all`
All traffic is compressed.
- `dc`
Traffic between data centers is compressed.
- `none`
No compression.

inter_dc_tcp_nodelay

(Default: false) Enable or disable `tcp_nodelay` for inter-data center communication. When disabled larger, but fewer, network packets are sent. This reduces overhead from the TCP protocol itself. However, if cross data-center responses are blocked, it will increase latency.

streaming_socket_timeout_in_ms

(Default: 3600000 - 1 hour)^{note} Enable or disable socket timeout for streaming operations. When a timeout occurs during streaming, streaming is retried from the start of the current file. Avoid setting this value too low, as it can result in a significant amount of data re-streaming.

Native transport (CQL Binary Protocol)

start_native_transport

(Default: true) Enable or disable the native transport server. Uses the same address as the [rpc_address](#), but the port is different from the [rpc_port](#). See [native_transport_port](#).

native_transport_port

(Default: 9042) Port on which the CQL native transport listens for clients.

native_transport_max_threads

(Default: 128)^{note} The maximum number of thread handling requests. Similar to [rpc_max_threads](#) and differs as follows:

- Default is different (128 versus unlimited).
- No corresponding [native_transport_min_threads](#).
- Idle threads are stopped after 30 seconds.

native_transport_max_frame_size_in_mb

(Default: 256MB) The maximum size of allowed frame. Frame (requests) larger than this are rejected as invalid.

native_transport_max_concurrent_connections

(Default: -1) Specifies the maximum number of concurrent client connections. The default value of -1 means unlimited.

native_transport_max_concurrent_connections_per_ip

(Default: -1) Specifies the maximum number of concurrent client connections per source IP address. The default value of -1 means unlimited.

RPC (remote procedure call) settings

Settings for configuring and tuning client connections.

broadcast_rpc_address

(Default: unset)^{note} RPC address to broadcast to drivers and other Cassandra nodes. This cannot be set to 0.0.0.0. If blank, it is set to the value of the [rpc_address](#) or [rpc_interface](#). If [rpc_address](#) or [rpc_interface](#) is set to 0.0.0.0, this property must be set.

rpc_port

(Default: 9160) Thrift port for client connections.

start_rpc

(Default: true) Starts the Thrift RPC server.

rpc_keepalive

(Default: true) Enable or disable keepalive on client connections (RPC or native).

rpc_max_threads

(Default: unlimited)^{note} Regardless of your choice of RPC server ([rpc_server_type](#)), the number of maximum requests in the RPC thread pool dictates how many concurrent requests are possible. However, if you are using the parameter `sync` in the [rpc_server_type](#), it also dictates the number of clients that can be connected. For a large number of client connections, this could cause excessive memory usage for the thread stack. Connection pooling on the client side is highly recommended. Setting a maximum thread pool size acts as a safeguard against misbehaved clients. If the maximum is reached, Cassandra blocks additional connections until a client disconnects.

rpc_min_threads

(Default: 16)^{note} Sets the minimum thread pool size for remote procedure calls.

rpc_recv_buff_size_in_bytes

(Default: N/A)^{note} Sets the receiving socket buffer size for remote procedure calls.

rpc_send_buff_size_in_bytes

(Default: N/A)^{note} Sets the sending socket buffer size in bytes for remote procedure calls.

rpc_server_type

(Default: sync) Cassandra provides three options for the RPC server. On Windows, sync is about 30% slower than hsha. On Linux, sync and hsha performance is about the same, but hsha uses less memory.

- sync: (Default One thread per Thrift connection.)

For a very large number of clients, memory is the limiting factor. On a 64-bit JVM, 180KB is the minimum stack size per thread and corresponds to your use of virtual memory. Physical memory may be limited depending on use of stack space.

- hsha:

Half synchronous, half asynchronous. All Thrift clients are handled asynchronously using a small number of threads that does not vary with the number of clients and thus scales well to many clients. The RPC requests are synchronous (one thread per active request).

Note: When selecting this option, you must change the default value (unlimited) of [rpc_max_threads](#).

- Your own RPC server

You must provide a fully-qualified class name of an `o.a.c.t.TServerFactory` that can create a server instance.

Advanced fault detection settings

Settings to handle poorly performing or failing components.

gc_warn_threshold_in_ms

(Default: 1000) Any GC pause longer than this interval is logged at the WARN level. (By default, Cassandra logs any GC pause greater than 200 ms at the INFO level.)

Additional information: [Configuring logging](#) on page 97.

dynamic_snitch_badness_threshold

(Default: 0.1) Sets the performance threshold for dynamically routing client requests away from a poorly performing node. Specifically, it controls how much worse a poorly performing node has to be before the [dynamic snitch](#) prefers other replicas over it. A value of 0.2 means Cassandra continues to prefer the static snitch values until the node response time is 20% worse than the best performing node. Until the threshold is reached, incoming requests are statically routed to the closest replica (as determined by the snitch). If the value of this parameter is greater than zero and [read_repair_chance](#) is less than 1.0, cache capacity is maximized across the nodes.

dynamic_snitch_reset_interval_in_ms

(Default: 600000 milliseconds) Time interval to reset all node scores, which allows a bad node to recover.

dynamic_snitch_update_interval_in_ms

(Default: 100 milliseconds) The time interval for how often the snitch calculates node scores. Because score calculation is CPU intensive, be careful when reducing this interval.

hints_flush_period_in_ms

(Default: 10000) Set how often hints are flushed from internal buffers to disk.

hints_directory

(Default: `$CASSANDRA_HOME/data/hints`) Set directory where hints are stored.

hinted_handoff_enabled

(Default: true) Enable or disable hinted handoff. To enable per data center, add data center list. For example: `hinted_handoff_enabled: DC1,DC2`. A hint indicates that the write needs to be replayed to an unavailable node. Where Cassandra writes the hint to a hints file on the coordinator node.

Related information: [Hinted Handoff: repair during write path](#) on page 125

hinted_handoff_disabled_datacenters

(Default: none) Specify blacklist of data centers that will not perform hinted handoffs. To enable per data center, add data center list. For example: `hinted_handoff_disabled_datacenters: - DC1 - DC2`.

Related information: [Hinted Handoff: repair during write path](#) on page 125

hinted_handoff_throttle_in_kb

(Default: 1024) Maximum throttle per delivery thread in kilobytes per second. This rate reduces proportionally to the number of nodes in the cluster. For example, if there are two nodes in the cluster, each delivery thread will use the maximum rate. If there are three, each node will throttle to half of the maximum, since the two nodes are expected to deliver hints simultaneously.

max_hint_window_in_ms

(Default: 10800000 milliseconds [3 hours]) Maximum amount of time that hints are generated for an unresponsive node. After this interval, new hints are no longer generated until the node is back up and responsive. If the node goes down again, a new interval begins. This setting can prevent a sudden demand for resources when a node is brought back online and the rest of the cluster attempts to replay a large volume of hinted writes.

Related information: [Failure detection and recovery](#) on page 13

max_hints_delivery_threads

(Default: 2) Number of threads with which to deliver hints. In multiple data-center deployments, consider increasing this number because cross data-center handoff is generally slower.

max_hints_file_size_in_mb

(Default: 128) The maximum size for a single hints file, in megabytes.

hints_compression

(Default: LZ4Compressor) The compressor for hint files. Supported compressors: [LZ](#), [Snappy](#), and [Deflate](#). If you do not specify a compressor, the hints files are not compressed.

batchlog_replay_throttle_in_kb

(Default: 1024KB per second) Total maximum throttle. Throttling is reduced proportionally to the number of nodes in the cluster.

Request scheduler properties

Settings to handle incoming client requests according to a defined policy. If you need to use these properties, your nodes are overloaded and dropping requests. It is recommended that you add more nodes and not try to prioritize requests.

Note: The properties in this section apply only to the Thrift transport. They have no effect on the use of CQL over the native protocol.

request_scheduler

(Default: `org.apache.cassandra.scheduler.NoScheduler`) Defines a scheduler to handle incoming client requests according to a defined policy. This scheduler is useful for throttling client requests in single clusters containing multiple keyspaces. This parameter is specifically for requests from the client and does not affect inter-node communication. Valid values are:

- `org.apache.cassandra.scheduler.NoScheduler`
No scheduling takes place.
- `org.apache.cassandra.scheduler.RoundRobinScheduler`
Round robin of client requests to a node with a separate queue for each [request_scheduler_id](#) property.
- A Java class that implements the `RequestScheduler` interface.

request_scheduler_id

(Default: `keyspace`)^{note} An identifier on which to perform request scheduling. Currently the only valid value is `keyspace`. See [weights](#).

request_scheduler_options

(Default: disabled) Contains a list of properties that define configuration options for [request_scheduler](#):

Configuration

- `throttle_limit`: The number of in-flight requests per client. Requests beyond this limit are queued up until running requests complete. Recommended value is $((\text{concurrent_reads} + \text{concurrent_writes}) \times 2)$.
- `default_weight`: (Default: 1)^{note}
How many requests are handled during each turn of the `RoundRobin`.
- `weights`: (Default: Keyspace: 1)
Takes a list of keyspaces. It sets how many requests are handled during each turn of the `RoundRobin`, based on the `request_scheduler_id`.

Thrift interface properties

Legacy API for older clients. [CQL](#) is a simpler and better API for Cassandra.

thrift_framed_transport_size_in_mb

(Default: 15) Frame size (maximum field length) for Thrift. The frame is the row or part of the row that the application is inserting.

thrift_max_message_length_in_mb

(Default: 16) The maximum length of a Thrift message in megabytes, including all fields and internal Thrift overhead (1 byte of overhead for each frame). Message length is usually used in conjunction with batches. A frame length greater than or equal to 24 accommodates a batch with four inserts, each of which is 24 bytes. The required message length is greater than or equal to $24+24+24+24+4$ (number of frames).

Security properties

Server and client security settings.

authenticator

(Default: `AllowAllAuthenticator`) The authentication backend. It implements `IAuthenticator` for identifying users. The available authenticators are:

- `AllowAllAuthenticator`:
Disables authentication; no checks are performed.
- `PasswordAuthenticator`

Authenticates users with user names and hashed passwords stored in the `system_auth.credentials` table. If you do not change the replication factor of the `system_auth` keyspace from its default, 1, and the node with the single replica goes down, login to the cluster becomes impossible because the `system_auth` keyspace has not been replicated.

Related information: [Internal authentication](#) on page 87

internode_authenticator

(Default: `enabled`)^{note} Internode authentication backend. It implements `org.apache.cassandra.auth.AllowAllInternodeAuthenticator` to allow or disallow connections from peer nodes.

authorizer

(Default: `AllowAllAuthorizer`) The authorization backend. It implements `IAuthenticator` to limit access and provide permissions. The available authorizers are:

- `AllowAllAuthorizer`
Disables authorization; allows any action to any user.
- `CassandraAuthorizer`

Stores permissions in `system_auth.permissions` table. If you do not change the replication factor of the `system_auth` keyspace from its default, 1, and the node with the single replica goes down, login to the cluster becomes impossible because the `system_auth` keyspace has not been replicated.

Related information: [Object permissions](#) on page 89

role_manager

(Default: `CassandraRoleManager`) Part of the Authentication & Authorization backend that implements `IRoleManager` to maintain grants and memberships between roles. Out of the box, Cassandra provides `org.apache.cassandra.auth.CassandraRoleManager`, which stores role information in the `system_auth` keyspace. Most functions of the `IRoleManager` require an authenticated login, so unless the configured `IAuthenticator` actually implements authentication, most of this functionality will be unavailable. `CassandraRoleManager` stores role data in the `system_auth` keyspace. Please increase `system_auth` keyspace replication factor if you use the role manager.

roles_validity_in_ms

(Default: 2000) Fetching permissions can be an expensive operation depending on the authorizer, so this setting allows flexibility. Validity period for roles cache; set to 0 to disable. Granted roles are cached for authenticated sessions in `AuthenticatedUser` and after the period specified here, become eligible for (async) reload. Will be disabled automatically for `AllowAllAuthenticator`.

roles_update_interval_in_ms

(Default: 2000) Refresh interval for roles cache, if enabled. Defaults to the same value as `roles_validity_in_ms`. After this interval, cache entries become eligible for refresh. Upon next access, an async reload is scheduled and the old value returned until it completes. If `roles_validity_in_ms` is non-zero, then this must be also.

credentials_validity_in_ms

(Default: 2000) How long credentials in cache remain valid. This cache is tightly coupled to the provided `PasswordAuthenticator` implementation of `IAuthenticator`. If another `IAuthenticator` implementation is configured, this cache is not used, and these settings have no effect. Set to 0 to disable.

Related information: [Internal authentication](#) on page 87, [Internal authorization](#) on page 89

Note: Credentials are cached in encrypted form. This may cause a performance penalty that offsets the reduction in latency gained by caching.

credentials_update_interval_in_ms

(Default: same value as `credentials_validity_in_ms`) After this interval, cache entries become eligible for refresh. The next time the cache is accessed, the system schedules an asynchronous reload of the cache. Until this cache reload is complete, the cache returns the old values.

If `credentials_validity_in_ms` is nonzero, this property must also be nonzero.

permissions_validity_in_ms

(Default: 2000) How long permissions in cache remain valid. Depending on the authorizer, such as `CassandraAuthorizer`, fetching permissions can be resource intensive. This setting disabled when set to 0 or when `AllowAllAuthorizer` is set.

Related information: [Object permissions](#) on page 89

permissions_update_interval_in_ms

(Default: same value as [permissions_validity_in_ms](#))^{note} Refresh interval for permissions cache (if enabled). After this interval, cache entries become eligible for refresh. On next access, an async reload is scheduled and the old value is returned until it completes. If `permissions_validity_in_ms`, then this property must be non-zero.

server_encryption_options

Enable or disable 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. The available options are:

- `internode_encryption`: (Default: none) Enable or disable encryption of inter-node communication using the `TLS_RSA_WITH_AES_128_CBC_SHA` cipher suite for authentication, key exchange, and encryption of data transfers. Use the `DHE/ECDHE` ciphers if running in (Federal Information Processing Standard) FIPS 140 compliant mode. The available inter-node options are:

Configuration

- all
Encrypt all inter-node communications.
- none
No encryption.
- dc
Encrypt the traffic between the data centers (server only).
- rack
Encrypt the traffic between the racks (server only).
- keystore: (Default: `conf/.keystore`)
The location of a 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.
- keystore_password: (Default: `cassandra`)
Password for the keystore.
- truststore: (Default: `conf/.truststore`)
Location of the truststore containing the trusted certificate for authenticating remote servers.
- truststore_password: (Default: `cassandra`)
Password for the truststore.

The passwords used in these options must match the passwords used when generating the keystore and truststore. For instructions on generating these files, see [Creating a Keystore to Use with JSSE](#).

The advanced settings are:

- protocol: (Default: TLS)
- algorithm: (Default: SunX509)
- store_type: (Default: JKS)
- cipher_suites: (Default: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA)
- require_client_auth: (Default: false)
Enables or disables certificate authentication.

Related information: [Node-to-node encryption](#) on page 86

client_encryption_options

Enable or disable 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. The available options are:

- enabled: (Default: false)
To enable, set to true.
- keystore: (Default: `conf/.keystore`)
The location of a 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.
- keystore_password: (Default: `cassandra`)
Password for the keystore. This must match the password used when generating the keystore and truststore.
- require_client_auth: (Default: false)
Enables or disables certificate authentication. (Available starting with Cassandra 1.2.3.)

- `truststore:` (Default: `conf/.truststore`)
Set if `require_client_auth` is true.
- `truststore_password:` `<truststore_password>`
Set if `require_client_auth` is true.

The advanced settings are:

- `protocol:` (Default: TLS)
- `algorithm:` (Default: SunX509)
- `store_type:` (Default: JKS)
- `cipher_suites:` (Default: TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA)

Related information: [Client-to-node encryption](#) on page 84

transparent_data_encryption_options

Enables encryption of data *at rest* (on-disk). Recommendation: download and install the [Java Cryptography Extension \(JCE\) Unlimited Strength Jurisdiction Policy Files](#) for your version of the JDK.

Cassandra supports transparent data encryption for the following file types:

- [commitlog](#)
- [hints](#)

The available options are:

- `enabled:` (Default: false)
- `chunk_length_kb:` (Default: 64)
- `cipher:` options:
 - AES
 - CBC
 - PKCS5Padding
- `key_alias:` testing:1
- `iv_length:` 16

Note: `iv_length` is commented out in the default `cassandra.yaml` file. Uncomment only if cipher is set to AES. The value must be 16 (bytes).

- `key_provider:`
 - `class_name:` `org.apache.cassandra.security.JKSKeyProvider`
`parameters:`
 - `keystore:` `conf/.keystore`
 - `keystore_password:` `cassandra`
 - `store_type:` JCEKS
 - `key_password:` `cassandra`

ssl_storage_port

(Default: 7001) The SSL port for encrypted communication. Unused unless enabled in `encryption_options`.

native_transport_port_ssl

(Default: 9142) In Cassandra 3.0 and later, an additional dedicated port can be designated for encryption. If client encryption is enabled and `native_transport_port_ssl` is disabled, the `native_transport_port` (default: 9042) will encrypt all traffic. To use both unencrypted and encrypted traffic, enable `native_transport_port_ssl`.

Cassandra include file

To set environment variables, Cassandra can use the `cassandra.in.bat` include file, located in:
`C:\Program Files\DataStax-DDC\apache-cassandra\bin\cassandra.in.bat`

Security

Securing Cassandra

Cassandra provides these security features to the open source community.

- [SSL encryption](#)

Cassandra provides secure communication between a client machine and a database cluster, and among nodes in a cluster. Enabling SSL encryption ensures that data in flight is not compromised and is transferred securely. You can configure client-to-node and node-to-node encryption independently.

- [Authentication based on internally controlled login accounts/passwords](#)

Administrators can create users and roles who can be authenticated to Cassandra database clusters using the `CREATE USER` or `CREATE ROLE` command. Internally, Cassandra manages user accounts and access to the database cluster using passwords. User accounts may be altered and dropped using CQL.

- [Object permission management](#)

Once authenticated into a database cluster using either internal authentication, the next security issue to be tackled is permission management. What can the user do inside the database? Authorization capabilities for Cassandra use the familiar `GRANT/REVOKE` security paradigm to manage object permissions.

SSL encryption

The Secure Socket Layer (SSL) is a cryptographic protocol used to secure communications between computers. For reference, see [SSL in wikipedia](#).

Briefly, it works in the following manner. A client and server are defined as two entities that are communicating with one another, either software or hardware. These entities must exchange information to set up trust between them. Each entity that will provide such information must have a generated key that consists of a private key that only the entity stores and a public key that can be exchanged with other entities. If the client wants to connect to the server, the client requests the secure connection and the server sends a certificate that includes its public key. The client checks the validity of the certificate by exchanging information with the server, which the server validates with its private key. If a two-way validation is desired, this process must be carried out in both directions. Private keys are stored in the `keystore` and public keys are stored in the `truststore`.

For Cassandra, the entities can be nodes or one of the tools such as `cqlsh` or `nodetool` running on either a local node or a remote node.

Preparing server certificates

To use SSL encryption for client-to-node encryption or node-to-node encryption, SSL certificates must be generated using [keytool](#). If you generate the certificates for one type of encryption, you do not need to generate them again for the other; the same certificates are used for both. All nodes must have all

the relevant SSL certificates on all nodes. A keystore contains private keys. The truststore contains SSL certificates for each node. The certificates in the truststore don't require signing by a trusted and recognized public certification authority.

Procedure

- Generate a private and public key pair on each node of the cluster. Use an alias that identifies the node. Prompts for the keystore password, dname (first and last name, organizational unit, organization, city, state, country), and key password. The dname should be generated with the CN value as the IP address or FQDN for the node.

```
C:\> keytool -genkey -keyalg RSA -alias node0 -validity 36500 -keystore
keystore.node0
```

Note: In this example, the value for `--validity` gives this key pair a validity period of 100 years. The default `validity` value for a key pair is 90 days.

- The generation command can also include all prompted-for information in the command line. This example uses an alias of `node0`, a keystore name of `keystore.node0`, uses the same password of `cassandra` for both the keystore and the key, and a `dname` that identifies the IP address of `node0` as `172.31.10.22`.

```
C:\> keytool -genkey -keyalg RSA -alias node0 -keystore keystore.node0 -
storepass cassandra -keypass cassandra -dname "CN=172.31.10.22, OU=None,
O=None, L=None, C=None"
```

- Export the public part of the certificate to a separate file.

```
C:\> keytool -export -alias cassandra -file node0.cer -keystore .keystore
```

- Add the `node0.cer` certificate to the `node0` truststore of the node using the `keytool -import` command.

```
C:\> keytool -import -v -trustcacerts -alias node0 -file node0.cer -keystore
truststore.node0
```

- `cqlsh` does not work with the certificate in the format generated. `openssl` is used to generate a PEM file of the certificate with no keys, `node0.cer.pem`, and a PEM file of the key with no certificate, `node0.key.pem`. First, the keystore is imported in PKCS12 format to a destination keystore, `node0.p12`, in the example. This is followed by the two commands that extract the two PEM files.

```
C:\> keytool -importkeystore -srckeystore keystore.node0 -destkeystore
node0.p12 -deststoretype PKCS12 -srcstorepass cassandra -deststorepass
cassandra
openssl pkcs12 -in node0.p12 -nokeys -out node0.cer.pem -passin
pass:cassandra
openssl pkcs12 -in node0.p12 -nodes -nocerts -out node0.key.pem -passin
pass:cassandra
```

- For client-to-remote-node encryption or node-to-node encryption, use a copying tool such as `scp` to copy the `node0.cer` file to each node. Import the file into the truststore after copying to each node. The example imports the certificate for `node0` into the truststore for `node1`.

```
C:\> keytool -import -v -trustcacerts -alias node0 -file node0.cer -keystore
truststore.node1
```

- Make sure keystore file is readable only to the Cassandra daemon and not by any user of the system.
- Check that the certificates exist in the keystore and truststore files using `keytool -list`. The example shows checking for the `node1` certificate in the keystore file and for the `node0` and `node1` certificates in the truststore file.

```
C:\> keytool -list -keystore keystore.node1
keytool -list -keystore truststore.node1
```

What to do next

After you have enabled certificate authentication, you can [Add new trusted users](#).

Adding new trusted users

How to add new users when client certificate authentication is enabled.

Prerequisites

The client certificate authentication must be enabled (`require_client_auth=true`).

Procedure

1. Generate the certificate as described in [Client-to-node encryption](#) on page 84.
2. Import the user's certificate into every node's truststore using `keytool`:

```
C:\> keytool -import -v -trustcacerts -alias <username> -file <certificate file> -keystore .truststore
```

Client-to-node encryption

Client-to-node encryption protects data in flight from client machines to a database cluster using SSL (Secure Sockets Layer). It establishes a secure channel between the client and the coordinator node.

Prerequisites

All nodes must have all the relevant SSL certificates on all nodes. See [Preparing server certificates](#) on page 82.

To enable client-to-node SSL, you must set the `client_encryption_options` in the `cassandra.yaml` file.

Procedure

On each node under `client_encryption_options`:

- Enable encryption.
- Set the appropriate paths to your `.keystore` and `.truststore` files.
- Provide the required passwords. The passwords must match the passwords used when generating the keystore and truststore.
- To enable client certificate authentication for two-way SSL encryption, set `require_client_auth` to `true`. Enabling this option allows tools like `cqlsh` to connect to a remote node. If only local access is required, such as running `cqlsh` on a local node with SSL encryption, this option is not required. If the options is set to `true`, then the truststore and truststore password must also be included.

This example uses the password `cassandra` for both the keystore and the truststore.

```
client_encryption_options:
  enabled: true
  # The path to your keystore file; ex: conf/keystore.node0
  keystore: conf/keystore.node0
  # The password for your keystore file
  keystore_password: cassandra
  # The next 3 lines are included if 2-way SSL is desired
  require_client_auth: true
```

```
# The path to your truststore file; ex: conf/truststore.node0
truststore: conf/truststore.node0
# The password for your truststore file
truststore_password: cassandra
```

Note: Cassandra must be restarted after making changes to the `cassandra.yaml` file.

- Enabling client encryption will encrypt all traffic on the `native_transport_port` (default: 9042). If both encrypted and unencrypted traffic is required, an additional `cassandra.yaml` setting must be enabled. The `native_transport_port_ssl` (default: 9142) sets an additional dedicated port to carry encrypted transmissions, while `native_transport_port` carries unencrypted transmissions. It is beneficial to install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files if this option is enabled.

Using cqlsh with SSL encryption

Using a `cqlshrc` file is the easiest method of getting `cqlshrc` settings. The `cqlshrc.sample` provides an example that can be copied as a starting point.

Procedure

- To run `cqlsh` with SSL encryption, create a `.cassandra\cqlshrc` file in your home directory (as defined by your `HOME/USERPROFILE` environmental variable) with the following settings:

```
[authentication]
username = fred
password = !!bang!!$

[connection]
hostname = 127.0.0.1
port = 9042
factory = cqlshlib.ssl.ssl_transport_factory

[ssl]
certfile = %USERPROFILE%\keys\node0.cer.pem
# Optional, true by default
validate = true
# The next 2 lines must be provided when require_client_auth = true in the
# cassandra.yaml file
userkey = %USERPROFILE%\node0.key.pem
usercert = %USERPROFILE%\node0.cer.pem
[certfiles]
# Optional section, overrides the default certfile in the [ssl] section
172.31.10.22 = %USERPROFILE%\keys/node0.cer.pem
172.31.8.141 = %USERPROFILE%\keys/node1.cer.pem
```

When `validate` is enabled, to verify that the certificate is trusted, the host in the certificate is compared to the host of the machine that it is connected.

The use of the same IP addresses in the `[certfiles]` section, as is used to generate the `dname` of the certificates, is required for two-way SSL encryption. Each node must have a line in the `[certfiles]` section for client-to-remote-node or node-to-node. The SSL certificate must be provided either in the configuration file or as an environment variable. The environment variables (`SSL_CERTFILE` and `SSL_VALIDATE`) override any options set in this file.

Note: Additional settings in the `cqlshrc` file are described in [Creating and using the cqlshrc file](#).

- Start `cqlsh` with the `--ssl` option for `cqlsh` to local node encrypted connection.

```
C:\> %CASSANDRA_HOME%\bin\cqlsh.bat --ssl
```

3. For a remote node encrypted connection, start [cqlsh](#) with the `--ssl` option and an IP address:

```
C:\> %CASSANDRA_HOME%\bin\cqlsh.bat --ssl 172.31.10.22
```

Using nodetool (JMX) with SSL

Using `nodetool` with SSL requires some JMX setup. Changes to `cassandra-env.sh` are required, and a configuration file, `~/cassandra/nodetool-ssl.properties`, is created.

Procedure

1. First, follow steps #1-8 in [Enabling JMX authentication](#) on page 91.
2. To run `nodetool` with SSL encryption, some additional changes are required to `cassandra-env.sh`. The following settings must be added to the file. Use the file path to the keystore and truststore, and appropriate passwords for each file.

```
JVM_OPTS="$JVM_OPTS -Djavax.net.ssl.keyStore=%USERPROFILE  
\keystore.node0"  
JVM_OPTS="$JVM_OPTS -Djavax.net.ssl.keyStorePassword=cassandra"  
JVM_OPTS="$JVM_OPTS -Djavax.net.ssl.trustStore=%USERPROFILE  
\truststore.node0"  
JVM_OPTS="$JVM_OPTS -Djavax.net.ssl.trustStorePassword=cassandra"  
JVM_OPTS="$JVM_OPTS -  
Dcom.sun.management.jmxremote.ssl.need.client.auth=true"  
JVM_OPTS="$JVM_OPTS -Dcom.sun.management.jmxremote.registry.ssl=true"
```

3. [Restart Cassandra](#).
4. To run `nodetool` with SSL encryption, create a `.cassandra/nodetool-ssl.properties` file in your home or client program directory with the following settings.

```
-Djavax.net.ssl.keyStore=%USERPROFILE\keystore.node0  
-Djavax.net.ssl.keyStorePassword=cassandra  
-Djavax.net.ssl.trustStore=%USERPROFILE\truststore.node0  
-Djavax.net.ssl.trustStorePassword=cassandra  
-Dcom.sun.management.jmxremote.ssl.need.client.auth=true  
-Dcom.sun.management.jmxremote.registry.ssl=true
```

5. Start `nodetool` with the `--ssl` option for encrypted connection for any `nodetool` operation.

```
C:\> %CASSANDRA_HOME%\bin\nodetool.bat --ssl ring
```

Node-to-node encryption

Node-to-node encryption protects data transferred between nodes in a cluster, including gossip communications, using SSL (Secure Sockets Layer).

Prerequisites

All nodes must have all the relevant SSL certificates on all nodes. See [Preparing server certificates](#) on page 82.

To enable node-to-node SSL, you must set the [server_encryption_options](#) in the `cassandra.yaml` file.

Procedure

On each node under `server_encryption_options`:

- Enable `internode_encryption`.

The available options are:

- `all`
- `none`
- `dc`: Cassandra encrypts the traffic between the data centers.
- `rack`: Cassandra encrypts the traffic between the racks.
- Set the appropriate paths to your `keystore` and `truststore` files.
- Provide the required passwords. The passwords must match the passwords used when generating the keystore and truststore.
- To enable 2 way certificate authentication, set `require_client_auth` to `true`.

Example

```
server_encryption_options:
  internode_encryption: all
  keystore: /conf/keystore.node0
  keystore_password: cassandra
  truststore: /conf/truststore.node0
  truststore_password: cassandra
  require_client_auth: true
```

What to do next

Cassandra must be restarted after making changes to the `cassandra.yaml` file. Use the `nodetool` utility to check if all nodes are up after making the changes.

```
C:\> %CASSANDRA_HOME%\bin\nodetool ring
```

Internal authentication

Internal authentication

Like [object permission management](#) using internal authorization, internal authentication is based on Cassandra-controlled login accounts and passwords. Internal authentication works for the following clients when you provide a user name and password to start up the client:

- Astyanax
- `cqlsh`
- [DataStax drivers](#) - produced and certified by DataStax to work with Cassandra.
- Hector
- `pycassa`

Internal authentication stores usernames and bcrypt-hashed passwords in the `system_auth.credentials` table.

`PasswordAuthenticator` is an `IAuthenticator` implementation that you can use to configure Cassandra for internal authentication out-of-the-box.

Configuring authentication

To configure Cassandra to use internal authentication, first make a change to the `cassandra.yaml` file and increase the replication factor of the `system_auth` keyspace, as described in this procedure. Next, start up Cassandra using the default user name and password (`cassandra/cassandra`), and start `cqlsh` using the same credentials. Finally, use these CQL statements to set up user accounts to authorize users to access the database objects:

- [ALTER ROLE](#)
- [ALTER USER](#)
- [CREATE ROLE](#)
- [CREATE USER](#)
- [DROP ROLE](#)
- [DROP USER](#)
- [LIST ROLES](#)
- [LIST USERS](#)

Note: To configure authorization, see [Internal authorization](#) on page 89.

Procedure

1. Change the authenticator option in the `cassandra.yaml` file to `PasswordAuthenticator`.

By default, the authenticator option is set to `AllowAllAuthenticator`.

```
authenticator: PasswordAuthenticator
```

2. Change the `system_auth` keyspace setting to [Increase the replication factor](#). The recommended setting is 3 to 5 nodes per Data Center.

If you do not change the replication factor of the `system_auth` keyspace from its default, 1, and the node with the single replica goes down, login to the cluster becomes impossible because the `system_auth` keyspace has not been replicated.

3. Restart the Cassandra client.

The default [superuser](#) name and password that you use to start the client is stored in Cassandra.

```
C:\> client_startup_string -u cassandra -p cassandra
```

4. Start `cqlsh` using the superuser name and password.

```
C:\> cqlsh -u cassandra -p cassandra
```

5. The default user is named `cassandra`. Create another superuser, not named `cassandra`. The default user `cassandra` reads with a [consistency level](#) of `QUORUM` by default, whereas another superuser will read with a consistency level of `LOCAL_ONE`. This step is optional, but highly recommended because of the consistency level settings.
6. Log in as that new superuser.
7. Change the `cassandra` user password to something long and incomprehensible, and then forget about it. It won't be used again.
8. Take away the `cassandra` user's superuser status.
9. Use the CQL statements listed previously to set up user accounts and then grant permissions to access the database objects.

Logging in using cqlsh

Typically, after configuring authentication, you log into cqlsh using the `-u` and `-p` options to the `cqlsh` command. To avoid having enter credentials every time you launch cqlsh, you can create a `.cassandra/cqlshrc` file. When present, this file passes default login information to cqlsh. The `cqlshrc.sample` file provides an example.

Procedure

1. Open a text editor and create a file that specifies a user name and password.

```
[authentication]
username = fred
password = !!bang!!$
```

Note: Additional settings in the `cqlshrc` file are described in [Creating and using the cqlshrc file](#).

2. Save the file in your `home\.cassandra` directory and name it `cqlshrc`, where *home* is set by the user's HOME/USERPROFILE environmental variable.
3. Set permissions on the file.

To protect database login information, ensure that the file is secure from unauthorized access.

Internal authorization

Object permissions

Object permission management is based on [internal authorization](#). Cassandra uses roles to assign object permissions, and authorization is assigned by role using a username and password. Object permissions may be assigned for any data object, such as keyspace, table, function, aggregate.

[Permission is configurable](#) for CQL commands CREATE, ALTER, DROP, SELECT, MODIFY, and DESCRIBE, which are used to interact with the database. The EXECUTE command may be used to grant permission to a role for the SELECT, INSERT, and UPDATE commands. In addition, the AUTHORIZE command may be used to grant permission for a role to GRANT, REVOKE or AUTHORIZE another role's permissions.

Read access to these system tables is implicitly given to every authenticated user or role because the tables are used by most Cassandra tools:

- system_schema.keyspaces
- system_schema.columns
- system_schema.tables
- system.local
- system.peers

Configuring internal authorization

CassandraAuthorizer is one of many possible IAuthorizer implementations. Its advantage is that it stores permissions in the system_auth.permissions table to support all authorization-related CQL statements. To activate it, change the authorizer option in `cassandra.yaml` to use the CassandraAuthorizer.

Note: To configure authentication, see [Internal authentication](#).

Procedure

1. In the `cassandra.yaml` file, comment out the default `AllowAllAuthorizer` and add the `CassandraAuthorizer`.

```
authorizer: CassandraAuthorizer
```

You can use any authenticator except `AllowAll`.

2. [Configure the replication factor](#) for the `system_auth` keyspace to increase the replication factor to a number greater than 1.
3. Adjust the validity period for permissions caching by setting the [permissions_validity_in_ms](#) option in the `cassandra.yaml` file.

Alternatively, disable permission caching by setting this option to 0.

Results

CQL supports these authorization statements:

- [GRANT](#)
- [LIST PERMISSIONS](#)
- [REVOKE](#)

Configuring firewall port access

If you have a firewall running on the nodes in your Cassandra cluster, you must open up the following ports to allow bi-directional communication between the nodes, including certain Cassandra ports. If this isn't done, when you start Cassandra on a node, the node acts as a standalone database server rather than joining the database cluster.

Table: Public port

Port number	Description
22	SSH port

Table: Cassandra inter-node ports

Port number	Description
7000	Cassandra inter-node cluster communication.
7001	Cassandra SSL inter-node cluster communication.
7199	Cassandra JMX monitoring port.

Table: Cassandra client ports

Port number	Description
9042	Cassandra client port.
9160	Cassandra client port (Thrift).
9142	Default for native_transport_port_ssl , useful when both encrypted and unencrypted connections are supported.

Enabling JMX authentication

The default settings for Cassandra make JMX accessible only from localhost. If you want to enable remote JMX connections, change the `LOCAL_JMX` setting in `cassandra-env.ps1` and enable authentication and/or SSL. After enabling JMX authentication, ensure that tools that use JMX, such as [nodetool](#), are configured to use authentication.

Procedure

1. Open the `cassandra-env.ps1` file for editing and update or add these lines:

```
$env:JVM_OPTS="$env:JVM_OPTS -
Dcom.sun.management.jmxremote.authenticate=true"
$env:JVM_OPTS="$env:JVM_OPTS -Dcom.sun.management.jmxremote.password.file=
/etc/cassandra/jmxremote.password"
```

If the `LOCAL_JMX` setting is in your file, set:

```
LOCAL_JMX=no
```

2. Copy the `jmxremote.password.template` from `C:\Program Files\DataStax-DDC\jre\lib\management` to `C:\Users\current_user\jmx` and rename it to `jmxremote.password`.

Note: This is a sample path. Set the location of this file in `C:\Program Files\DataStax-DDC\jre\lib\management\management.properties`.

3. Edit `jmxremote.password` and add the user and password for JMX-compliant utilities:

```
monitorRole QED
controlRole R&D
cassandra cassandrapassword ## Specify the credentials for your
environment.
```

4. For the user running Cassandra, change permission of `jmxremote.password` to read only.
5. Add the `cassandra` user with read permission to `C:\Program Files\DataStax-DDC\jre\lib\management\jmxremote.access`:

```
monitorRole readonly
cassandra readwrite
controlRole readwrite \
create javax.management.monitor.,javax.management.timer. \
unregister
```

6. [Restart Cassandra](#).
7. Run `nodetool status` with the `cassandra` user and password.

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra status
```

Example

If you run `nodetool status` without user and password, you see an error similar to:

```
Exception in thread "main" java.lang.SecurityException: Authentication failed!
Credentials required
at
com.sun.jmx.remote.security.JMXPluggableAuthenticator.authenticationFailure(Unknown
Source)
```

```

at com.sun.jmx.remote.security.JMXPluggableAuthenticator.authenticate(Unknown
Source)
at sun.management.jmxremote.ConnectorBootstrap
$AccessFileCheckerAuthenticator.authenticate(Unknown Source)
at javax.management.remote.rmi.RMIServerImpl.doNewClient(Unknown Source)
at javax.management.remote.rmi.RMIServerImpl.newClient(Unknown Source)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at sun.rmi.server.UnicastServerRef.dispatch(Unknown Source)
at sun.rmi.transport.Transport$1.run(Unknown Source)
at sun.rmi.transport.Transport$1.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at sun.rmi.transport.Transport.serviceCall(Unknown Source)
at sun.rmi.transport.tcp.TCPTransport.handleMessages(Unknown Source)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run0(Unknown Source)
at sun.rmi.transport.tcp.TCPTransport$ConnectionHandler.run(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
at java.lang.Thread.run(Unknown Source)
at sun.rmi.transport.StreamRemoteCall.exceptionReceivedFromServer(Unknown
Source)
at sun.rmi.transport.StreamRemoteCall.executeCall(Unknown Source)
at sun.rmi.server.UnicastRef.invoke(Unknown Source)
at javax.management.remote.rmi.RMIServerImpl_Stub.newClient(Unknown Source)
at javax.management.remote.rmi.RMIConnector.getConnection(Unknown Source)
at javax.management.remote.rmi.RMIConnector.connect(Unknown Source)
at javax.management.remote.JMXConnectorFactory.connect(Unknown Source)
at org.apache.cassandra.tools.NodeProbe.connect(NodeProbe.java:146)
at org.apache.cassandra.tools.NodeProbe.<init>(NodeProbe.java:116)
at org.apache.cassandra.tools.NodeCmd.main(NodeCmd.java:1099)

```

Configuring gossip settings

When a node first starts up, it looks at its `cassandra.yaml` configuration file to determine the name of the Cassandra cluster it belongs to; which nodes (called *seeds*) to contact to obtain information about the other nodes in the cluster; and other parameters for determining port and range information.

Procedure

In the `cassandra.yaml` file, set the following parameters:

Property	Description
cluster_name	Name of the cluster that this node is joining. Must be the same for every node in the cluster.
listen_address	The IP address or hostname that Cassandra binds to for connecting to other Cassandra nodes.
listen_interface	Use this option instead of <code>listen_address</code> to specify the network interface by name, rather than address/hostname
(Optional) broadcast_address	The IP address a node tells other nodes in the cluster to contact it by. It allows public and private address to be different. For example, use the <code>broadcast_address</code> parameter in topologies

Property	Description
	where not all nodes have access to other nodes by their private IP addresses. The default is the <code>listen_address</code> .
<code>seed_provider</code>	A <code>-seeds</code> list is comma-delimited list of hosts (IP addresses) that gossip uses to learn the topology of the ring. Every node should have the same list of seeds. In multiple data-center clusters, it is a good idea to include at least one node from each data center (replication group) in the seed list. Designating 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 it is recommended to use a small seed list (approximately three nodes per data center).
<code>storage_port</code>	The inter-node communication port (default is 7000). Must be the same for every node in the cluster.
<code>initial_token</code>	For legacy clusters. Used in the single-node-per-token architecture, where a node owns exactly one contiguous range in the ring space.
<code>num_tokens</code>	For new clusters. Defines the number of tokens randomly assigned to this node on the ring when using virtual nodes (vnodes).

Configuring the heap dump directory

Analyzing the heap dump file can help troubleshoot memory problems. Cassandra starts Java with the option `-XX:+HeapDumpOnOutOfMemoryError`. Using this option triggers a heap dump in the event of an out-of-memory condition. The heap dump file consists of references to objects that cause the heap to overflow. By default, Cassandra puts the file a subdirectory of the working, root directory when running as a service. If Cassandra does not have write permission to the root directory, the heap dump fails. If the root directory is too small to accommodate the heap dump, the server crashes.

To ensure that a heap dump succeeds and to prevent crashes, configure a heap dump directory that is:

- Accessible to Cassandra for writing
- Large enough to accommodate a heap dump

Base the size of the directory on the value of the Java `-mx` option.

Procedure

Set the location of the heap dump in the `cassandra-env.ps1` file.

1. Open the `cassandra-env.ps1` file for editing.

Configuration

2. Scroll down to the comment about the heap dump path:

```
set jvm HeapDumpPath with CASSANDRA_HEAPDUMP_DIR
```

3. On the line after the comment, set the CASSANDRA_HEAPDUMP_DIR to the path you want to use:

```
set jvm HeapDumpPath with CASSANDRA_HEAPDUMP_DIR CASSANDRA_HEAPDUMP_DIR  
=<path>
```

4. Save the `cassandra-env.ps1` file and restart.

Configuring virtual nodes

Enabling virtual nodes on a new cluster

Generally when all nodes have equal hardware capability, they should have the same number of virtual nodes (vnodes). If the hardware capabilities vary among the nodes in your cluster, assign a proportional number of vnodes to the larger machines. For example, you could designate your older machines to use 128 vnodes and your new machines (that are twice as powerful) with 256 vnodes.

Procedure

Set the number of tokens on each node in your cluster with the [num_tokens](#) parameter in the `cassandra.yaml` file.

The recommended value is 256. Do not set the [initial_token](#) parameter.

Related reference

[Installation locations](#) on page 61

Enabling virtual nodes on an existing production cluster

You cannot directly convert a single-token nodes to a vnode. However, you can configure another data center configured with vnodes already enabled and let Cassandra automatic mechanisms distribute the existing data into the new nodes. This method has the least impact on performance.

Procedure

1. [Add a new data center to the cluster.](#)
2. Once the new data center with vnodes enabled is up, switch your clients to use the new data center.
3. Run a full repair with [nodetool repair](#).

This step ensures that after you move the client to the new data center that any previous writes are added to the new data center and that nothing else, such as hints, is dropped when you remove the old data center.

4. Update your schema to no longer reference the old data center.
5. Remove the old data center from the cluster.

See [Decommissioning a data center](#) on page 113.

Using multiple network interfaces

How to configure Cassandra for multiple network interfaces or when using different regions in cloud implementations.

You must configure settings in both the `cassandra.yaml` file and the property file (`cassandra-rackdc.properties` or `cassandra-topology.properties`) used by the snitch.

Configuring `cassandra.yaml` for multiple networks or across regions in cloud implementations

In multiple networks or cross-region cloud scenarios, communication between data centers can only take place using an external IP address. The external IP address is defined in the `cassandra.yaml` file using the `broadcast_address` setting. Configure each node as follows:

1. In the `cassandra.yaml`, set the `listen_address` to the *private* IP address of the node, and the `broadcast_address` to the *public* address of the node.

This allows Cassandra nodes to bind to nodes in another network or region, thus enabling multiple data-center support. For intra-network or region traffic, Cassandra switches to the private IP after establishing a connection.

2. Set the addresses of the seed nodes in the `cassandra.yaml` file to that of the *public* IP. Private IP are not routable between networks. For example:

```
seeds: 50.34.16.33, 60.247.70.52
```

Note: Do not make all nodes seeds, see [Internode communications \(gossip\)](#) on page 13.

3. Be sure that the `storage_port` or `ssl_storage_port` is open on the public IP firewall.

CAUTION: Be sure to enable encryption and authentication when using public IPs. See [Node-to-node encryption](#) on page 86. Another option is to use a custom VPN to have local, inter-region/ data center IPs.

Additional `cassandra.yaml` configuration for non-EC2 implementations

If multiple network interfaces are used in a non-EC2 implementation, enable the `listen_on_broadcast_address` option.

```
listen_on_broadcast_address: true
```

In non-EC2 environments, the public address to private address routing is not automatically enabled. Enabling `listen_on_broadcast_address` allows Cassandra to listen on both `listen_address` and `broadcast_address` with two network interfaces.

Configuring the snitch for multiple networks

External communication between the data centers can only happen when using the `broadcast_address` (public IP).

The [GossipingPropertyFileSnitch](#) on page 21 is recommended for production. The `cassandra-rackdc.properties` file defines the data centers used by this snitch. Enable the option `prefer_local` to ensure that traffic to `broadcast_address` will re-route to `listen_address`.

For each node in the network, specify its data center in `cassandra-rackdc.properties` file.

Configuration

In the example below, there are two cassandra data centers and each data center is named for its workload. The data center naming convention in this example is based on the workload. You can use other conventions, such as DC1, DC2 or 100, 200. (Data center names are case-sensitive.)

Network A	Network B
Node and data center: <ul style="list-style-type: none">• node0 dc=DC_A_cassandra rack=RAC1• node1 dc=DC_A_cassandra rack=RAC1• node2 dc=DC_B_cassandra rack=RAC1• node3 dc=DC_B_cassandra rack=RAC1• node4 dc=DC_A_analytics rack=RAC1• node5 dc=DC_A_search rack=RAC1	Node and data center: <ul style="list-style-type: none">• node0 dc=DC_A_cassandra rack=RAC1• node1 dc=DC_A_cassandra rack=RAC1• node2 dc=DC_B_cassandra rack=RAC1• node3 dc=DC_B_cassandra rack=RAC1• node4 dc=DC_A_analytics rack=RAC1• node5 dc=DC_A_search rack=RAC1

Configuring the snitch for cross-region communication in cloud implementations

Note: Be sure to use the appropriate [snitch](#) for your implementation. If your deploying on Amazon EC2, see the instructions in [Ec2MultiRegionSnitch](#) on page 22.

In cloud deployments, the region name is treated as the data center name and availability zones are treated as racks within a data center. For example, if a node is in the us-east-1 region, us-east is the data center name and 1 is the rack location. (Racks are important for distributing replicas, but not for data center naming.)

In the example below, there are two cassandra data centers and each data center is named for its workload. The data center naming convention in this example is based on the workload. You can use other conventions, such as DC1, DC2 or 100, 200. (Data center names are case-sensitive.)

For each node, specify its data center in the cassandra-rackdc.properties. The dc_suffix option defines the data centers used by the snitch. Any other lines are ignored.

Region: us-east	Region: us-west
Node and data center: <ul style="list-style-type: none">• node0 dc_suffix=_1_cassandra• node1 dc_suffix=_1_cassandra• node2	Node and data center: <ul style="list-style-type: none">• node0 dc_suffix=_1_cassandra• node1 dc_suffix=_1_cassandra• node2

Region: us-east	Region: us-west
dc_suffix=_2_cassandra • node3 dc_suffix=_2_cassandra • node4 dc_suffix=_1_analytics • node5 dc_suffix=_1_search This results in four us-east data centers:	dc_suffix=_2_cassandra • node3 dc_suffix=_2_cassandra • node4 dc_suffix=_1_analytics • node5 dc_suffix=_1_search This results in four us-west data centers:
us-east_1_cassandra us-east_2_cassandra us-east_1_analytics us-east_1_search	us-west_1_cassandra us-west_2_cassandra us-west_1_analytics us-west_1_search

Configuring logging

Cassandra provides logging functionality using Simple Logging Facade for Java (SLF4J) with a [logback](#) backend. Logs are written to the `system.log` and `debug.log` in the Cassandra logging directory. You can configure logging [programmatically](#) or manually. Manual ways to configure logging are:

- Run the `nodetool setlogginglevel` command.
- Configure the `logback-test.xml` or `logback.xml` file installed with Cassandra.
- Use the [JConsole](#) tool to configure logging through JMX.

Logback looks for `logback-test.xml` first, and then for `logback.xml` file.

The XML configuration files looks like this:

```
<configuration scan="true">
  <jmxConfigurator />
  <appender name="FILE"
    class="ch.qos.logback.core.rolling.RollingFileAppender">
    <file>${cassandra.logdir}/system.log</file>
    <rollingPolicy
      class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
        <fileNamePattern>${cassandra.logdir}/system.log.%i.zip</
fileNamePattern>
        <minIndex>1</minIndex>
        <maxIndex>20</maxIndex>
      </rollingPolicy>

      <triggeringPolicy
        class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
        <maxFileSize>20MB</maxFileSize>
      </triggeringPolicy>
    <encoder>
      <pattern>%-5level [%thread] %date{ISO8601} %F:%L - %msg%n</pattern>
      <!-- old-style log format
      <pattern>%5level [%thread] %date{ISO8601} %F (line %L) %msg%n</
pattern>
      -->
    </encoder>
  </appender>
```

```
<appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
  <encoder>
    <pattern>%-5level %date{HH:mm:ss,SSS} %msg%n</pattern>
  </encoder>
</appender>

<root level="INFO">
  <appender-ref ref="FILE" />
  <appender-ref ref="STDOUT" />
</root>

<logger name="com.thinkaurelius.thrift" level="ERROR"/>
</configuration>
```

The appender configurations specify where to print the log and its configuration. The first appender directs logs to a file. The second appender directs logs to the console. You can change the following logging functionality:

- Rolling policy
 - The policy for rolling logs over to an archive
 - Location and name of the log file
 - Location and name of the archive
 - Minimum and maximum file size to trigger rolling
- Format of the message
- The log level

Log levels

The valid values for setting the log level include ALL for logging information at all levels, TRACE through ERROR, and OFF for no logging. TRACE creates the most verbose log, and ERROR, the least.

- ALL
- TRACE
- DEBUG
- INFO (Default)
- WARN
- ERROR
- OFF

Note: Increasing logging levels can generate heavy logging output on a moderately trafficked cluster.

You can use the `nodetool getlogginglevels` command to see the current logging configuration.

```
C:\> %CASSANDRA_HOME%\bin\nodetool getlogginglevels
Logger Name      Log Level
ROOT             INFO
com.thinkaurelius.thrift  ERROR
```

To add debug logging to a class permanently using the logback framework, use `nodetool setlogginglevel` to check you have the right class before you set it in the logback.xml file in `install_location/conf`. Modify to include the following line or similar at the end of the file:

```
<logger name="org.apache.cassandra.gms.FailureDetector" level="DEBUG"/>
```

Restart the node to invoke the change.

Migrating to logback from log4j

If you upgrade from a previous version of Cassandra that used log4j, you can convert *log4j.properties* files to *logback.xml* using the logback [PropertiesTranslator](#) web-application.

Using log file rotation

The default policy rolls the `system.log` file after the size exceeds 20MB. Archives are compressed in zip format. Logback names the log files `system.log.1.zip`, `system.log.2.zip`, and so on. For more information, see [logback documentation](#).

Enabling extended compaction logging

You can configure Cassandra to collect in-depth information about compaction activity on a node, and write it to a dedicated log file. For details, see [Enabling extended compaction logging](#).

Commit log archive configuration

Cassandra provides commit log archiving and point-in-time recovery. The commit log is archived at node startup and when a commit log is written to disk, or at a specified point-in-time. You configure this feature in the `commitlog_archiving.properties` configuration file.

The commands `archive_command` and `restore_command` expect only a single command with arguments. The parameters must be entered verbatim. STDOUT and STDIN or multiple commands cannot be executed. To workaround, you can script multiple commands and add a pointer to this file. To disable a command, leave it blank.

Procedure

- Archive a commit log segment:

Command	archive_command=	
Parameters	%path	Fully qualified path of the segment to archive.
	%name	Name of the commit log.
Example	archive_command=/bin/ln %path /backup/%name	

- Restore an archived commit log:

Command	restore_command=	
Parameters	%from	Fully qualified path of the an archived commitlog segment fr
	%to	Name of live commit log directory.
Example	restore_command=cp -f %from %to	

- Set the restore directory location:

Command	restore_directories=
Format	restore_directories=restore_directory_location

- Restore mutations created up to and including the specified timestamp:

Command	restore_point_in_time=
Format	<timestamp> (YYYY:MM:DD HH:MM:SS)

Command	restore_point_in_time=
Example	restore_point_in_time=2013:12:11 17:00:00

Restore stops when the first client-supplied timestamp is greater than the restore point timestamp. Because the order in which Cassandra receives mutations does not strictly follow the timestamp order, this can leave some mutations unrecovered.

Generating tokens

If not using virtual nodes (vnodes), you must calculate tokens for your cluster.

The following topics in the Cassandra 1.1 documentation provide conceptual information about tokens:

- [Data Distribution in the Ring](#)
- [Replication Strategy](#)

About calculating tokens for single or multiple data centers in Cassandra 1.2 and later

- Single data center deployments: calculate tokens by dividing the hash range by the number of nodes in the cluster.
- Multiple data center deployments: calculate the tokens for each data center so that the hash range is evenly divided for the nodes in each data center.

For more explanation, see be sure to read the conceptual information mentioned above.

The method used for calculating tokens depends on the type of partitioner:

Calculating tokens for the Murmur3Partitioner

Use this method for generating tokens when you are **not** using virtual nodes (vnodes) and using the [Murmur3Partitioner](#) (default). This partitioner uses a maximum possible range of hash values from -2^{63} to $+2^{63}-1$. To calculate tokens for this partitioner:

```
C:\> python -c "print [str(((2**64 / number_of_tokens) * i) - 2**63) for i in range(number_of_tokens)]"
```

For example, to generate tokens for 6 nodes:

```
C:\> python -c "print [str(((2**64 / 6) * i) - 2**63) for i in range(6)]"
```

The command displays the token for each node:

```
[ '-9223372036854775808', '-6148914691236517206', '-3074457345618258604', '-2', '3074457345618258600', '6148914691236517202' ]
```

Calculating tokens for the RandomPartitioner

To calculate tokens when using the [RandomPartitioner](#) in Cassandra 1.2 clusters, use the [Cassandra 1.1 Token Generating Tool](#).

Hadoop support

Cassandra support for integrating Hadoop with Cassandra includes:

- MapReduce

Notice: Apache Pig is no longer supported as of Cassandra 3.0.

You can use Cassandra 3.0 with Hadoop 2.x or 1.x with some restrictions:

- You must run separate data centers: one or more data centers with nodes running just Cassandra (for Online Transaction Processing) and others with nodes running C* & with Hadoop installed. See [Isolate Cassandra and Hadoop](#) for details.
- Before starting the data centers of Cassandra/Hadoop nodes, disable virtual nodes (vnodes).

Note: You only need to disable vnodes in data centers with nodes running Cassandra AND Hadoop.

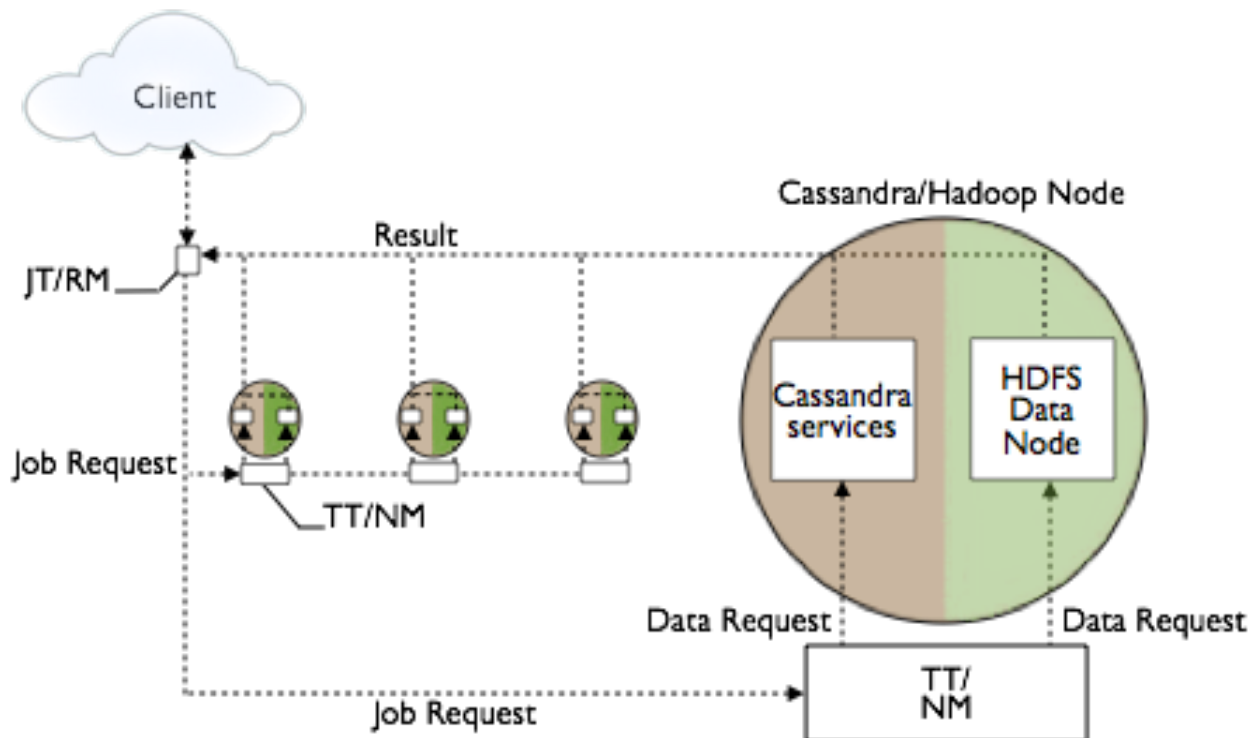
To disable virtual nodes:

1. In the `cassandra.yaml` file, set `num_tokens` to 1.
2. Uncomment the `initial_token` property and set it to 1 or to the value of a generated token for a multi-node cluster.
3. Start the cluster for the first time.

You cannot convert single-token nodes to vnodes. See [Enabling virtual nodes on an existing production cluster](#) for another option.

Setup and configuration, described in the [Apache docs](#), involves overlaying a Hadoop cluster on Cassandra nodes, configuring a separate server for the Hadoop NameNode/JobTracker, and installing a Hadoop TaskTracker and Data Node on each Cassandra node. The nodes in the Cassandra data center can draw from data in the HDFS Data Node as well as from Cassandra. The Job Tracker/Resource Manager (JT/RM) receives MapReduce input from the client application. The JT/RM sends a MapReduce job request to the Task Trackers/Node Managers (TT/NM) and an optional clients MapReduce. The data is written to Cassandra and results sent back to the client.

MapReduce Process in a Cassandra/Hadoop Cluster



The Apache docs also cover how to get configuration and integration support.

Input and Output Formats

Hadoop jobs can receive data from CQL tables and indexes and can write their output to Cassandra tables as well as to the Hadoop FileSystem. Cassandra 3.0 supports the following formats for these tasks:

- `CqlInputFormat` class: for importing job input into the Hadoop filesystem from CQL tables
- `CqlOutputFormat` class: for writing job output from the Hadoop filesystem to CQL tables
- `CqlBulkOutputFormat` class: generates Cassandra SSTables from the output of Hadoop jobs, then loads them into the cluster using the `SSTableLoaderBulkOutputFormat` class

Reduce tasks can store keys (and corresponding bound variable values) as CQL rows (and respective columns) in a given CQL table.

Running the wordcount example

Wordcount example JARs are located in the `examples` directory of the Cassandra source code installation. There are CQL and legacy examples in the `hadoop_cql3_word_count` and `hadoop_word_count` subdirectories, respectively. Follow instructions in the readme files.

Isolating Hadoop and Cassandra workloads

When you create a keyspace using CQL, Cassandra creates a virtual data center for a cluster, even a one-node cluster, automatically. You assign nodes that run the same type of workload to the same data center. The separate, virtual data centers for different types of nodes segregate workloads running Hadoop from those running Cassandra. Segregating workloads ensures that only one type of workload is active per data center. Separating nodes running a sequential data load, from nodes running any other type of workload, such as Cassandra real-time OLTP queries is a best practice.

Initializing a cluster

Initializing a multiple node cluster (single data center)

This topic contains information for deploying a Cassandra cluster with a single data center. If you're new to Cassandra, and haven't set up a cluster, see [Planning and testing cluster deployments](#) or [10 Minute Cassandra Walkthrough](#).

Prerequisites

Each node must be correctly configured before starting the cluster. You must determine or perform the following before starting the cluster:

- A good understanding of how Cassandra works. At minimum, be sure to read [Understanding the architecture](#) on page 11, especially the Data replication section, and [Cassandra's rack feature](#).
- Install Cassandra on each node.
- Choose a name for the cluster.
- Get the IP address of each node.
- Determine which nodes will be seed nodes. **Do not make all nodes seed nodes.** Please read [Internode communications \(gossip\)](#) on page 13.
- Determine the [snitch](#) and [replication strategy](#). The [GossipingPropertyFileSnitch](#) on page 21 and [NetworkTopologyStrategy](#) are recommended for production environments.

- Determine a naming convention for each rack. For example, good names are RAC1, RAC2 or R101, R102.
- The `cassandra.yaml` configuration file, and property files such as `cassandra-rackdc.properties`, give you more configuration options. See the [Configuration section](#) for more information.

This example describes installing a 6 node cluster spanning 2 racks in a single data center. Each node is already configured to use the [GossipingPropertyFileSnitch](#) and 256 virtual nodes (vnodes).

In Cassandra, "Data center" is synonymous with "replication group". Both terms refer to a set of nodes configured as a group for replication purposes.

Procedure

1. Suppose you install Cassandra on these nodes:

```
node0 110.82.155.0 (seed1)
node1 110.82.155.1
node2 110.82.155.2
node3 110.82.156.3 (seed2)
node4 110.82.156.4
node5 110.82.156.5
```

Note: It is a best practice to have more than one seed node per data center.

2. If you have a firewall running in your cluster, you must open certain ports for communication between the nodes. See .
3. If Cassandra is running, you must stop the server and clear the data:

Doing this removes the default `cluster_name` (Test Cluster) from the system table. All nodes must use the same cluster name.

Windows installations:

- a) Stop Cassandra:

```
C:\> net stop DataStax_Cassandra_Community_Server
```

```
C:\> net stop DataStax_DDC_Server
```

- b) Clear the data:

```
C:\> rmdir /s "Program Files\DataStax-DDC\apache-cassandra\data"
```

4. Set the properties in the `cassandra.yaml` file for each node:

Note: After making any changes in the `cassandra.yaml` file, you must restart the node for the changes to take effect.

Properties to set:

- `cluster_name`:
- `num_tokens`: *recommended value: 256*
- `-seeds`: *internal IP address of each seed node*

In new clusters. Seed nodes don't perform [bootstrap](#) (the process of a new node joining an existing cluster.)

- `listen_address`:

If the node is a seed node, this address must match an IP address in the seeds list. Otherwise, gossip communication fails because it doesn't know that it is a seed.

Initializing a cluster

If not set, Cassandra asks the system for the local address, the one associated with its hostname. In some cases Cassandra doesn't produce the correct address and you must specify the `listen_address`.

- `rpc_address`: *listen address for client connections*
- `endpoint_snitch`: *name of snitch* (See [endpoint_snitch](#).) If you are changing snitches, see [Switching snitches](#) on page 114.
- `auto_bootstrap`: `false` (Add this setting **only** when initializing a fresh cluster with no data.)

Note: If the nodes in the cluster are identical in terms of disk layout, shared libraries, and so on, you can use the same `cassandra.yaml` file on all of them.

Example:

```
cluster_name: 'MyCassandraCluster'
num_tokens: 256
seed_provider:
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider
    parameters:
      - seeds: "110.82.155.0,110.82.155.3"
listen_address:
rpc_address: 0.0.0.0
endpoint_snitch: GossipingPropertyFileSnitch
```

If `rpc_address` is set to a wildcard address (0.0.0.0), then `broadcast_rpc_address` must be set, or the service won't even start.

5. In the `cassandra-rackdc.properties` file, assign the data center and rack names you determined in the Prerequisites. For example:

```
# indicate the rack and dc for this node
dc=DC1
rack=RAC1
```

6. The `GossipingPropertyFileSnitch` always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the `PropertyFileSnitch`.
7. After you have installed and configured Cassandra on all nodes, start the seed nodes one at a time, and then start the rest of the nodes.

Note: If the node has restarted because of automatic restart, you must first stop the node and clear the data directories, as described [above](#).

```
C:\> net start DataStax_DDC_Server
```

8. To check that the ring is up and running, run:

Package installations:

```
C:\> %CASSANDRA_HOME%\bin\nodetool status
```

The output should list each node, and show its status as `UN` (Up Normal).

```
paul@ubuntu:~/cassandra-2.1.0$ bin/nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
// State=Normal/Leaving/Joining/Moving
-- Address                      Load          Tokens       Owns    Host ID                               Rack
UN  10.194.171.160                53.98 KB      256          0.8%    a9fa31c7-f3c0-44d1-b8e7-a2628867840c rack1
UN  10.196.14.48                   93.62 KB      256          9.9%    f5bb146c-db51-475c-a44f-9facf2f1ad6e rack1
UN  10.196.14.239                  83.98 KB      256          8.2%    b8e6748f-ec11-410d-c94f-b8e7d88a28e7 rack1
...
```

Related reference

[Installation locations](#) on page 61

Initializing a multiple node cluster (multiple data centers)

This topic contains information for deploying a Cassandra cluster with multiple data centers. If you're new to Cassandra, and haven't set up a cluster, see [Planning and testing cluster deployments](#) or [10 Minute Cassandra Walkthrough](#).

This example describes installing a six node cluster spanning two data centers. Each node is configured to use the [GossipingPropertyFileSnitch](#) (multiple rack aware) and 256 virtual nodes (vnodes).

In Cassandra, "Data center" is synonymous with "replication group". Both terms refer to a set of nodes configured as a group for replication purposes.

Prerequisites

Each node must be correctly configured before starting the cluster. You must determine or perform the following before starting the cluster:

- A good understanding of how Cassandra works. At minimum, be sure to read [Understanding the architecture](#) on page 11 (especially the [Data replication](#) on page 17 section) and [the rack feature of Cassandra](#).
- Install Cassandra on each node.
- Choose a name for the cluster.
- Get the IP address of each node.
- Determine which nodes will be seed nodes. **Do not make all nodes seed nodes.** Please read [Internode communications \(gossip\)](#) on page 13.
- Determine the [snitch](#) and [replication strategy](#). The [GossipingPropertyFileSnitch](#) on page 21 and [NetworkTopologyStrategy](#) are recommended for production environments.
- Determine a naming convention for each data center and rack. Examples: DC1, DC2 or 100, 200 / RAC1, RAC2 or R101, R102. Choose the name carefully; renaming a data center is not possible.
- The [cassandra.yaml configuration file](#), and property files such as `cassandra-rackdc.properties`, give you more configuration options. See the [Configuration section](#) for more information.

Procedure

1. Suppose you install Cassandra on these nodes:

```
node0 10.168.66.41 (seed1)
node1 10.176.43.66
node2 10.168.247.41
node3 10.176.170.59 (seed2)
node4 10.169.61.170
node5 10.169.30.138
```

Note: It is a best practice to have more than one seed node per data center.

2. If you have a firewall running in your cluster, you must open certain ports for communication between the nodes. See .
3. If Cassandra is running, you must stop the server and clear the data:

Doing this removes the default `cluster_name` (Test Cluster) from the system table. All nodes must use the same cluster name.

Windows installations:

Initializing a cluster

a) Stop Cassandra:

```
C:\> net stop DataStax_Cassandra_Community_Server
```

```
C:\> net stop DataStax_DDC_Server
```

b) Clear the data:

```
C:\> rmdir /s "Program Files\DataStax-DDC\apache-cassandra\data"
```

4. Set the properties in the `cassandra.yaml` file for each node:

Note: After making any changes in the `cassandra.yaml` file, you must restart the node for the changes to take effect.

Properties to set:

- `cluster_name`:
- `num_tokens`: *recommended value: 256*
- `-seeds`: *internal IP address of each seed node*

In new clusters. Seed nodes don't perform [bootstrap](#) (the process of a new node joining an existing cluster.)

- `listen_address`:

If the node is a seed node, this address must match an IP address in the seeds list. Otherwise, gossip communication fails because it doesn't know that it is a seed.

If not set, Cassandra asks the system for the local address, the one associated with its hostname. In some cases Cassandra doesn't produce the correct address and you must specify the `listen_address`.

- `rpc_address`: *listen address for client connections*
- `endpoint_snitch`: *name of snitch* (See [endpoint_snitch](#).) If you are changing snitches, see [Switching snitches](#) on page 114.
- `auto_bootstrap`: `false` (Add this setting **only** when initializing a fresh cluster with no data.)

Note: If the nodes in the cluster are identical in terms of disk layout, shared libraries, and so on, you can use the same `cassandra.yaml` file on all of them.

Example:

```
cluster_name: 'MyCassandraCluster'
num_tokens: 256
seed_provider:
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider
    parameters:
      - seeds: "10.168.66.41,10.176.170.59"
listen_address:
endpoint_snitch: GossipingPropertyFileSnitch
```

Note: Include at least one node from *each* data center in the seeds list.

5. In the `cassandra-rackdc.properties` file, assign the data center and rack names you determined in the Prerequisites. For example:

Nodes 0 to 2

```
## Indicate the rack and dc for this node
dc=DC1
rack=RAC1
```

Nodes 3 to 5

```
## Indicate the rack and dc for this node
dc=DC2
rack=RAC1
```

6. The GossipingPropertyFileSnitch always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the PropertyFileSnitch.

7. After you have installed and configured Cassandra on all nodes, start the seed nodes one at a time, and then start the rest of the nodes.

Note: If the node has restarted because of automatic restart, you must first stop the node and clear the data directories, as described [above](#).

```
C:\> net start DataStax_DDC_Server
```

8. To check that the ring is up and running, run:

Package installations:

```
C:\> %CASSANDRA_HOME%\bin\nodetool status
```

The output should list each node, and show its status as UN (Up Normal).

```
paul@ubuntu:~/cassandra-2.1.0$ bin/nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
// State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens      Owns    Host ID                               Rack
UN  10.194.171.160    53.98 KB      256        0.8%    a9fa31c7-f3c0-44d1-b8e7-a2628867840c rack1
UN  10.196.14.48      93.62 KB      256        9.9%    f5bb146c-db51-475c-a44f-9facf2f1ad6e rack1
UN  10.196.14.239     83.98 KB      256        8.2%    b8e6748f-ec11-410d-c94f-b8e7d88a28e7 rack1
...
```

Related reference

[Installation locations](#) on page 61

Starting and stopping Cassandra on Windows

Steps for starting or stopping the Cassandra Windows service.

Procedure

Starting Cassandra

Note: You must start Cassandra as a service with administrator privileges.

- Net command:

```
C:\> net start DataStax_DDC_Server
```

- Services menu:

- a) From **Start**, select **Control Panel > System and Security > Administrative Tools**.
- b) Select **Services**.
- c) Select **DataStax_DDC_Server** and right-click to start the service.

Stopping Cassandra

Operations

Note: You need administrator privileges to stop Cassandra.

- Net command:

```
C:\> net stop DataStax_DDC_Server
```

- Services menu:
 - a) From **Start**, select **Control Panel > System and Security > Administrative Tools**.
 - b) Select **Services**.
 - c) Select **DataStax_DDC_Server** and right-click to stop the service.

Clearing the data from Windows

There are two options for clearing data from a Windows installation:

Procedure

- To delete all data from the **default** directories, including the commitlog and saved_caches:
 - a) Complete the process of [stopping Cassandra](#).
 - b) Run the following command from the install directory:

```
C:\> rmdir /s "Program Files\DataStax-DDC\apache-cassandra\data"
```

- To delete only the data in the data directory:
 - a) Complete the process of [stopping Cassandra](#).
 - b) Run the following command from the install directory:

```
C:\> rmdir /s "Program Files\DataStax-DDC\data\data"
```

Operations

Adding or removing nodes, data centers, or clusters

Adding nodes to an existing cluster

Virtual nodes (vnodes) greatly simplify adding nodes to an existing cluster:

- Calculating tokens and assigning them to each node is no longer required.
- Rebalancing a cluster is no longer necessary because a node joining the cluster assumes responsibility for an even portion of the data.

For a detailed explanation about how vnodes work, see [Virtual nodes](#) on page 15.

Note: If you do not use vnodes, see [Adding or replacing single-token nodes](#) on page 117.

Procedure

Be sure to install the same version of Cassandra as is installed on the other nodes in the cluster. See [Installing earlier releases](#).

1. Install Cassandra on the new nodes, but do not start Cassandra.

If your Cassandra installation on Debian or Windows installation starts automatically, you must [stop](#) the node and [clear](#) the data.

2. Depending on the snitch used in the cluster, set either the properties in the `cassandra-topology.properties` or the `cassandra-rackdc.properties` file:

- The [PropertyFileSnitch](#) uses the `cassandra-topology.properties` file.
- The [GossipingPropertyFileSnitch](#), [Ec2Snitch](#), [Ec2MultiRegionSnitch](#), and [GoogleCloudSnitch](#) use the `cassandra-rackdc.properties` file.

3. Set the following properties in the `cassandra.yaml` file:

[auto_bootstrap](#)

If this option has been set to false, you must set it to true. This option is not listed in the default `cassandra.yaml` configuration file and defaults to true.

[cluster_name](#)

The name of the cluster the new node is joining.

[listen_address/broadcast_address](#)

Can usually be left blank. Otherwise, use IP address or host name that other Cassandra nodes use to connect to the new node.

[endpoint_snitch](#)

The snitch Cassandra uses for locating nodes and routing requests.

[num_tokens](#)

The number of vnodes to assign to the node. If the hardware capabilities vary among the nodes in your cluster, you can assign a proportional number of vnodes to the larger machines.

[seed_provider](#)

Make sure that the new node lists at least one node in the existing cluster. The `-seeds` list determines which nodes the new node should contact to learn about the cluster and establish the gossip process.

Note: Seed nodes cannot [bootstrap](#). Make sure the new node is not listed in the `-seeds` list. **Do not make all nodes seed nodes.** Please read [Internode communications \(gossip\)](#) on page 13.

Other non-default settings

Change any other non-default settings you have made to your existing cluster in the `cassandra.yaml` file and `cassandra-topology.properties` or `cassandra-rackdc.properties` files. Use the `diff` command to find and merge any differences between existing and new nodes.

4. Start the bootstrap node.
5. Use [nodetool status](#) to verify that the node is fully bootstrapped and all other nodes are up (UN) and not in any other state.
6. After all new nodes are running, run [nodetool cleanup](#) on each of the previously existing nodes to remove the keys that no longer belong to those nodes. Wait for cleanup to complete on one node before running `nodetool cleanup` on the next node.

Cleanup can be safely postponed for low-usage hours.

Related tasks

[Starting or stopping Cassandra](#) on page 107

Related reference

[The nodetool utility](#) on page 149

[Installation locations](#) on page 61

Adding a data center to a cluster

Steps for adding a data center to an existing cluster.

Procedure

Be sure to install the same version of Cassandra as is installed on the other nodes in the cluster. See [Installing earlier releases](#).

1. Make sure that all keyspaces use [NetworkTopologyStrategy](#).
2. Make sure that all keyspaces have a replication factor of 0.
3. For each new node you are adding to the cluster, set the following properties in the `cassandra.yaml` file:
 - a) Add (or edit) `auto_bootstrap: false`.

By default, this setting is true and not listed in the `cassandra.yaml` file. Setting this parameter to false prevents the new nodes from attempting to get all the data from the other nodes in the data center. Until you run [nodetool rebuild](#) in the last step, the new node should not stream data from other nodes, or errors may occur.

- b) Set other properties, such as `-seeds` and `endpoint_snitch`, to match the cluster settings.

For more guidance, see [Initializing a multiple node cluster \(multiple data centers\)](#) on page 105.

Note: Do not make all nodes seeds, see [Internode communications \(gossip\)](#) on page 13.

- c) If you want to enable vnodes, set `num_tokens`.

The recommended value is 256. Do not set the `initial_token` parameter.

4. Update the relevant property file for snitch used on all servers to include the new nodes. You do not need to restart.
 - [GossipingPropertyFileSnitch](#) on page 21: `cassandra-rackdc.properties`
 - [PropertyFileSnitch](#): `cassandra-topology.properties`
5. The `GossipingPropertyFileSnitch` always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the `PropertyFileSnitch`.
6. Ensure that your clients are configured correctly for the new cluster:
 - If your client uses the DataStax Java, C#, or Python driver, set the load-balancing policy to `DCAwareRoundRobinPolicy` ([Java](#), [C#](#), [Python](#)).
7. If using a QUORUM [consistency level](#) for reads or writes, check whether the `LOCAL_QUORUM` or `EACH_QUORUM` meets your requirements for multiple datacenters.
8. If using a ONE [consistency level](#) for reads or writes, check whether the `LOCAL_ONE` consistency level meets your requirements for multiple data centers.
9. Start Cassandra on the new nodes.
10. After all nodes are running in the cluster:
 - a) Change the [keyspace properties](#) to specify the desired replication factor for the new data center.

For example, set strategy options to `DC1:2, DC2:2`:

```
ALTER KEYSPACE cycling
WITH replication = {'class': 'NetworkTopologyStrategy', 'DC1' : 1,
                    'DC2' : 2}
```

For more information, see [ALTER KEYSPACE](#).

- b) Run `nodetool rebuild` specifying the existing data center on all nodes in the new data center:

```
C:\> %CASSANDRA_HOME%\bin\nodetool rebuild -- name_of_existing_data_center
```

Otherwise, requests to the new data center with `LOCAL_ONE` or `ONE` consistency levels may fail if the existing data centers are not completely in-sync.

You can run `rebuild` on one or more nodes at the same time. The choices depends on whether your cluster can handle the extra IO and network pressure of running on multiple nodes. Running on one node at a time has the least impact on the existing cluster.

Attention: If you don't specify the existing data center in the command line, the new nodes will appear to rebuild successfully, but will not contain any data.

11. Change to true or remove `auto_bootstrap: false` in the `cassandra.yaml` file.

This returns this parameter to its normal setting, which allows the node to get all the data from the other nodes in the data center if it is restarted.

Related tasks

[Starting or stopping Cassandra](#) on page 107

Related reference

[Installation locations](#) on page 61

Replacing a dead node or dead seed node

Steps to replace a node that has died for some reason, such as hardware failure. Prepare and start the replacement node, then attach it to the cluster. After the replacement node is running in the cluster, [remove the dead node](#).

Replacing a dead seed node

1. Promote an existing node to a seed node by adding its IP address to `-seeds` list and remove the IP address of the dead seed node from the `cassandra.yaml` file for each node in the cluster.
2. Replace the dead node, as described in the next section.

Replacing a dead node

You must prepare and start the replacement node, integrate it into the cluster, and then remove the dead node.

Procedure

Be sure to install the same version of Cassandra as is installed on the other nodes in the cluster. See [Installing earlier releases](#).

1. Confirm that the node is dead using `nodetool status`:

The `nodetool` command shows a down status for the dead node (DN):


```
paul@ubuntu:~/cassandra-2.1.0$ bin/nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
// State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens      Owns    Host ID                               Rack
UN 10.194.171.160    53.98 KB      256         0.8%    a9fa31c7-f3c0-44d1-b8e7-a2628867840c rack1
UN 10.196.14.48      93.62 KB      256         9.9%    f5bb146c-db51-475c-a44f-9facf2f1ad6e rack1
DN 10.196.14.239     ?             256         8.2%    null
```

2. Note the Address of the dead node; it is used in [step 5](#).

3. Install Cassandra on the new node, but do not start Cassandra.

If Windows has started Cassandra automatically, you must [stop](#) the node and [clear](#) the data.

4. Depending on the snitch used in the cluster, set either the properties in the `cassandra-topology.properties` or the `cassandra-rackdc.properties` file:

- The [PropertyFileSnitch](#) uses the `cassandra-topology.properties` file.
- The [GossipingPropertyFileSnitch](#), [Ec2Snitch](#), [Ec2MultiRegionSnitch](#), and [GoogleCloudSnitch](#) use the `cassandra-rackdc.properties` file.

Note: The [GossipingPropertyFileSnitch](#) always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the [PropertyFileSnitch](#).

5. Set the following properties in the `cassandra.yaml` file:

[auto_bootstrap](#)

If this option has been set to false, you must set it to true. This option is not listed in the default `cassandra.yaml` configuration file and defaults to true.

6. Start the replacement node with the [replace_address](#) option:

Add the following option to the `cassandra-env.ps1` file:

```
$env:JVM_OPTS="$env:JVM_OPTS -
Dcassandra.replace_address=address_of_dead_node"
```

7. If using a packaged install, after the new node finishes bootstrapping, remove the option you added in [step 5](#).

What to do next

- Wait at least 72 hours to ensure that [gossip](#) removes the old node information from the cluster.
- Remove the old node's IP address from the `cassandra-topology.properties` or `cassandra-rackdc.properties` file.

CAUTION: If you do not wait long enough for gossip to remove the old node information before you remove the IP address from the property file too soon, problems may result.

- [Remove the node](#).

Replacing a running node

Steps to replace a node with a new node, such as when updating to newer hardware or performing proactive maintenance.

You must prepare and start the replacement node, integrate it into the cluster, and then decommission the old node.

Note: To change the IP address of a node, simply change the IP of node and then restart Cassandra. If you change the IP address of a seed node, you must update the `-seeds` parameter in the `seed_provider` for each node in the `cassandra.yaml` file.

Procedure

Be sure to install the same version of Cassandra as is installed on the other nodes in the cluster. See [Installing earlier releases](#).

1. Prepare and start the replacement node, as described in [Adding nodes to an existing cluster](#).

Note: If not using vnodes, see [Adding or replacing single-token nodes](#) on page 117.

2. Confirm that the replacement node is alive:

- Run `nodetool ring` if not using vnodes.
- Run `nodetool status` if using vnodes.

The status should show:

- `nodetool ring: Up`
- `nodetool status: UN`

3. Note the `Host ID` of the original node; it is used in the next step.
4. Using the `Host ID` of the original node, decommission the original node from the cluster using the `nodetool decommission` command.

Related tasks

[Removing a node](#) on page 114

Moving a node from one rack to another

A common task is moving a node from one rack to another. For example, when using `GossipPropertyFileSnitch`, a common error is mistakenly placing a node in the wrong rack. To correct the error, use one of the following procedures.

- The preferred method is to [decommission the node](#) and re-add it to the correct rack and data center.
 - This method takes longer to complete than the alternative method. Data is moved that the decommissioned node doesn't need anymore. Then the node gets new data while bootstrapping. The alternative method does both operations simultaneously.
- An alternative method is to [update the node's topology](#) and restart the node. Once the node is up, run a [full repair](#) on the cluster.

CAUTION: This method is not preferred because until the repair is completed, the node may blindly handle requests for data the node doesn't yet have. To mitigate this problem with request handling, start the node with `-Dcassandra.join_ring=false` after repairing once, then fully join the node to the cluster using the [JMX method](#) `org.apache.cassandra.db.StorageService.joinRing()`. The node will be less likely to be out of sync with other nodes before it serves any requests. After joining the node to the cluster, repair the node again, so that any writes missed during the first repair will be captured.

Decommissioning a data center

Steps to properly remove a data center so no information is lost.

Procedure

1. Make sure no clients are still writing to any nodes in the data center.

2. Run a full repair with [nodetool repair](#).

This ensures that all data is propagated from the data center being decommissioned.

3. [Change all keyspaces](#) so they no longer reference the data center being removed.
4. Run [nodetool decommission](#) on every node in the data center being removed.

Removing a node

Use these instructions when you want to remove nodes to reduce the size of your cluster, not for [replacing a dead node](#).

Attention: If you are not using [virtual nodes](#) (vnodes), you must rebalance the cluster.

Procedure

- Check whether the node is up or down using [nodetool status](#):

The nodetool command shows the status of the node (UN=up, DN=down):

```
paul@ubuntu:~/cassandra-1.2.0$ bin/nodetool status
Datacenter: datacenter1
=====
Status=Up/Down
// State=Normal/Leaving/Joining/Moving
-- Address                Load          Tokens       Owns    Host ID                               Rack
UN  10.194.171.160         53.98 KB      256          0.8%    a9fa31c7-f3c0-44d1-b8e7-a2628867840c rack1
UN  10.196.14.48           93.62 KB      256          9.9%    f5bb146c-db51-475c-a44f-9facf2f1ad6e rack1
DN  10.196.14.239           ?              256          8.2%    null
```

- If the node is up, run [nodetool decommission](#).

This assigns the ranges that the node was responsible for to other nodes and replicates the data appropriately.

Use [nodetool netstats](#) to monitor the progress.

- If the node is down, choose the appropriate option:
 - If the cluster uses vnodes, remove the node using the [nodetool removemode](#) command.
 - If the cluster does not use vnodes, before running the [nodetool removemode](#) command, [adjust your tokens](#) to evenly distribute the data across the remaining nodes to avoid creating a hot spot.
- If [removemode](#) fails, run [nodetool assassinate](#).

Switching snitches

Because [snitches](#) determine how Cassandra distributes replicas, the procedure to switch snitches depends on whether or not the topology of the cluster will change:

- If data has not been inserted into the cluster, there is no change in the network topology. This means that you only need to set the snitch; no other steps are necessary.
- If data has been inserted into the cluster, it's possible that the topology has changed and you will need to perform additional steps.
- If data has been inserted into the cluster that must be kept, change the snitch without changing the topology. Then add a new data center with new nodes and racks as desired. Finally, remove nodes from the old data centers and racks. Simply altering the snitch and replication to move some nodes to a new data center will result in data being replicated incorrectly.

A change in topology means that there is a change in the data centers and/or racks where the nodes are placed. Topology changes may occur when the replicas are placed in different places by the new snitch. Specifically, the replication strategy places the replicas based on the information provided by the new snitch. The following examples demonstrate the differences:

- **No topology change**

Change from: five nodes using the [SimpleSnitch](#) in a single data center

To: five nodes in one data center and 1 rack using a network snitch such as the [GossipingPropertyFileSnitch](#)

- **Topology changes**

- **Change from:** 5 nodes using the SimpleSnitch in a single data center

To: 5 nodes in 2 data centers using the [PropertyFileSnitch](#) (add a data center).

Note: If "splitting" one data center into two, [create a new data center](#) with new nodes. [Alter the keyspace](#) replication settings for the [keyspace](#) that originally existed to reflect that two data centers now exist. Once data is replicated to the new data center, remove the number of nodes from the original data center that have "moved" to the new data center.

- **Change From:** 5 nodes using the SimpleSnitch in a single data center

To: 5 nodes in 1 data center and 2 racks using the [RackInferringSnitch](#) (add rack information).

Procedure

Steps for switching snitches:

1. Create a properties file with datacenter and rack information.

- `cassandra-rackdc.properties`

[GossipingPropertyFileSnitch](#) on page 21, [Ec2Snitch](#), and [Ec2MultiRegionSnitch](#) only.

- `cassandra-topology.properties`

All other network snitches.

2. Copy the `cassandra-rackdc.properties` or `cassandra-topology.properties` file to the Cassandra configuration directory on all the cluster's nodes. They won't be used until the new snitch is enabled.

3. Change the snitch for each node in the cluster in the node's `cassandra.yaml` file. For example:

```
endpoint_snitch: GossipingPropertyFileSnitch
```

4. If the topology has not changed, you can restart each node one at a time.

Any change in the `cassandra.yaml` file requires a node restart.

5. If the topology of the network has changed, but no data centers are added:

- a) Shut down all the nodes, then restart them.

- b) Run a [sequential repair](#) and [nodetool cleanup](#) on each node.

6. If the topology of the network has changed and a data center is added:

- a) [Create a new data center](#).

- b) Replicate data into new data center. [Remove nodes](#) from old data center.

- c) Run a [sequential repair](#) and [nodetool cleanup](#) on each node.

Related concepts

[Snitches](#) on page 19

Changing keyspace replication strategy

A keyspace is created with a strategy. For development work, the `SimpleStrategy` class is acceptable. For production work, the `NetworkTopologyStrategy` class must be set. To change the strategy, two steps are required. Altering the distribution of nodes within multiple data centers when data is present should be accomplished by adding a data center, and then adding data to the new nodes in the new data center and removing nodes from the old data center.

Procedure

- [Change the snitch](#) to a network-aware setting.
- Alter the keyspace properties using the `ALTER KEYSPACE` command. For example, the keyspace cycling set to `SimpleStrategy` is switched to `NetworkTopologyStrategy` for a single data center `DC1`.

```
cqlsh> ALTER KEYSPACE cycling WITH REPLICATION = {'class' :
'NetworkTopologyStrategy', 'DC1' : 3};
```

- Alter the keyspace properties using the `ALTER KEYSPACE` command. For example, the keyspace cycling set to `SimpleStrategy` is switched to `NetworkTopologyStrategy`. Altering a keyspace to add a data center involves additional steps. Simply altering the keyspace may lead to faulty data replication. See [switching snitches](#) for additional information.

```
cqlsh> ALTER KEYSPACE cycling WITH REPLICATION = {'class' :
'NetworkTopologyStrategy', 'DC1' : 3, 'DC2' : 2 };
```

- Run [nodetool-repair](#) on each node that is affected by the change. For details, see [Updating the replication factor](#)

It is possible to restrict the replication of a keyspace to selected data centers, or a single data center. To do this, use the `NetworkTopologyStrategy` and set the replication factors of the excluded data centers to 0 (zero), as in the following example:

```
cqlsh> ALTER KEYSPACE cycling WITH REPLICATION = {'class' :
'NetworkTopologyStrategy', 'DC1' : 0, 'DC2' : 3, 'DC3' : 0 };
```

Edge cases for transitioning or migrating a cluster

The information in this topic is intended for the following types of scenarios (without any interruption of service):

- Transition a cluster on EC2 to a cluster on Amazon virtual private cloud (VPC).
- Migrate from a cluster when the network separates the current cluster from the future location.
- Migrate from an early Cassandra cluster to a recent major version.

Procedure

The following method ensures that if something goes wrong with the new cluster, you still have the existing cluster until you no longer need it.

1. Set up and configure the new cluster as described in [Initializing a cluster](#) on page 102.

Note: If you're not using `vnodes`, be sure to configure the token ranges in the new nodes to match the ranges in the old cluster.

2. Set up the schema for the new cluster using [CQL](#).

3. Configure your client to write to both clusters.

Depending on how the writes are done, code changes may be needed. Be sure to use identical consistency levels.

4. Ensure that the data is flowing to the new nodes so you won't have any gaps when you copy the snapshots to the new cluster in step 6.

5. [Snapshot](#) the old EC2 cluster.

6. Copy the data files from your keyspaces to the nodes.

- You may be able to copy the data files to their matching nodes in the new cluster, which is simpler and more efficient. This will work if:
 - You are not using vnodes
 - The destination is not a different version of Cassandra
 - The node ratio is 1:1
- If the clusters are different sizes or if you are using vnodes, use the [sstableloader \(Cassandra bulk loader\)](#) on page 237 (sstableloader).

7. You can either switch to the new cluster all at once or perform an incremental migration.

For example, to perform an incremental migration, you can set your client to designate a percentage of the reads that go to the new cluster. This allows you to test the new cluster before decommissioning the old cluster.

8. Decommission the old cluster, as described in [Decommissioning a data center](#) on page 113.

Adding or replacing single-token nodes

This topic applies only to clusters using single-token architecture, not vnodes.

About adding Capacity to an Existing Cluster

Cassandra allows you to add capacity to a cluster by introducing new nodes to the cluster in stages and by adding an entire data center. When a new node joins an existing cluster, it needs to know:

- Its position in the ring and the range of data it is responsible for, which is assigned by the [initial_token](#) and the [partitioner](#).
- The [seed](#) nodes to contact for learning about the cluster and establish the [gossip process](#).
- The name of the cluster it is joining and how the node should be addressed within the cluster.
- Any other non-default settings made to `cassandra.yaml` on your existing cluster.

When you add one or more nodes to a cluster, you must calculate the tokens for the new nodes. Use one of the following approaches:

Add capacity by doubling the cluster size

Adding capacity by doubling (or tripling or quadrupling) the number of nodes is less complicated when assigning tokens. Existing nodes can keep their existing token assignments, and new nodes are assigned tokens that bisect (or trisect) the existing token ranges. For example, when you generate tokens for six nodes, three of the generated token values will be the same as if you generated for three nodes. To clarify, you first obtain the token values that are already in use, and then assign the newly calculated token values to the newly added nodes.

Recalculate new tokens for all nodes and move nodes around the ring

When increasing capacity by a non-uniform number of nodes, you must recalculate tokens for the entire cluster, and then use [nodetool move](#) to assign the new tokens to the existing nodes. After all nodes are restarted with their new token assignments, run a [nodetool cleanup](#) to remove unused keys on all nodes. These operations are resource intensive and should be done during low-usage times.

CAUTION:

When configuring the new node in Cassandra2.1 or later, you must supply a value for the `initial_token` property. If you leave this property with no value, Cassandra assigns this node a random token range. Adding nodes with random token range assignments results in a badly unbalanced ring.

Adding Nodes to a Cluster

1. Calculate the tokens for the nodes based on the expansion strategy you are using the [Token Generating Tool](#).
2. Install and configure Cassandra on each new node:
 - a. [Install Cassandra](#) on the node
 - b. If your Cassandra installation on Debian or Windows installation starts automatically, you must [stop](#) the node and [clear](#) the data.
 - c. Edit the `cassandra.yaml` on the new node:

`auto_bootstrap`

If this option has been set to false, you must set it to true. This option is not listed in the default `cassandra.yaml` configuration file and defaults to true.

`cluster_name`

The name of the cluster the new node is joining.

`listen_address/broadcast_address`

Can usually be left blank. Otherwise, use IP address or host name that other Cassandra nodes use to connect to the new node.

`endpoint_snitch`

The snitch Cassandra uses for locating nodes and routing requests.

`initial_token`

Set this property according to your token calculations.

`seed_provider`

Make sure that the new node lists at least one node in the existing cluster. The `-seeds` list determines which nodes the new node should contact to learn about the cluster and establish the gossip process.

Note: Seed nodes cannot [bootstrap](#). Make sure the new node is not listed in the `-seeds` list. **Do not make all nodes seed nodes.** Please read [Internode communications \(gossip\)](#) on page 13.

Other non-default settings

Change any other non-default settings you have made to your existing cluster in the `cassandra.yaml` file and `cassandra-topology.properties` or `cassandra-rackdc.properties` files. Use the `diff` command to find and merge any differences between existing and new nodes.

3. By default, the new nodes are configured for consistent range movement. To reconfigure each new node for non-strict range movement:
4. Start Cassandra on the new nodes:

If you have added more than one node, and configured the new nodes for consistent range movement (the default), start the nodes serially.

If you have configured the new nodes for non-strict range movement, allow **two** minutes between node initializations.

You can monitor the startup and data streaming process using [nodetool netstats](#).

- 5.
- 6.
7. Start Cassandra on each new node. If consistent range movement is configured (default), add nodes serially if more than one node is added. If non-strict range movement is desired, use

the flag `-Dcassandra.consistent.rangemovement=false` to disable strict range movement and allow overlapping range movement.

8. After the new nodes are fully bootstrapped, assign the new `initial_token` property value to the nodes that required new tokens, and then run `nodetool move new_token`, one node at a time.
9. After all nodes have their new tokens assigned, run `nodetool cleanup` one node at a time for each node. Wait for cleanup to complete before doing the next node. This step removes the keys that no longer belong to the previously existing nodes.

Note: Cleanup may be safely postponed for low-usage hours.

Adding a Data Center to a Cluster

Before starting this procedure, please read the guidelines in [Adding Capacity to an Existing Cluster](#) above.

1. Ensure that you are using `NetworkTopologyStrategy` for all of your keyspaces.
2. For each new node, edit the configuration properties in the `cassandra.yaml` file:
 - Set `auto_bootstrap` to `False`.
 - Set the `initial_token`. Be sure to offset the tokens in the new data center, see [Generating tokens](#) on page 100.
 - Set the `cluster_name`.
 - Set any other non-default settings.
 - Set the [seed lists](#). Every node in the cluster must have the same list of seeds and include at least one node from each data center. Typically one to three seeds are used per data center.
3. Update either the `cassandra-rackdc.properties` (`GossipingPropertyFileSnitch`) or `cassandra-topology.properties` (`PropertyFileSnitch`) on all servers to include the new nodes. You do not need to restart.
4. Ensure that your client does not auto-detect the new nodes so that they aren't contacted by the client until explicitly directed.
5. If using a `QUORUM consistency level` for reads or writes, check the `LOCAL_QUORUM` or `EACH_QUORUM` consistency level to make sure that the level meets the requirements for multiple data centers.
6. [Start the new nodes](#).
7. The `GossipingPropertyFileSnitch` always loads `cassandra-topology.properties` when that file is present. Remove the file from each node on any new cluster, or any cluster migrated from the `PropertyFileSnitch`.
8. After all nodes are running in the cluster:
 - a. Change the [replication factor](#) for your keyspace for the expanded cluster.
 - b. Run `nodetool rebuild` on each node in the new data center.

Replacing a Dead Node

1. Confirm that the node is dead using the `nodetool ring` command on any live node in the cluster.

The `nodetool ring` command shows a *Down* status for the token value of the dead node:

```
$ nodetool ring -h localhost
```

Address	DC	Rack	Status	State	Load	Owns	Token
10.46.123.11	datacenter1	rack1	Up	Normal	179.58 KB	16.67%	0
10.46.123.12	datacenter1	rack1	Down	Normal	315.21 KB	16.67%	28356863910078205288614550619314017621
10.46.123.13	datacenter1	rack1	Up	Normal	267.71 KB	16.67%	56713727820156410577229101238628035242
10.46.123.14	datacenter1	rack1	Up	Normal	315.21 KB	16.67%	85070591730234615865843651857942052863
10.46.123.15	datacenter1	rack1	Up	Normal	292.36 KB	16.67%	113427455640312821154458202477256070485
10.46.123.16	datacenter1	rack1	Up	Normal	300.02 KB	16.67%	141784319550391026443072753096570088106

2. [Install Cassandra](#) on the replacement node.
3. Remove any preexisting Cassandra data on the replacement node:


```
C:\> rmdir /s "Program Files\DataStax-DDC\apache-cassandra\data"
```

4. Set `auto_bootstrap: true`. (If `auto_bootstrap` is not in the `cassandra.yaml` file, it automatically defaults to `true`.)
5. Set the `initial_token` in the `cassandra.yaml` file to the value of the dead node's token -1. Using the value from the above graphic, this is 28356863910078205288614550619314017621-1:

```
initial_token: 28356863910078205288614550619314017620
```

6. Configure any non-default settings in the node's `cassandra.yaml` to match your existing cluster.
7. [Start the new nodes](#).
8. After the new node has finished bootstrapping, check that it is marked up using the `nodetool ring` command.
9. Run [nodetool repair](#) on each keyspace to ensure the node is fully consistent. For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool repair -h 10.46.123.12 keyspace_name
```

10. Remove the dead node.

Backing up and restoring data

About snapshots

Cassandra backs up data by taking a snapshot of all on-disk data files (SSTable files) stored in the data directory. You can take a snapshot of all keyspaces, a single keyspace, or a single table while the system is online.

Using a parallel ssh tool (such as `pssh`), you can snapshot an entire cluster. This provides an *eventually consistent* backup. Although no one node is guaranteed to be consistent with its replica nodes at the time a snapshot is taken, a restored snapshot resumes consistency using Cassandra's built-in consistency mechanisms.

After a system-wide snapshot is performed, you can enable incremental backups on each node to backup data that has changed since the last snapshot: each time a memtable is flushed to disk and an SSTable is created, a hard link is copied into a `/backups` subdirectory of the data directory (provided JNA is enabled). Compacted SSTables will not create hard links in `/backups` because these SSTables do not contain any data that has not already been linked.

Taking a snapshot

Snapshots are taken per node using the [nodetool snapshot](#) command. To take a global snapshot, run the `nodetool snapshot` command using a parallel ssh utility, such as `pssh`.

A snapshot first flushes all in-memory writes to disk, then makes a hard link of the SSTable files for each keyspace. You must have enough free disk space on the node to accommodate making snapshots of your data files. A single snapshot requires little disk space. However, snapshots can cause your disk usage to grow more quickly over time because a snapshot prevents old obsolete data files from being deleted. After the snapshot is complete, you can move the backup files to another location if needed, or you can leave them in place.

Note: Cassandra can only restore data from a snapshot when the table schema exists. It is recommended that you also backup the schema. See `DESCRIBE SCHEMA` in [DESCRIBE](#).

Procedure

Run the `nodetool snapshot` command, specifying the hostname, JMX port, and keyspace. For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h localhost -p 7199 snapshot mykeyspace
```

Results

The snapshot is created in `data_directory\keyspace_name\table_name-UUID\snapshots\snapshot_name` directory. Each snapshot directory contains numerous `.db` files that contain the data at the time of the snapshot.

For example:

```
C:\Program Files\DataStax-DDC\mykeyspace
\users-081a1500136111e482d09318a3b15cc2\snapshots\1406227071618\mykeyspace-
users-ka-1-Data.db
```

Deleting snapshot files

When taking a snapshot, previous snapshot files are not automatically deleted. You should remove old snapshots that are no longer needed.

The `nodetool clearsnapshot` command removes all existing snapshot files from the snapshot directory of each keyspace. You should make it part of your back-up process to clear old snapshots before taking a new one.

Procedure

1. To delete all snapshots for a node, run the `nodetool clearsnapshot` command. For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h localhost -p 7199 clearsnapshot
```

To delete snapshots on all nodes at once, run the `nodetool clearsnapshot` command using a parallel `ssh` utility.

2. To delete a single snapshot, run the `clearsnapshot` command with the snapshot name:

```
C:\> %CASSANDRA_HOME%\bin\nodetool clearsnapshot -t <snapshot_name>
```

The file name and path vary according to the type of snapshot. See [nodetools snapshot](#) for details about snapshot names and paths.

Enabling incremental backups

When incremental backups are enabled (disabled by default), Cassandra hard-links each memtable-flushed SSTable to a backups directory under the keyspace data directory. This allows storing backups offsite without transferring entire snapshots. Also, incremental backups combined with snapshots to provide a dependable, up-to-date backup mechanism. Compacted SSTables will not create hard links in `/backups` because these SSTables do not contain any data that has not already been linked. A snapshot at a point in time, plus all incremental backups and commit logs since that time form a complete backup.

As with snapshots, Cassandra does not automatically clear incremental backup files. DataStax recommends setting up a process to clear incremental backup hard-links each time a new snapshot is created.

Procedure

Edit the `cassandra.yaml` configuration file on each node in the cluster and change the value of `incremental_backups` to `true`.

Restoring from a snapshot

Restoring a keyspace from a snapshot requires all snapshot files for the table, and if using incremental backups, any incremental backup files created after the snapshot was taken. Streamed SSTables (from repair, decommission, and so on) are also hardlinked and included.

Note: Restoring from snapshots and incremental backups temporarily causes intensive CPU and I/O activity on the node being restored.

Restoring from local nodes

This method copies the SSTables from the snapshots directory into the correct data directories.

1. Make sure the table schema exists.

Cassandra can only restore data from a snapshot when the table schema exists. If the schema does not exist and has not been backed up, you must recreate the schema.

2. If necessary, `truncate` the table.

Note: You may not need to truncate under certain conditions. For example, if a node lost a disk, you might restart before restoring so that the node continues to receive new writes before starting the restore procedure.

Truncating is usually necessary. For example, if there was an accidental deletion of data, the tombstone from that delete has a later write timestamp than the data in the snapshot. If you restore without truncating (removing the tombstone), Cassandra continues to shadow the restored data. This behavior also occurs for other types of overwrites and causes the same problem.

3. Locate the most recent snapshot folder. For example:

```
data_directory\keyspace_name\table_name-UUID\snapshots\snapshot_name
```

4. Copy the most recent snapshot SSTable directory to the `data_directory\keyspace\table_name-UUID` directory.
5. Run `nodetool refresh`.

Restoring from centralized backups

This method uses `sstableloader` to restore snapshots.

1. Make sure the table schema exists.

Cassandra can only restore data from a snapshot when the table schema exists. If the schema does not exist and has not been backed up, you must recreate the schema.

2. If necessary, `truncate` the table.

Note: You may not need to truncate under certain conditions. For example, if a node lost a disk, you might restart before restoring so that the node continues to receive new writes before starting the restore procedure.

Truncating is usually necessary. For example, if there was an accidental deletion of data, the tombstone from that delete has a later write timestamp than the data in the snapshot. If you restore without truncating (removing the tombstone), Cassandra continues to shadow the restored data. This behavior also occurs for other types of overwrites and causes the same problem.

3. Restore the most recent snapshot using the `sstableloader` tool on the backed-up SSTables.

The sstableloader streams the SSTables to the correct nodes. You do not need to remove the commitlogs or drain or restart the nodes.

Restoring a snapshot into a new cluster

Suppose you want to copy a snapshot of SSTable data files from a three node Cassandra cluster with vnodes enabled (256 tokens) and recover it on another newly created three node cluster (256 tokens). The token ranges will not match, because the token ranges cannot be exactly the same in the new cluster. You need to specify the tokens for the new cluster that were used in the old cluster.

Note: This procedure assumes you are familiar with [restoring a snapshot](#) and configuring and [initializing a cluster](#).

Procedure

To recover the snapshot on the new cluster:

1. From the old cluster, retrieve the list of tokens associated with each node's IP:

```
C:\> nodetool ring ip_address_of_node
```

2. Copy the output of the `nodetool ring` into a spreadsheet (space-delimited).
3. Edit the output, keeping the list of tokens and deleting the other columns,.
4. In the `cassandra.yaml` file for each node in the new cluster, add the list of tokens you obtained in the previous step to the `initial_token` parameter using the same `num_tokens` setting as in the old cluster.
5. Make any other necessary changes in the new cluster's `cassandra.yaml` and property files so that the new nodes match the old cluster settings. Make sure the seed nodes are set for the new cluster.
6. Clear the system table data from each new node:

```
C:\> rmdir /s "Program Files\DataStax-DDC\apache-cassandra\data"
```

This allows the new nodes to use the initial tokens defined in the `cassandra.yaml` when they restart.

7. Start each node using the specified list of token ranges in new cluster's `cassandra.yaml`:

```
initial_token: -9211270970129494930, -9138351317258731895,
               -8980763462514965928, ...
```

8. Create schema in the new cluster. All the schemas from the old cluster must be reproduced in the new cluster.
9. [Stop the node](#). Using `nodetool refresh` is unsafe because files within the data directory of a running node can be silently overwritten by identically named just-flushed SSTables from memtable flushes or compaction. Copying files into the data directory and restarting the node will not work for the same reason.
10. [Restore the SSTable files snapshotted](#) from the old cluster onto the new cluster using the same directories, while noting that the UUID component of target directory names has changed. Without restoration, the new cluster will not have data to read upon restart.
11. Restart the node.

Recovering from a single disk failure using JBOD

How to recover from a single disk failure in a disk array using JBOD (just a bunch of disks).

Node can restart

1. [Stop Cassandra](#) and shut down the node.
2. Replace the failed disk.
3. Start the node and [Cassandra](#).
4. Run [nodetool repair](#) on the node.

Node cannot restart

If the node cannot restart, it is possible the system directory is corrupted. If the node cannot restart after completing these steps, see [Replacing a dead node or dead seed node](#) on page 111.

If using the node uses vnodes:

1. [Stop Cassandra](#) and shut down the node.
2. Replace the failed disk.
3. On a healthy node run the following command:

```
C:\> nodetool ring ip_address_of_node
```

4. Copy the output of the `nodetool ring` into a spreadsheet (space-delimited).
5. Edit the output, keeping the list of tokens and deleting the other columns,.
6. On the node with the new disk, add the list of tokens from the previous step (separated by commas), under [initial_token](#) in the `cassandra.yaml` file.
7. Clear each `system` directory for every functioning drive:

Assuming disk1 has failed and the [data_file_directories](#) setting in the `cassandra.yaml` for each drive is:

```
- \data1\cassandra\data
- \data2\cassandra\data
- \data3\cassandra\data
```

Run the following commands:

```
C:\> rmdir /s \data2\cassandra\data\system
C:\> rmdir /s \data3\cassandra\data\system
```

8. Start the node and [Cassandra](#).
9. Run [nodetool repair](#).
10. After the node is fully integrated into the cluster, it is recommended to return to normal vnode settings:
 - Set [num_tokens](#) to the correct `number_of_tokens`
 - Comment out the [#initial_token](#) setting

If the node uses assigned tokens (single-token architecture):

1. [Stop Cassandra](#) and shut down the node.
2. Replace the failed disk.
3. Clear each `system` directory for every functioning drive:

Assuming disk1 has failed and the [data_file_directories](#) setting in the `cassandra.yaml` for each drive is:

```
- \data1\cassandra\data
- \data2\cassandra\data
- \data3\cassandra\data
```

Run the following commands:

```
C:\> rmdir /s \data2\cassandra\data\system
C:\> rmdir /s \data3\cassandra\data\system
```

4. Start the node and [Cassandra](#).
5. Run [nodetool repair](#) on the node.

Repairing nodes

Over time, data in a replica can become inconsistent with other replicas due to the distributed nature of the database. Node repair corrects the inconsistencies so that eventually all nodes have the same and most up-to-date data. It is an important part of regular maintenance for every Cassandra cluster.

Cassandra provides the following repair processes:

- [Hinted Handoff](#)

If a node becomes unable to receive a particular write, the write's coordinator node preserves the data to be written as a set of *hints*. When the node comes back online, the coordinator effects repair by handing off hints so that the node can catch up with the required writes.

- [Read Repair](#)

During the read path, a query assembles data from several nodes. The coordinator node for this write compares the data from each replica node. If any replica node has outdated data, the coordinator node sends it the most recent version. The scope of this type of repair depends on the keyspace's replication factor. During a write, Cassandra collects only enough replica data to satisfy the replication factor, and only performs read repair on nodes that participate in that write operation.

But Cassandra can also choose a write at random and perform read repair on all replicas, regardless of the replication factor.

- [Anti-Entropy Repair](#)

Cassandra provides the [nodetool repair](#) tool, which you can use to repair recovering nodes, and which you should use as part of regular maintenance purposes.

You can use Cassandra settings or Cassandra tools to configure each type of repair. For details on when to use each type of repair and how to configure each one, see the pages listed above.

Hinted Handoff: repair during write path

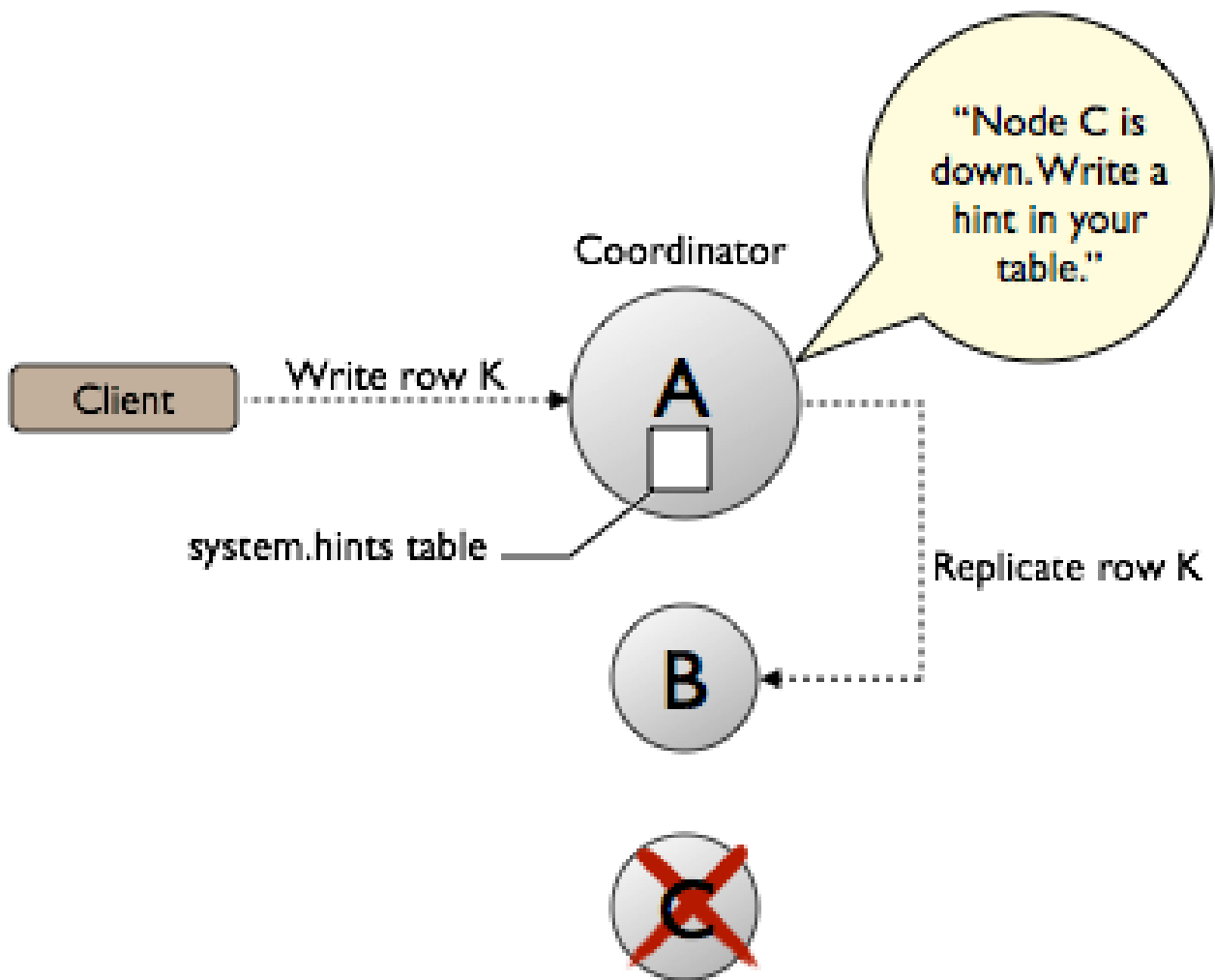
On occasion, a node becomes unresponsive while data is being written. Reasons for unresponsiveness are hardware problems, network issues, or overloaded nodes that experience long garbage collection (GC) pauses. By design, hinted handoff inherently allows Cassandra to continue performing the same number of writes even when the cluster is operating at reduced capacity.

After the failure detector marks a node as down, missed writes are stored by the coordinator for a period of time, if hinted handoff is [enabled](#) in the `cassandra.yaml` file. In Cassandra 3.0 and later, the hint is stored in a local hints directory on each node for improved replay. The hint consists of a target ID for the downed node, a hint ID that is a time UUID for the data, a message ID that identifies the Cassandra version, and the data itself as a blob. Hints are flushed to disk every 10 seconds, reducing the staleness of the hints. When gossip discovers when a node has come back online, the coordinator replays each remaining hint to write the data to the newly-returned node, then deletes the hint file. If a node is down for longer than [max_hint_window_in_ms](#) (3 hours by default), the coordinator stops writing new hints.

The coordinator also checks every ten minutes for hints corresponding to writes that timed out during an outage too brief for the failure detector to notice through gossip. If a replica node is overloaded or unavailable, and the failure detector has not yet marked the node as down, then expect most or all writes to that node to fail after the timeout triggered by [write_request_timeout_in_ms](#), (10 seconds by default). The coordinator returns a `TimeoutException` exception, and the write will fail but a hint will be stored. If several nodes experience brief outages simultaneously, substantial memory pressure can build up on the coordinator. The coordinator tracks how many hints it is currently writing, and if the number increases too much, the coordinator refuses writes and throws the `OverloadedException` exception.

The consistency level of a write request affects whether hints are written and a write request subsequently fails. If the cluster consists of two nodes, A and B, with a replication factor of 1, each row is stored on only one node. Suppose node A is the coordinator, but goes down before a row K is written to it with a consistency level of ONE. In this case, the consistency level specified cannot be met, and since node A is the coordinator, it cannot store a hint. Node B cannot write the data, because it has not received the data as the coordinator nor has a hint been stored. The coordinator checks the number of replicas that are up and will not attempt to write the hint if the consistency level specified by a client cannot be met. A hinted handoff failure occurs and will return a `UnavailableException` exception. The write request fails and the hint is not written.

In general, the recommendation is to have enough nodes in the cluster and a replication factor sufficient to avoid write request failures. For example, consider a cluster consisting of three nodes, A, B, and C, with a replication factor of 2. When a row K is written to the coordinator (node A in this case), even if node C is down, the consistency level of ONE or QUORUM can be met. Why? Both nodes A and B will receive the data, so the consistency level requirement is met. A hint is stored for node C and written when node C comes up. In the meantime, the coordinator can acknowledge that the write succeeded.



For applications that want Cassandra to accept writes when all the normal replicas are down and consistency level ONE cannot be satisfied, Cassandra provides consistency level ANY. ANY guarantees that the write is durable and readable after an appropriate replica target becomes available and receives the hint replay.

Nodes that die might have stored undelivered hints, because any node can be a coordinator. The data on the dead node will be stale after a long outage as well. If a node has been down for an extended period of time, a [manual repair](#) should be run.

At first glance, it seems that hinted handoff eliminates the need for manual repair, but this is not true because hardware failure is inevitable and has the following ramifications:

- Loss of the historical data necessary to tell the rest of the cluster exactly what data is missing.
- Loss of hints-not-yet-replayed from requests that the failed node coordinated.

When removing a node from the cluster by decommissioning the node or by using the [nodetool removename](#) command, Cassandra automatically removes hints targeting the node that no longer exists. Cassandra also removes hints for dropped tables.

For more explanation about hint storage, see [What's Coming to Cassandra in 3.0: Improved Hint Storage and Delivery](#) or an older blog that discusses the basics, [Modern hinted handoff](#).

Read Repair: repair during read path

Read repair improves consistency in a Cassandra cluster with every read request.

In a read, the coordinator node sends a data request to one replica node and digest requests to others (for consistency level greater than 1). If all nodes return consistent data, the coordinator returns it to the client. For a description of how Cassandra handles inconsistency among replicas, see [How are read requests accomplished?](#) on page 45.

In read repair, Cassandra sends a digest request to each replica not directly involved in the read. Cassandra compares all replicas and writes the most recent version to any replica node that does not have it. If the query's consistency level is `ALL`, Cassandra performs this process on all replica nodes in the foreground before the data is returned to the client. For other consistency levels, this process occurs in the background after the read completes.

Cassandra can also perform read repair randomly on a table, independent of any read. You can configure how often this happens using the [read_repair_chance](#) property for a table.

Read repair cannot be performed on tables that use [DateTieredCompactionStrategy](#), because of the way timestamps are checked for DTCS compaction. If your table uses `DateTieredCompactionStrategy`, set `read_repair_chance` to zero. For other compaction strategies, `read_repair_chance` is typically set to a value of 0.2.

Manual repair: Anti-entropy repair

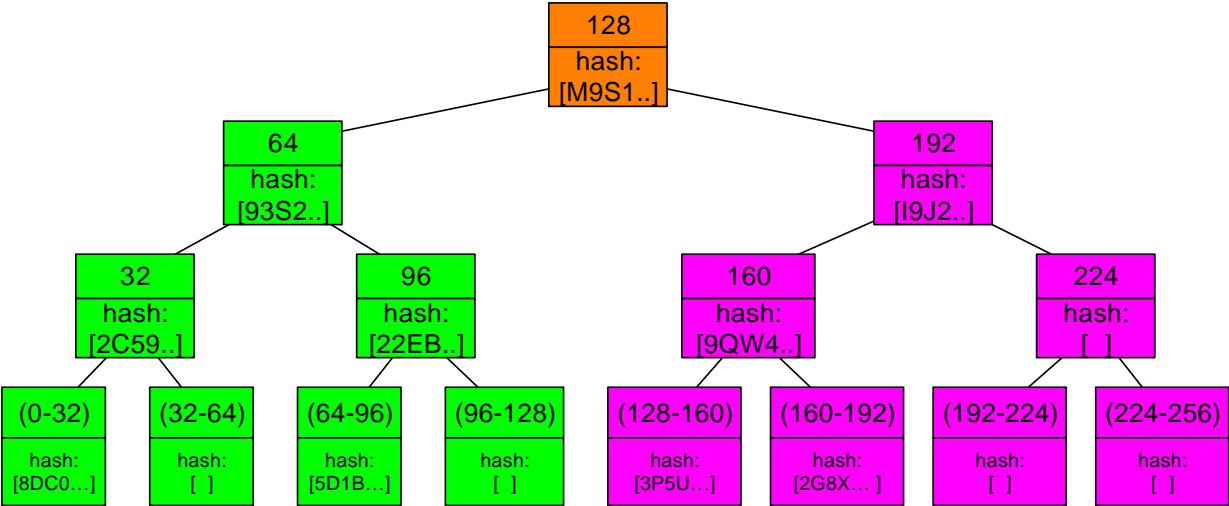
[Anti-entropy](#) node repairs are important for every Cassandra cluster. Frequent data deletions and downed nodes are common causes of data inconsistency. Use anti-entropy repair for routine maintenance and when a cluster needs fixing by running the [nodetool repair](#) command.

How does anti-entropy repair work?

Cassandra accomplishes anti-entropy repair using Merkle trees, similar to Dynamo and Riak. Anti-entropy is a process of comparing the data of all replicas and updating each replica to the newest version. Cassandra has two phases to the process:

1. Build a Merkle tree for each replica
2. Compare the Merkle trees to discover differences

Merkle trees are binary hash trees whose leaves are hashes of the individual key values. The leaf of a Cassandra Merkle tree is the hash of a row value. Each Parent node higher in the tree is a hash of its respective children. Because higher nodes in the Merkle tree represent data further down the tree, Cassandra can check each branch independently without requiring the coordinator node to download the entire data set. For anti-entropy repair Cassandra uses a compact tree version with a depth of 15 ($2^{15} = 32K$ leaf nodes). For example, a node containing a million partitions with one damaged partition, about 30 partitions are streamed, which is the number that fall into each of the *leaves* of the tree. Cassandra works with smaller Merkle trees because they require less storage memory and can be transferred more quickly to other nodes during the comparison process.



Row key: jack	Row key: jill	Row key: terry	Row key: misty
Row token: 5	Row token: 7	Row token: 10	Row token: 20
hash: 8DC0....	hash: 5D1B...	hash: 3P5U...	hash: @G8X...

After the initiating node receives the Merkle trees from the participating peer nodes, the initiating node compares every tree to every other tree. If the initiating node detects a difference, it directs the differing nodes to exchange data for the conflicting range(s). The new data is written to SSTables. The comparison begins with the top node of the Merkle tree. If Cassandra detects no difference between corresponding tree nodes, the process goes on to compares the left *leaves* (child nodes), then the right leaves. A difference between corresponding leaves indicates inconsistencies between the data in each replica for the data range that corresponds to that leaf. Cassandra replaces all data that corresponds to the leaves below the differing leaf with the newest version of the data.

Merkle tree building is quite resource intensive, stressing disk I/O and using memory. Some of the options discussed here help lessen the impact on the cluster performance. For details, see [Repair in Cassandra](#).

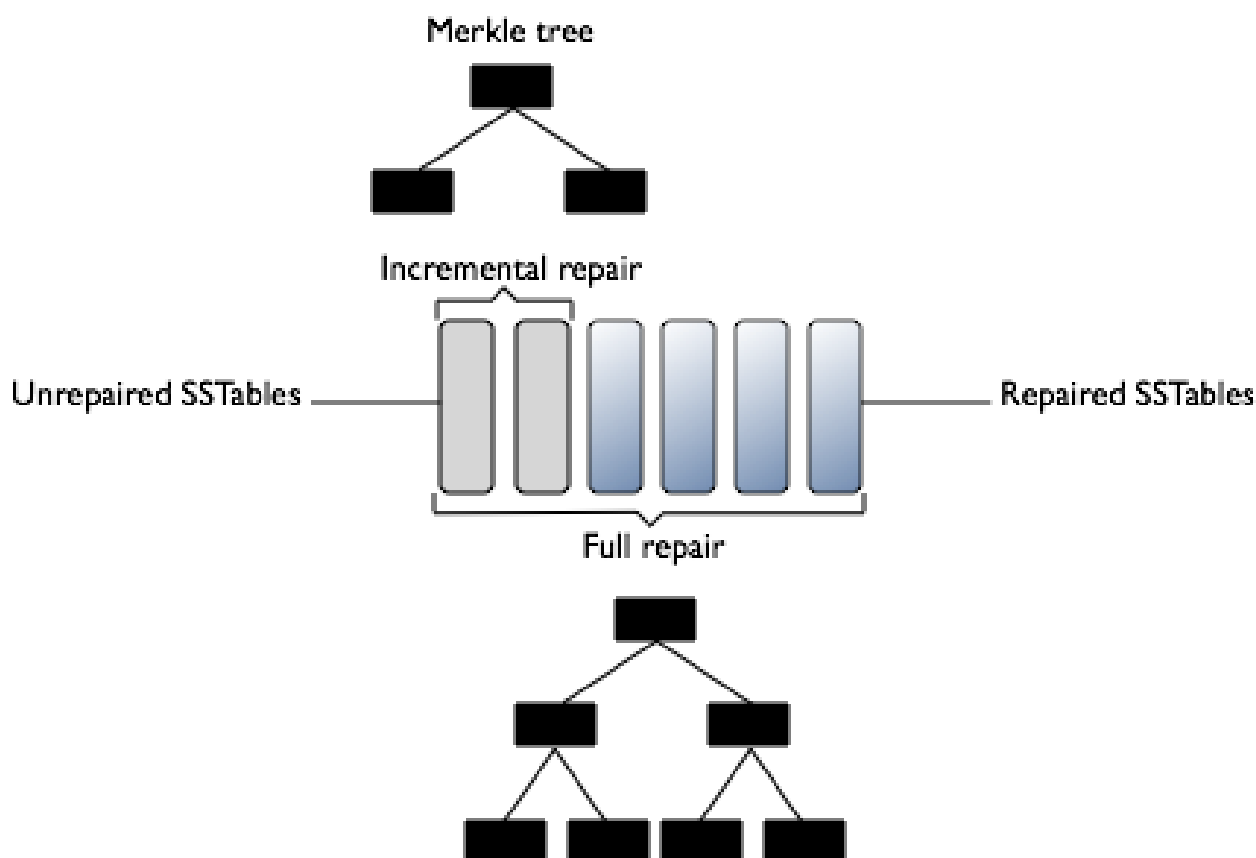
You can run the `nodetool repair` command on a specified node or on all nodes. The node that initiates the repair becomes the coordinator node for the operation. The coordinator node finds peer nodes with matching ranges of data and performs a major, or validation, compaction on each peer node. The validation compaction builds a Merkle tree and returns the tree to the initiating node. The initiating mode processes the Merkle trees as described.

Repair requires intensive disk I/O because validation compaction occurs during Merkle tree construction. For any given replica set, Cassandra performs validation compaction on only one replica at a time.

Full vs Incremental repair

Th section above describes a full repair of a node's data: Cassandra compares all SSTables for that node and makes necessary repairs. Cassandra 2.1 and later support incremental repair. An incremental repair persists data that has already been repaired, and only builds Merkle trees for unrepaired SSTables. This more efficient process depends on new metadata that marks the rows in an SSTable as `repaired` or `unrepaired`.

Merkle Trees of an Incremental Versus a Full Repair



If you run incremental repairs frequently, the repair process works with much smaller Merkle trees. The incremental repair process works with Merkle trees as described above. Once the process had reconciled the data and built new SSTables, the initiating node issues an anti-compaction command. Anti-compaction segregates repaired and unrepaired ranges into separate SSTables, unless the SSTable fits entirely within the repaired range. If it does, the process just updates the SSTable's `repairedAt` field.

Incremental repair works equally well with any compaction scheme, but each compaction strategy handles anti-compaction differently:

- Size-tiered compaction splits repaired and unrepaired data into separate pools for separate compactions. A major compaction generates two SSTables, one for each pool of data.
- Leveled compaction performs size-tiered compaction on unrepaired data. After repair completes, Cassandra moves data from the set of unrepaired SSTables to L0.

Full repair is the default in Cassandra.

Parallel vs Sequential

Sequential repair takes action on one node after another. Parallel repair repairs all nodes with the same replica data at the same time.

Sequential repair takes a snapshot of each replica. Snapshots are hardlinks to existing SSTables. They are immutable and require almost no disk space. The snapshots are active while the repair proceeds, then Cassandra deletes them. When the coordinator node finds discrepancies in the Merkle trees, the coordinator node makes required repairs from the snapshots. For example, for a table in a keyspace with a Replication factor $RF=3$ and replicas A, B and C, the `repair` command takes a snapshot of each replica immediately and then repairs each replica from the snapshots sequentially (using snapshot A to repair replica B, then snapshot A to repair replica C, then snapshot B to repair replica C).

Parallel repair works on nodes A, B, and C all at once. During parallel repair, the [dynamic snitch](#) processes queries for this table using a replica in the snapshot that is not undergoing repair.

Sequential repair is the default in Cassandra 2.1 and earlier.

Note: Do not run repair using both the Sequential and the incremental options in Cassandra 2.1.

Partitioner range (`-pr`)

Within a cluster, Cassandra stores a particular range of data on multiple nodes. If you run `nodetool repair` on one node at a time, Cassandra may repair the same range of data several times (depending on the replication factor used in the keyspace). If you use the partitioner range option (`-pr`), `nodetool repair` only repairs a specified range of data once, rather than repeating the repair operation. This decreases the strain on network resources, although `nodetool repair` still builds Merkle trees for each replica.

Note: If you use this option, you must run `nodetool repair -pr` on EVERY node in the cluster to repair all data. Otherwise, some ranges of data will not be repaired.

The partitioner range option is recommended for routine maintenance. Do not use it to repair a downed node.

Local (`-local`, `--in-local-dc`) vs datacenter (`dc`, `--in-dc`) vs Cluster-wide

Consider carefully before using `nodetool repair` across datacenters, instead of within a local datacenter. When you run repair locally on a node using `-local` or `--in-local-dc`, the command runs only on nodes within the same datacenter as the node that runs it. Otherwise, the command runs cluster-wide repair processes on all nodes that contain replicas, even those in different datacenters. For example, if you start `nodetool repair` over two datacenters, DC1 and DC2, each with a replication factor of 3, repair must build Merkle tables for 6 nodes. The number of Merkle Tree increases linearly for additional data centers. Cluster-wide repair also increases network traffic between data centers tremendously, and can cause cluster issues.

If the local option is too limited, consider using the `-dc` or `--in-dc` options, limiting repairs to a specific datacenter. This does not repair replicas on nodes in other datacenters, but it can decrease network traffic while repairing more nodes than the local options.

The `nodetool repair -pr` option is good for repairs across multiple datacenters.

Additional notes for `-local` repairs:

- The `nodetool repair` tool does not support the use of `-local` with the `-pr` option unless the datacenter's nodes have all the data for all ranges.
- Also, the tool does not support the use of `-local` with `-inc` (incremental repair).

Note: For Cassandra 2.2 and later, a recommended option for repairs across datacenters: use the `-dcpair` or `--dc-parallel` to repair datacenters in parallel.

Endpoint range vs Subrange repair (`-st`, `--start-token`, `-et` `--end-token`)

A repair operation runs on all partition ranges on a node, or an endpoint range, unless you use the `-st` and `-et` (or `--start-token` and `--end-token`) options to run subrange repairs. When you specify a start token and end token, `nodetool repair` works between these tokens, repairing only those partition ranges.

Subrange repair is not a good strategy because it requires generated token ranges. However, if you know which partition has an error, you can target that partition range precisely for repair. This approach can relieve the problem known as overstreaming, which ties up resources by sending repairs to a range over and over.

You can use subrange repair with Java to reduce overstreaming further. Send a Java `describe_splits` call to ask for a split containing 32k partitions can be iterated throughout the entire range incrementally or in parallel. Once the tokens are generated for the split, you can pass them to `nodetool repair -st <start_token> -et <end_token>`. Add the `-local` option to limit the repair to the local datacenter. This reduces cross datacenter transfer.

When to run anti-entropy repair

When to run anti-entropy repair is dependent on the characteristics of a Cassandra cluster. General guidelines are presented here, and should be tailored to each particular case.

When is repair needed?

Run repair in these situations:

- To routinely maintain node health.

Note: Even if deletions never occur, schedule regular repairs. Setting a column to null is a delete.
- To recover a node after a failure while bringing it back into the cluster.
- To update data on a node containing data that is not read frequently, and therefore does not get read repair.
- To update data on a node that has been down.
- To recover missing data or corrupted SSTables. To do this, you must run non-incremental repair.

Guidelines for running routine node repair include:

- Run incremental repair daily, run full repairs weekly to monthly. Monthly is generally sufficient, but run more frequently if warranted.

Important: Full repair is useful for maintaining data integrity, even if deletions never occur.

- Use the parallel and partitioner range options, unless precluded by the scope of the repair.
- Run a full repair to eliminate anti-compaction. Anti-compaction is the process of splitting an SSTable into two SSTables, one with repaired data and one with non-repaired data. This has [compaction strategy implications](#).

Note: Before you can run incremental repair, you must set the repaired state of each SSTable. For instructions, see [Migrating to incremental repairs](#).

- Run repair frequently enough that every node is repaired before reaching the time specified in the `gc_grace_seconds` setting. Deleted data is properly handled in the cluster if this requirement is met.
- Schedule routine node repair to minimize cluster disruption.
 - If possible, schedule repair operation for low-usage hours.
 - If possible, schedule repair operations on single nodes at a time.
- Increase the time value setting of `gc_grace_seconds` if data is seldom deleted or overwritten. For these tables, changing the setting will:
 - Minimizes impact to disk space.
 - Allow longer interval between repair operations.
- Mitigate heavy disk usage by configuring `nodetool` compaction throttling options ([setcompactionthroughput](#) and [setcompactionthreshold](#)) before running a repair.

Guidelines for running repair on a downed node:

- Do not use partitioner range, `-pr`.

Migrating to incremental repairs

Repairing SSTables using [anti-entropy repair](#) is a necessary part of Cassandra maintenance. A full repair of all SSTables on a node takes a lot of time and is resource-intensive. You can manage repairs with less service disruption using [incremental repair](#). Incremental repair consumes less time and resources because it skips SSTables that are already marked as repaired.

Incremental repair works equally well with any compaction scheme — Size-Tiered Compaction (STCS), Date-Tiered Compaction (DTCS) or Leveled Compaction (LCS).

However, Cassandra's default is full repair: a new SSTable is created without metadata that identifies its repaired state. Before you can start using incremental repairs, you must add this marker to each SSTable on each node in the cluster. Follow these instructions to migrate the cluster to incremental repair gradually, one node at a time.

Overview of the procedure

To migrate one Cassandra node to incremental repair:

1. Disable autocompaction on the node.
2. Run the default full, sequential repair.
3. Stop the node.
4. Set the `repairedAt` metadata value to each SSTable that existed before you disabled compaction.
5. Restart Cassandra on the node.
6. Re-enable autocompaction on the node.

Prerequisites

Listing SSTables

Before you run a full repair on the node, list its SSTables. The existing SSTables may not be changed by the repair process, and the incremental repair process you run later will not process these SSTables unless you set the `repairedAt` value for each SSTable (see [Step 4](#) below).

You can find the node's SSTables in one of the following locations:

This directory contains a subdirectory for each keyspace. Each of these subdirectories contains a set of files for each SSTable. The name of the file that contains the SSTable data has the following format:

```
<version_code>-<generation>-<format>-Data.db
```

Note: You can mark multiple SSTables as a batch by running `sstablerepairedset` with a text file of filenames — see [Step 4](#).

Migrating the node to incremental repair

Note: In RHEL and Debian installations, you must install the tools packages before you can follow these steps.

1. Disable autocompaction on the node

From the *install_directory*:

```
$ bin/nodetool disableautocompaction
```

Running this command without parameters disables autocompaction for all keyspaces. For details, see [disableautocompaction](#).

2. Run the default full, sequential repair

From the *install_directory*:

```
$ bin/nodetool repair
```

Running this command without parameters starts a full sequential repair of all SSTables on the node. This may take a substantial amount of time. For details, see [repair](#).

3. Stop the node.

4. Set the `repairAt` metadata value to each SSTable that existed before you disabled compaction.

Use `sstablerepairedset` on page 243. To mark a single SSTable `SSTable-example-Data.db`:

```
sudo bin/sstablerepairedset --is-repaired SSTable-example-Data.db
```

To do this as a batch process using a text file of SSTable names:

```
sudo bin/sstablerepairedset --is-repaired -f SSTable-names.txt
```

Note: The value of the `repairAt` metadata is the timestamp of the last repair. The `sstablerepairedset` command applies the current date/time. To check the value of the `repairAt` metadata for an SSTable, use:

```
$ bin/sstablemetadata example-keyspace-SSTable-example-Data.db | grep  
"Repaired at"
```

5. Restart the node.

6. Re-enable autocompaction on the node.

From the *install_directory*:

```
$ bin/nodetool enableautocompaction
```

Running this command without parameters enables autocompaction for all keyspaces and tables. For details, see [enableautocompaction](#).

What to do next

After you have migrated all nodes, you will be able to run incremental repairs using `nodetool repair` with the `-inc` parameter. For details, see <http://www.datastax.com/dev/blog/more-efficient-repairs>.

Related information

<http://www.datastax.com/dev/blog/repair-in-cassandra>

<http://www.datastax.com/dev/blog/more-efficient-repairs>

<http://www.datastax.com/dev/blog/anticompaction-in-cassandra-2-1>

Monitoring Cassandra

Monitoring a Cassandra cluster

Understanding the performance characteristics of a Cassandra cluster is critical to diagnosing issues and planning capacity.

Cassandra exposes a number of statistics and management operations via Java Management Extensions (JMX). JMX is a Java technology that supplies tools for managing and monitoring Java applications

and services. Any statistic or operation that a Java application has exposed as an MBean can then be monitored or manipulated using JMX.

JMX). JMX is a Java technology that supplies tools for managing and monitoring Java applications and services. Any statistic or operation that a Java application has exposed as an MBean can then be monitored or manipulated using JMX.

During normal operation, Cassandra outputs information and statistics that you can monitor using JMX-compliant tools, such as:

- The Cassandra [nodetool utility](#)
- JConsole

Using the same tools, you can perform certain administrative commands and operations such as flushing caches or doing a [node repair](#).

Monitoring using the nodetool utility

The [nodetool utility](#) is a command-line interface for monitoring Cassandra and performing routine database operations. It is included in the Cassandra distribution. `nodetool` is typically run directly from an operational Cassandra node.

The `nodetool` utility supports the most important JMX metrics and operations, and includes other useful commands for Cassandra administration, such as the [proxyhistogram command](#). This example shows the output from `nodetool proxyhistograms` after running 4,500 insert statements and 45,000 select statements on a three [ccm](#) node-cluster on a local computer.

```
C:\> %CASSANDRA_HOME%\bin\nodetool proxyhistograms
```

```
proxy histograms
Percentile      Read Latency      Write Latency      Range Latency
                (micros)          (micros)           (micros)
50%             1502.50           375.00             446.00
75%             1714.75           420.00             498.00
95%            31210.25          507.00             800.20
98%            36365.00          577.36             948.40
99%            36365.00          740.60            1024.39
Min              616.00           230.00             311.00
Max            36365.00          55726.00          59247.00
```

For a summary of the ring and its current state of general health, use the [status command](#). For example:

```
C:\> \bin\nodetool status
```

```
Note: Ownership information does not include topology; for complete
      information, specify a keyspace
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load          Tokens   Owns    Host ID
   Rack
UN 127.0.0.1    47.66 KB      1         33.3%   aaalb7c1-6049-4a08-
ad3e-3697a0e30e10 rack1
UN 127.0.0.2    47.67 KB      1         33.3%   1848c369-4306-4874-
afdf-5cle95b8732e rack1
UN 127.0.0.3    47.67 KB      1         33.3%   49578bf1-728f-438d-b1c1-
d8dd644b6f7f rack1
```

The `nodetool` utility provides commands for viewing detailed metrics for tables, server metrics, and compaction statistics:

- `nodetool tablestats` displays statistics for each table and keyspace.
- `nodetool tablehistograms` provides statistics about a table, including read/write latency, row size, column count, and number of SSTables.
- `nodetool netstats` provides statistics about network operations and connections.
- `nodetool tpstats` provides statistics about the number of active, pending, and completed tasks for each stage of Cassandra operations by thread pool.

Monitoring using JConsole

JConsole is a JMX-compliant tool for monitoring Java applications such as Cassandra. It is included with Sun JDK 5.0 and higher. JConsole consumes the JMX metrics and operations exposed by Cassandra and displays them in a well-organized GUI. For each node monitored, JConsole provides these six separate tab views:

- Overview
Displays overview information about the Java VM and monitored values.
- Memory
Displays information about memory use.
- Threads
Displays information about thread use.
- Classes
Displays information about class loading.
- VM Summary
Displays information about the Java Virtual Machine (VM).
- Mbeans
Displays information about MBeans.

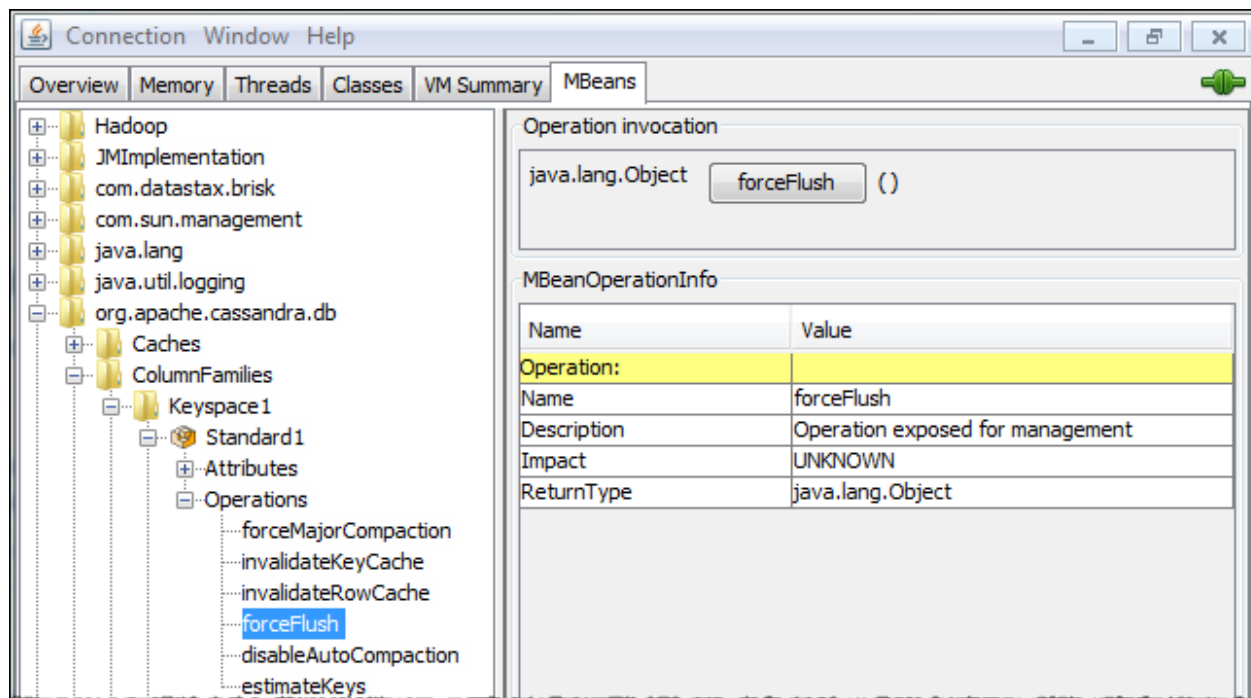
The Overview and Memory tabs contain information that is very useful for Cassandra developers. The Memory tab allows you to compare heap and non-heap memory usage, and provides a control to immediately perform Java garbage collection.

For specific Cassandra metrics and operations, the most important area of JConsole is the MBeans tab. This tab lists the following Cassandra MBeans:

- `org.apache.cassandra.auth`
Includes permissions cache.
- `org.apache.cassandra.db`
Includes caching, table metrics, and compaction.
- `org.apache.cassandra.internal`
Internal server operations such as gossip, hinted handoff, and Memtable values.
- `org.apache.cassandra.metrics`
Includes metrics on CQL, clients, keyspaces, read repair, storage, and threadpools and other topics.
- `org.apache.cassandra.net`
Inter-node communication including FailureDetector, MessagingService and StreamingManager.
- `org.apache.cassandra.request`
Tasks related to read, write, and replication operations.
- `org.apache.cassandra.service`
Includes GCInspector.

When you select an MBean in the tree, its MBeanInfo and MBean Descriptor are displayed on the right, and any attributes, operations or notifications appear in the tree below it. For example, selecting and

expanding the `org.apache.cassandra.db` MBean to view available actions for a table results in a display like the following:



If you choose to monitor Cassandra using JConsole, keep in mind that JConsole consumes a significant amount of system resources. For this reason, DataStax recommends running JConsole on a remote machine rather than on the same host as a Cassandra node.

The JConsole `CompactionManagerMBean` exposes [compaction metrics](#) that can indicate when you need to add capacity to your cluster.

Compaction metrics

Monitoring compaction performance is an important aspect of knowing when to add capacity to your cluster. The following attributes are exposed through `CompactionManagerMBean`:

Table: Compaction Metrics

Attribute	Description
BytesCompacted	Total number of bytes compacted since server [re]start
CompletedTasks	Number of completed compactions since server [re]start
PendingTasks	Estimated number of compactions remaining to perform
TotalCompactionsCompleted	Total number of compactions since server [re]start

Thread pool and read/write latency statistics

Cassandra maintains distinct thread pools for different stages of execution. Each of the thread pools provide statistics on the number of tasks that are active, pending, and completed. Trends on these pools for increases in the pending tasks column indicate when to add additional capacity. After a baseline is established, configure alarms for any increases above normal in the pending tasks column. Use [nodetool tpstats](#) on the command line to view the thread pool details shown in the following table.

Table: Thread Pool statistics reported by nodetool tpstats

Thread Pool	Description
AntiEntropyStage	Tasks related to repair
CacheCleanupExecutor	Tasks related to cache maintenance (counter cache, row cache)
CompactionExecutor	Tasks related to compaction
CounterMutationStage	Tasks related to leading counter writes
GossipStage	Tasks related to the gossip protocol
HintsDispatcher	Tasks related to sending hints
InternalResponseStage	Tasks related to miscellaneous internal task responses
MemtableFlushWriter	Tasks related to flushing memtables
MemtablePostFlush	Tasks related to maintenance after memtable flush completion
MemtableReclaimMemory	Tasks related to reclaiming memtable memory
MigrationStage	Tasks related to schema maintenance
MiscStage	Tasks related to miscellaneous tasks, including snapshots and removing hosts
MutationStage	Tasks related to writes
Native-Transport-Requests	Tasks related to client requests from CQL
PendingRangeCalculator	Tasks related to recalculating range ownership after bootstraps/decommissions
PerDiskMemtableFlushWriter	Tasks related to flushing memtables to a given disk
ReadRepairStage	Tasks related to performing read repairs
ReadStage	Tasks related to reads
RequestResponseStage	Tasks for callbacks from intra-node requests
Sampler	Tasks related to sampling statistics
SecondaryIndexManager	Tasks related to secondary index maintenance
ValidationExecutor	Tasks related to validation compactions
ViewMutationStage	Tasks related to maintaining materialized views

Read/Write latency metrics

Cassandra tracks latency (averages and totals) of read, write, and slicing operations at the server level through `StorageProxyMBean`.

Table statistics

For individual tables, `ColumnFamilyStoreMBean` provides the same general latency attributes as `StorageProxyMBean`. Unlike `StorageProxyMBean`, `ColumnFamilyStoreMBean` has a number of other statistics that are important to monitor for performance trends. The most important of these are:

Table: Table Statistics

Attribute	Description
MemtableDataSize	The total size consumed by this table's data (not including metadata).
MemtableColumnsCount	Returns the total number of columns present in the memtable (across all keys).
MemtableSwitchCount	How many times the memtable has been flushed out.
RecentReadLatencyMicros	The average read latency since the last call to this bean.
RecentWriterLatencyMicros	The average write latency since the last call to this bean.
LiveSSTableCount	The number of live SSTables for this table.

The recent read latency and write latency counters are important in making sure operations are happening in a consistent manner. If these counters start to increase after a period of staying flat, you probably need to add capacity to the cluster.

You can set a threshold and monitor LiveSSTableCount to ensure that the number of [SSTables](#) for a given table does not become too great.

Tuning Java resources

Tuning Java resources can help correct performance degradation or high memory consumption.

The properties in the Cassandra file `jvm.options` and `cassandra-env.ps1` control environment settings, such as Java Virtual Machine (JVM) configuration settings.

Tuning the Java heap

Because Cassandra interacts intensively with the operating system infrastructure through the JVM, it is important to configure the Java heap effectively.

How Cassandra uses heap and off-heap memory

Cassandra defines the following properties to control the JVM's heap size:

MAX_HEAP_SIZE

The maximum amount of RAM that Cassandra can use. Cassandra also uses this value as the minimum RAM size. This strategy locks the heap in memory at process start to keep it from being swapped out by the OS.

Cassandra calculates the default value for MAX_HEAP_SIZE in the `cassandra-env.ps1` file, based on the amount of the computer's RAM:

System Memory	Heap Size
Less than 2GB	1/2 of system memory
2GB to 4GB	1GB
Greater than 4GB	1/4 system memory

You can override the default by setting a new value for the `MAX_HEAP_SIZE` property in the `jvm.options` file. For details, see [Heap sizing options](#).

HEAP_NEWSIZE

Also called "young generation" — the amount of heap memory allocated to newer objects. Objects that survive garbage collection long enough move into an "old generation" space of the heap. Cassandra calculates the default value for this property (in MB) as the lesser of:

- 100 times the number of cores
- $\frac{1}{4}$ of MAX_HEAP_SIZE

Heap sizing options

To override Cassandra's calculated values for heap sizing, uncomment and change the following properties in the `jvm.options` file:

Heap size property	Property in <code>jvm.options</code>
MAX_HEAP_SIZE	Set both properties to the same value: # -Xms4G # -Xmx4G
HEAP_NEWSIZE	# -Xmn800M

Before adjusting these properties, review the following considerations carefully.

How Cassandra uses memory

Cassandra performs its major operations within JVM heap:

- To perform reads, Cassandra maintains the following components in heap memory:
 - Bloom filters
 - Partition summary
 - Partition key cache
 - Compression offsets
 - SSTable index summary

This metadata resides in memory and is proportional to total data. Some of the components [grow proportionally to the size of total memory](#).

- When Cassandra gathers replicas for a read or for anti-entropy repair, Cassandra compares the replicas in heap memory.
- data written to Cassandra is first stored in memtables in heap memory. Memtables are flushed to SSTables on disk.

To improve performance, Cassandra also uses off-heap memory as follows:

- The most important off-heap facility is the computer's page cache. Cassandra uses additional memory as page cache when reading files on disk.
- The Bloom filter and compression offset maps reside off-heap.
- Cassandra can store cached rows in native memory, outside the Java heap. This reduces JVM heap requirements, which helps keep the heap size in the sweet spot for JVM garbage collection performance.

Considerations for sizing the Java heap

On older computers with limited RAM, the recommended MAX_HEAP_SIZE is 8MB, with the HEAP_NEWSIZE calculated by `cassandra-env.ps1`. However, there are many other factors you should consider when fine-tuning the heap size:

- Many users new to Cassandra are tempted to set the Java heap to consume the majority of the computer's RAM. Increasing the Java heap size may interfere with the operation of the OS page cache. Modern operating systems maintain the OS page cache for frequently accessed data and are very good at keeping this data in memory. Proper tuning of the OS page cache can result in better performance

than increasing the Cassandra row cache. But an elevated Java heap size can prevent the page cache from doing its job.

- Cassandra performance within the JVM is also closely tied to the configuration of the Java garbage collection facility. For details, see [Tuning Java garbage collection](#) on page 140 below.
- More advanced services that work within Cassandra (Solr, MapReduce, etc.) may require you to adjust the heap size to optimize their performance. For details, see [Adjusting JVM parameters for other Cassandra services](#) on page 141 below.

Tuning Java garbage collection

On older computers, you can typically allocate about 8GB of memory to the heap before garbage collection pause time starts to become a problem. Modern computers have much more memory up to 256GB. You can allocate more memory to the heap on newer computers, but you may encounter diminishing performance returns as the garbage collection facility works with the increasing amount of Cassandra metadata in heap memory. However, garbage collection has also improved in later releases of Java.

The default garbage collector for Cassandra 2.2 and later is the Concurrent-Mark-Sweep (CMS) garbage collector. You can also configure Cassandra to use the G1 garbage collector, which will become the default garbage collector for Java 9. G1 performs better than CMS for 4GB heaps or larger. G1 scans the regions of the heap that contain the most garbage objects first. It also compacts the heap on-the-go, while the CMS garbage collector only compacts during full stop-the-world garbage collection.

Recommended MAX_HEAP sizes for computers with up to 256GB of RAM:

Hardware setup:	Recommend MAX_HEAP_SIZE:
Up to 256GB RAM, CMS garbage collection	up to 16GB
Up to 256GB RAM, G1 garbage collection	up to 32GB

Using G1 in Cassandra

Cassandra's default garbage collection service is CMS. To configure Cassandra to use G1:

1. Open `$CASSANDRA_HOME/conf/jvm.options`.
2. Comment out all lines in the `### CMS Settings` section.
3. Uncomment the relevant G1 settings in the `### G1 Settings` section.

Adjusting HEAP_NEWSIZE

The HEAP_NEWSIZE can also be adjusted. A larger HEAP_NEWSIZE leads to longer GC pause times. But for a smaller HEAP_NEWSIZE, GC pauses are shorter but more expensive (usually). Recommended range: between 25% and 50% of MAX_HEAP_SIZE.

Adjusting and testing garbage collection and heap size

The best way to optimize the Java heap size and garbage collection is to change settings gradually and test each configuration. Some tips:

- Always enable GC logging when adjusting GC.
- Enable parallel processing for GC, particularly when using DSE/Solr
- Comment out the `-Xmn` line when switching to G1.
- Recommended MAX_HEAP_SIZE when using G1, from the Cassandra community: 6GB.
- Cassandra's GCInspector class logs information about garbage collection whenever a garbage collection takes longer than 200ms. Garbage collections that occur frequently and take a moderate length of time to complete (such as ConcurrentMarkSweep taking a few seconds), indicate that there is a lot of garbage collection pressure on the JVM. Remedies include adding nodes, lowering cache sizes, or adjusting the JVM options regarding garbage collection.
- For more tuning tips, see [Secret HotSpot option improving GC pauses on large heaps](#)

Adjusting JVM parameters for other Cassandra services

- **Solr:** Some Solr users have reported that increasing the stack size improves performance under Tomcat. To increase the stack size, uncomment and modify the default setting in the `cassandra-env.ps1` file. Also, decreasing the memtable space to make room for Solr caches can improve performance. Modify the memtable space by changing the `memtable_heap_space_in_mb` and `memtable_offheap_space_in_mb` properties in the `cassandra.yaml` file.
- **MapReduce:** Because MapReduce runs outside the JVM, changes to the JVM do not affect Analytics/Hadoop operations directly.

Other JMX options

Cassandra exposes other statistics and management operations via Java Management Extensions (JMX). [JConsole](#) and the [nodetool](#) utility are JMX-compliant management tools.

Configure Cassandra for JMX management by editing these properties in `cassandra-env.ps1`.

- `com.sun.management.jmxremote.port`
Set the port on which Cassandra listens from JMX connections.
- `com.sun.management.jmxremote.ssl`
Enable/disable SSL for JMX.
- `com.sun.management.jmxremote.authenticate`
Enable/disable remote authentication for JMX.
- `-Djava.rmi.server.hostname`
Set the interface hostname or IP that JMX should use to connect. Uncomment and set if you are having trouble connecting.

Note: By default, you can interact with Cassandra using JMX on port 7199 without authentication.

Related information

<http://blog.ragozin.info/2012/03/secret-hotspot-option-improving-gc.html>

Data caching

Configuring data caches

Cassandra includes integrated caching and distributes cache data around the cluster. When a node goes down, the client can read from another cached replica of the data. The integrated architecture also facilitates troubleshooting because there is no separate caching tier, and cached data matches what is in the database exactly. The integrated cache alleviates the cold start problem by saving the cache to disk periodically. Cassandra reads contents back into the cache and distributes the data when it restarts. The cluster does not start with a cold cache.

The saved key cache files include the ID of the table in the file name. A saved key cache filename for the `users` table in the `mykeyspace` keyspace looks similar to: `mykeyspace-users.users_name_idx-19bd7f80352c11e4aa6a57448213f97f-KeyCache-b.db2046071785672832311.tmp`

About the partition key cache

The partition key cache is a cache of the [partition index](#) for a Cassandra table. Using the key cache instead of relying on the OS page cache decreases seek times. Enabling just the key cache results in disk (or OS page cache) activity to actually read the requested data rows, but not enabling the key cache results in more reads from disk.

About the row cache

Note: Utilizing appropriate OS page cache will result in better performance than using row caching. Consult resources for page caching for the operating system on which Cassandra is hosted.

Configure the number of rows to cache in a partition by setting the `rows_per_partition` table option. To cache rows, if the row key is not already in the cache, Cassandra reads the first portion of the partition, and puts the data in the cache. If the newly cached data does not include all cells configured by user, Cassandra performs another read. The actual size of the row-cache depends on the workload. You should properly benchmark your application to get "the best" row cache size to configure.

There are two row cache options, the old serializing cache provider and a new off-heap cache (OHC) provider. The new OHC provider has been benchmarked as performing about 15% better than the older option.

Using key cache and row cache

Typically, you enable either the partition key or row cache for a table.

Tip: Enable a row cache only when the number of reads is much bigger (rule of thumb is 95%) than the number of writes. Consider using the operating system page cache instead of the row cache, because writes to a partition invalidate the whole partition in the cache.

Tip: Disable caching entirely for archive tables, which are infrequently read.

Enabling and configuring caching

Use CQL to enable or disable caching by configuring the caching [table property](#). Set parameters in the `cassandra.yaml` file to configure global caching properties:

- [Partition key cache size](#)
- [Row cache size](#)
- How often Cassandra [saves partition key caches](#) to disk
- How often Cassandra [saves row caches](#) to disk

Configuring the `row_cache_size_in_mb` (in the `cassandra.yaml` configuration file) determines how much space in memory Cassandra allocates to store rows from the most frequently read partitions of the table.

Procedure

Set the table caching property that configures the partition key cache and the row cache.

```
CREATE TABLE users (
    userid text PRIMARY KEY,
    first_name text,
    last_name text,
)
WITH caching = { 'keys' : 'NONE', 'rows_per_partition' : '120' };
```

Tips for efficient cache use

[Tuning the row cache in Cassandra 2.1](#) describes best practices of using the built-in caching mechanisms and designing an effective data model. Some tips for efficient cache use are:

- Store lower-demand data or data with extremely long partitions in a table with minimal or no caching.
- Deploy a large number of Cassandra nodes under a relatively light load per node.
- Logically separate heavily-read data into discrete tables.

When you query a table, [turn on tracing](#) to check that the table actually gets data from the cache rather than from disk. The first time you read data from a partition, the trace shows this line below the query because the cache has not been populated yet:

```
Row cache miss [ReadStage:41]
```

In subsequent queries for the same partition, look for a line in the trace that looks something like this:

```
Row cache hit [ReadStage:55]
```

This output means the data was found in the cache and no disk read occurred. Updates invalidate the cache. If you query rows in the cache plus uncached rows, request more rows than the global limit allows, or the query does not grab the beginning of the partition, the trace might include a line that looks something like this:

```
Ignoring row cache as cached value could not satisfy query [ReadStage:89]
```

This output indicates that an insufficient cache caused a disk read. Requesting rows not at the beginning of the partition is a likely cause. Try removing constraints that might cause the query to skip the beginning of the partition, or [place a limit](#) on the query to prevent results from overflowing the cache. To ensure that the query hits the cache, try increasing the cache size limit, or restructure the table to position frequently accessed rows at the head of the partition.

Monitoring and adjusting caching

Make changes to cache options in small, incremental adjustments, then monitor the effects of each change using the [nodetool utility](#). The output of the `nodetool info` command shows the following row cache and key cache setting values, which are configured in the `cassandra.yaml` file:

- Cache size in bytes
- Capacity in bytes
- Number of hits
- Number of requests
- Recent hit rate
- Duration in seconds after which Cassandra saves the key cache.

For example, on start-up, the information from `nodetool info` might look something like this:

```
ID                : 387d15ba-7103-491b-9327-1a691dbb504a
Gossip active     : true
Thrift active     : true
Native Transport active: true
Load              : 65.87 KB
Generation No     : 1400189757
Uptime (seconds)  : 148760
Heap Memory (MB)  : 392.82 / 1996.81
Data Center       : datacenter1
Rack              : rack1
Exceptions        : 0
Key Cache         : entries 10, size 728 (bytes), capacity 103809024 (bytes),
  93 hits, 102 requests, 0.912 recent hit rate, 14400 save period in seconds
Row Cache         : entries 0, size 0 (bytes), capacity 0 (bytes), 0 hits, 0
  requests, NaN recent hit rate, 0 save period in seconds
Counter Cache     : entries 0, size 0 (bytes), capacity 51380224 (bytes), 0
  hits, 0 requests, NaN recent hit rate, 7200 save period in seconds
Token             : -9223372036854775808
```

In the event of high memory consumption, consider tuning data caches.

Configuring memtable thresholds

Configuring memtable thresholds can improve write performance. Cassandra flushes memtables to disk, creating SSTables when the [commit log space threshold](#) or the [memtable cleanup threshold](#) has been exceeded. Configure the commit log space threshold per node in the `cassandra.yaml`. How you tune memtable thresholds depends on your data and write load. Increase memtable thresholds under either of these conditions:

- The write load includes a high volume of updates on a smaller set of data.
- A steady stream of continuous writes occurs. This action leads to more efficient compaction.

Allocating memory for memtables reduces the memory available for caching and other internal Cassandra structures, so tune carefully and in small increments.

Configuring compaction

As discussed in the [Compaction](#) on page 27 topic, the compaction process merges keys, combines columns, evicts tombstones, consolidates SSTables, and creates a new index in the merged SSTable.

In the `cassandra.yaml` file, you configure these global compaction parameters:

- [snapshot_before_compaction](#)
- [concurrent_compactors](#)
- [compaction_throughput_mb_per_sec](#)

The `compaction_throughput_mb_per_sec` parameter is designed for use with large partitions because compaction is throttled to the specified total throughput across the entire system.

Cassandra provides a start-up option for [testing compaction strategies](#) without affecting the production workload.

Using CQL, you configure a compaction strategy:

- `SizeTieredCompactionStrategy` (STCS): The default compaction strategy. This strategy triggers a minor compaction when there are a number of similar sized SSTables on disk as configured by the table subproperty, `min_threshold`. A minor compaction does not involve all the tables in a keyspace. Also see [STCS compaction subproperties](#).
- `DateTieredCompactionStrategy` (DTCS): This strategy is particularly useful for [time series data](#). `DateTieredCompactionStrategy` stores data written within a certain period of time in the same SSTable. For example, Cassandra can store your last hour of data in one SSTable *time window*, and the next 4 hours of data in another time window, and so on. Compactions are triggered when the `min_threshold` (4 by default) for SSTables in those windows is reached. The most common queries for time series workloads retrieve the last hour/day/month of data. Cassandra can limit SSTables returned to those having the relevant data. Also, Cassandra can store data that has been set to expire using TTL in an SSTable with other data scheduled to expire at approximately the same time. Cassandra can then drop the SSTable without doing any compaction. Also see [DTCS compaction subproperties](#) and [DateTieredCompactionStrategy: Compaction for Time Series Data](#).
- `LeveledCompactionStrategy` (LCS): The leveled compaction strategy creates SSTables of a fixed, relatively small size (160 MB by default) that are grouped into levels. Within each level, SSTables are guaranteed to be non-overlapping. Each level (L0, L1, L2 and so on) is 10 times as large as the previous. Disk I/O is more uniform and predictable on higher than on lower levels as SSTables are continuously being compacted into progressively larger levels. At each level, row keys are merged into non-overlapping SSTables in the next level. This process can improve performance for reads, because Cassandra can determine which SSTables in each level to check for the existence of row key data.

This compaction strategy is modeled after Google's LevelDB implementation. Also see [LCS compaction subproperties](#).

To configure the compaction strategy property and [CQL compaction subproperties](#), such as the maximum number of SSTables to compact and minimum SSTable size, use [CREATE TABLE](#) or [ALTER TABLE](#).

Procedure

1. Update a table to set the compaction strategy using the ALTER TABLE statement.

```
ALTER TABLE users WITH
  compaction = { 'class' : 'LeveledCompactionStrategy' }
```

2. Change the [compaction strategy property](#) to SizeTieredCompactionStrategy and specify the minimum number of SSTables to trigger a compaction using the CQL min_threshold attribute.

```
ALTER TABLE users
  WITH compaction =
    { 'class' : 'SizeTieredCompactionStrategy', 'min_threshold' : 6 }
```

Results

You can monitor the results of your configuration using compaction metrics, see [Compaction metrics](#) on page 136.

What to do next

Cassandra 3.0 and later support extended logging for Compaction. This utility must be configured as part of the table configuration. The extended compaction logs are stored in a separate file. For details, see [Enabling extended compaction logging](#).

Compression

Compression maximizes the storage capacity of Cassandra nodes by reducing the volume of data on disk and disk I/O, particularly for read-dominated workloads. Cassandra quickly finds the location of rows in the SSTable index and decompresses the relevant row chunks. Compression is important for Cassandra 2.2, but Cassandra 3.0 and later uses a new storage engine that dramatically reduces disk volume automatically. For information on the Cassandra 3.0 improvements, see [Putting some structure in the storage engine](#)

Write performance is not negatively impacted by compression in Cassandra as it is in traditional databases. In traditional relational databases, writes require overwrites to existing data files on disk. The database has to locate the relevant pages on disk, decompress them, overwrite the relevant data, and finally recompress. In a relational database, compression is an expensive operation in terms of CPU cycles and disk I/O. Because Cassandra SSTable data files are immutable (they are not written to again after they have been flushed to disk), there is no recompression cycle necessary in order to process writes. SSTables are compressed only once when they are written to disk. Writes on compressed tables can show up to a 10 percent performance improvement.

In Cassandra 2.2 and later, the commit log can also be compressed and write performance can be improved 6-12%. For more information, see [Updates to Cassandra's Commit Log in 2.2](#).

When to compress data

Compression is most effective on a table with many rows, where each row contains the same set of columns (or the same number of columns) as all other rows. For example, a table containing user data

such as *username*, *email* and *state* is a good candidate for compression. The greater the similarity of the data across rows, the greater the compression ratio and gain in read performance.

A table whose rows contain differing sets of columns is not well-suited for compression.

Don't confuse table compression with [compact storage](#) of columns, which is used for backward compatibility of old applications with CQL.

Depending on the data characteristics of the table, compressing its data can result in:

- 25-33% reduction in data size
- 25-35% performance improvement on reads
- 5-10% performance improvement on writes

After configuring compression on an existing table, subsequently created SSTables are compressed. Existing SSTables on disk are not compressed immediately. Cassandra compresses existing SSTables when the normal Cassandra compaction process occurs. Force existing SSTables to be rewritten and compressed by using [nodetool upgradesstables](#) (Cassandra 1.0.4 or later) or [nodetool scrub](#).

Configuring compression

You configure a table property and subproperties to manage compression. The [CQL table properties documentation](#) describes the types of compression options that are available. Compression is enabled by default.

Procedure

1. Disable compression, using CQL to set the compression parameter enabled to false.

```
CREATE TABLE DogTypes (  
    block_id uuid,  
    species text,  
    alias text,  
    population varint,  
    PRIMARY KEY (block_id)  
)  
WITH compression = { 'enabled' : false };
```

2. Enable compression on an existing table, using ALTER TABLE to set the compression algorithm class to LZ4Compressor (Cassandra 1.2.2 and later), SnappyCompressor, or DeflateCompressor.

```
CREATE TABLE DogTypes (  
    block_id uuid,  
    species text,  
    alias text,  
    population varint,  
    PRIMARY KEY (block_id)  
)  
WITH compression = { 'class' : 'LZ4Compressor' };
```

3. Change compression on an existing table, using ALTER TABLE and setting the compression algorithm class to DeflateCompressor.

```
ALTER TABLE CatTypes  
WITH compression = { 'class' : 'DeflateCompressor',  
    'chunk_length_in_kb' : 64 }
```

You tune data compression on a per-table basis using CQL to alter a table.

Testing compaction and compression

Write survey mode is a Cassandra startup option for testing new compaction and compression strategies. In write survey mode, you can test out new compaction and compression strategies on that node and benchmark the write performance differences, without affecting the production cluster.

Write survey mode adds a node to a database cluster. The node accepts all write traffic as if it were part of the normal Cassandra cluster, but the node does not officially join the ring.

Also use write survey mode to try out a new Cassandra version. The nodes you add in write survey mode to a cluster must be of the same major release version as other nodes in the cluster. The write survey mode relies on the streaming subsystem that transfers data between nodes in bulk and differs from one major release to another.

If you want to see how read performance is affected by modifications, stop the node, bring it up as a standalone machine, and then benchmark read operations on the node.

Procedure

Start the Cassandra node by adding the `write_survey` option to the `cassandra-env.ps1` file:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.write_survey=true"
```

Tuning Bloom filters

Cassandra uses Bloom filters to determine whether an SSTable has data for a particular partition. Bloom filters are unused for range scans, but are used for index scans. Bloom filters are probabilistic sets that allow you to trade memory for accuracy. This means that higher Bloom filter attribute settings `bloom_filter_fp_chance` use less memory, but will result in more disk I/O if the SSTables are highly fragmented. Bloom filter settings range from 0 to 1.0 (disabled). The default value of `bloom_filter_fp_chance` depends on the `compaction strategy`. The `LeveledCompactionStrategy` uses a higher default value (0.1) than the `SizeTieredCompactionStrategy` or `DateTieredCompactionStrategy`, which have a default of 0.01. Memory savings are nonlinear; going from 0.01 to 0.1 saves about one third of the memory. SSTables using LCS contain a relatively smaller ranges of keys than those using STCS, which facilitates efficient exclusion of the SSTables even without a bloom filter; however, adding a small bloom filter helps when there are many levels in LCS.

The settings you choose depend the type of workload. For example, to run an analytics application that heavily scans a particular table, you would want to inhibit the Bloom filter on the table by setting it high.

To view the observed Bloom filters false positive rate and the number of SSTables consulted per read use `tablestats` in the `nodetool` utility.

Bloom filters are stored off-heap so you don't need include it when determining the `-Xmx` settings (the maximum memory size that the heap can reach for the JVM).

To change the `bloom filter property` on a table, use CQL. For example:

```
ALTER TABLE addamsFamily WITH bloom_filter_fp_chance = 0.1;
```

After updating the value of `bloom_filter_fp_chance` on a table, Bloom filters need to be regenerated in one of these ways:

- [Initiate compaction](#)
- [Upgrade SSTables](#)

You do not have to restart Cassandra after regenerating SSTables.

Moving data to or from other databases

Cassandra offers several solutions for migrating from other databases:

- The [COPY command](#), which mirrors what the PostgreSQL RDBMS uses for file/export import.
- The [Cassandra bulk loader](#) provides the ability to bulk load external data into a cluster.

About the COPY command

You can use COPY in CQL shell to load flat file data into Cassandra (nearly all relational databases have unload utilities that allow table data to be written to OS files) as well to write Cassandra data to CSV files.

ETL Tools

If you need more sophistication applied to a data movement situation (more than just extract-load), then you can use any number of extract-transform-load (ETL) solutions that now support Cassandra. These tools provide excellent transformation routines that allow you to manipulate source data in literally any way you need and then load it into a Cassandra target. They also supply many other features such as visual, point-and-click interfaces, scheduling engines, and more.

Many ETL vendors who support Cassandra supply community editions of their products that are free and able to solve many different use cases. Enterprise editions are also available that supply many other compelling features that serious enterprise data users need.

You can freely download and try ETL tools from Jaspersoft, Pentaho, and Talend that all work with Cassandra.

Purging gossip state on a node

Gossip information is persisted locally by each node to use immediately on node restart without having to wait for gossip communications.

Procedure

In the unlikely event you need to correct a problem in the gossip state:

1. Use the [nodetool assassinate](#) to shut down the problem node.

This takes approximately 35 seconds to complete, so wait for confirmation that the node is deleted.

2. If this method doesn't solve the problem, stop your client application from sending writes to the cluster.
3. Take the entire cluster offline:
 - a) [Drain](#) each node.

```
C:\> %CASSANDRA_HOME%\bin\nodetool options drain
```

- b) Stop each node:

```
C:\> net stop DataStax-DDC_Server
```

4. Clear the data from the `peers` directory, remove all directories in the `peers-UUID` directory, where `UUID` is the particular directory that corresponds to the appropriate node:

```
C:\> rmdir "Program Files\DataStax-DDC\data\data\system\peers-UUID\*" /s
```

CAUTION:

Use caution when performing this step. The action clears internal system data from Cassandra and may cause application outage without careful execution and validation of the results. To validate the results, run the following query individually on each node to confirm that all of the nodes are able to see all other nodes.

```
select * from system.peers;
```

5. Add the following line to the `cassandra-env.ps1` file to clear the gossip state when the node starts:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.load_ring_state=false"
```

6. Bring the cluster online one node at a time, starting with the seed nodes.

```
C:\> net start DataStax-DDC_Server
```

What to do next

Remove the line you added in the `cassandra-env.ps1` file.

Cassandra tools

The nodetool utility

The nodetool utility is a command line interface for managing a cluster.

Command formats

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] command [args]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- The repair and rebuild commands can affect multiple nodes in the cluster.
- Most nodetool commands operate on a single node in the cluster if -h is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the -h option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using -h.

Example

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra describing
demo_keyspace
```

Getting nodetool help

nodetool help

Provides a listing of nodetool commands.

nodetool help *command name*

Provides help on a specific command. For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool help upgradestables
```

nodetool assassinate

Forcefully removes a dead node without re-replicating any data. It is a last resort tool if you cannot successfully use [nodetool removenode](#).

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] assassinate [args]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool assassinate` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The `nodetool assassinate` command is a tool of last resort. Only use this tool to remove a node from a cluster when `removenode` is not successful.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra assassinate 192.168.100.2
```

nodetool bootstrap

Monitor and manage a node's bootstrap process.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] bootstrap [resume]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool bootstrap` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The `nodetool bootstrap` command can be used to monitor and manage a node's bootstrap process. If no argument is defined, the help information is displayed. If the argument `resume` is used, bootstrap streaming is resumed.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra bootstrap resume
```

nodetool cfhistograms

This tool has been renamed as [tablehistograms](#).

nodetool cfstats

This tool has been renamed as [nodetool tablestats](#).

nodetool cleanup

Cleans up keyspaces and partition keys no longer belonging to a node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> cleanup --
<keyspace> (<table> ...)
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option from an argument that could be mistaken for a option.
- keyspace is a keyspace name.
- table is one or more table names, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Use this command to remove unwanted data after adding a new node to the cluster. Cassandra does not automatically remove data from nodes that lose part of their partition range to a newly added node. Run `nodetool cleanup` on the source node and on neighboring nodes that shared the same subrange after the new node is up and running. Failure to run this command after adding a node causes Cassandra to include the old data to rebalance the load on that node. Running the `nodetool cleanup` command causes a temporary increase in disk space usage proportional to the size of your largest SSTable. Disk I/O occurs when running this command.

Running this command affects nodes that use a counter column in a table. Cassandra assigns a new counter ID to the node.

Optionally, this command takes a list of table names. If you do not specify a keyspace, this command cleans all keyspaces no longer belonging to a node.

nodetool clearsnapshot

Removes one or more snapshots.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> clearsnapshot -t <snapshot> -- (
<keyspace> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- t means the following file contains the snapshot.
- snapshot is the name of the snapshot.
- separates an option from an argument that could be mistaken for a option.
- keyspace is one or more keyspace names, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Deletes snapshots in one or more keyspaces. To remove all snapshots, omit the snapshot name.

Note: The `clearsnapshot` command doesn't always succeed when invoked (if, for example, the associated sstables are still being mapped). If `clearsnapshot` fails, Cassandra retries periodically, and also when the node is shutdown or restarted.

nodetool compact

Forces a major [compaction](#) on one or more tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> compact <keyspace> ( <table>
... )
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address.
-p	--port	Remote JMX agent port number.
-pw	--password	Password.
-pwf	--password-file	Password file path.

Short	Long	Description
-s	--split-output	Split output of STCS files to 50%-25%-12.5%-etc. of the total size.
-u	--username	Remote JMX agent user name.
	--user-defined	Submit listed files for user-defined compaction. For Casassandra 3.4 and later.

Note:

- If a username and password for RMI authentication are set explicitly in the cassandra-env.ps1 file for the host, then you must specify credentials.
- No -s will create one large SSTable for STCS.
- -s will not affect DTCS; it will create one large SSTable.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This command starts the [compaction process](#) on tables using SizeTieredCompactionStrategy (STCS), DateTieredCompactionStrategy (DTCS), or Leveled compaction (LCS):

- If you do not specify a keyspace or table, a major compaction is run on all keyspaces and tables.
- If you specify only a keyspace, a major compaction is run on all tables in that keyspace.
- If you specify one or more tables, a major compaction is run on those tables.

Major compactions may behave differently depending which compaction strategy is used for the affected tables:

- `SizeTieredCompactionStrategy` (STCS): The default compaction strategy. This strategy triggers a minor compaction when there are a number of similar sized SSTables on disk as configured by the table subproperty, `min_threshold`. A minor compaction does not involve all the tables in a keyspace. Also see [STCS compaction subproperties](#).
- `DateTieredCompactionStrategy` (DTCS): This strategy is particularly useful for [time series data](#). `DateTieredCompactionStrategy` stores data written within a certain period of time in the same SSTable. For example, Cassandra can store your last hour of data in one SSTable *time window*, and the next 4 hours of data in another time window, and so on. Compactions are triggered when the `min_threshold` (4 by default) for SSTables in those windows is reached. The most common queries for time series workloads retrieve the last hour/day/month of data. Cassandra can limit SSTables returned to those having the relevant data. Also, Cassandra can store data that has been set to expire using TTL in an SSTable with other data scheduled to expire at approximately the same time. Cassandra can then drop the SSTable without doing any compaction. Also see [DTCS compaction subproperties](#) and [DateTieredCompactionStrategy: Compaction for Time Series Data](#).
- `LeveledCompactionStrategy` (LCS): The leveled compaction strategy creates SSTables of a fixed, relatively small size (160 MB by default) that are grouped into levels. Within each level, SSTables are guaranteed to be non-overlapping. Each level (L0, L1, L2 and so on) is 10 times as large as the previous. Disk I/O is more uniform and predictable on higher than on lower levels as SSTables are continuously being compacted into progressively larger levels. At each level, row keys are merged into non-overlapping SSTables in the next level. This process can improve performance for reads, because Cassandra can determine which SSTables in each level to check for the existence of row key data. This compaction strategy is modeled after Google's LevelDB implementation. Also see [LCS compaction subproperties](#).

For more details, see [How is data maintained?](#) and [Configuring compaction](#).

Note: A major compaction can cause considerably more disk I/O than minor compactons.

nodetool compactionhistory

Provides the history of compaction operations.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> compactionhistory
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Example

The actual output of compaction history is seven columns wide. The first three columns show the id, keyspace name, and table name of the compacted SSTable.

```
C:\> %CASSANDRA_HOME%\bin\nodetool compactionhistory
```

```
Compaction History:
id                keyspace_name
columnfamily_name
d06f7080-07a5-11e4-9b36-abc3a0ec9088    system
schema_columnfamilies
d198ae40-07a5-11e4-9b36-abc3a0ec9088    libdata          users
0381bc30-07b0-11e4-9b36-abc3a0ec9088    Keyspace1        Standard1
74eb69b0-0621-11e4-9b36-abc3a0ec9088    system           local
e35dd980-07ae-11e4-9b36-abc3a0ec9088    system
compactions_in_progress
8d5cf160-07ae-11e4-9b36-abc3a0ec9088    system
compactions_in_progress
ba376020-07af-11e4-9b36-abc3a0ec9088    Keyspace1        Standard1
d18cc760-07a5-11e4-9b36-abc3a0ec9088    libdata          libout
64009bf0-07a4-11e4-9b36-abc3a0ec9088    libdata          libout
d04700f0-07a5-11e4-9b36-abc3a0ec9088    system           sstable_activity
c2a97370-07a9-11e4-9b36-abc3a0ec9088    libdata          users
cb928a80-07ae-11e4-9b36-abc3a0ec9088    Keyspace1        Standard1
cd8d1540-079e-11e4-9b36-abc3a0ec9088    system           schema_columns
62ced2b0-07a4-11e4-9b36-abc3a0ec9088    system           schema_keyspaces
d19cccf0-07a5-11e4-9b36-abc3a0ec9088    system
compactions_in_progress
640bbf80-07a4-11e4-9b36-abc3a0ec9088    libdata          users
6cd54e60-07ae-11e4-9b36-abc3a0ec9088    Keyspace1        Standard1
c29241f0-07a9-11e4-9b36-abc3a0ec9088    libdata          libout
```

c2a30ad0-07a9-11e4-9b36-abc3a0ec9088	system		
compactions_in_progress			
e3a6d920-079d-11e4-9b36-abc3a0ec9088	system	schema_keyspaces	
62c55cd0-07a4-11e4-9b36-abc3a0ec9088	system		
schema_columnfamilies			
62b07540-07a4-11e4-9b36-abc3a0ec9088	system	schema_columns	
cdd038c0-079e-11e4-9b36-abc3a0ec9088	system	schema_keyspaces	
b797af00-07af-11e4-9b36-abc3a0ec9088	Keyspace1	Standard1	
8c918b10-07ae-11e4-9b36-abc3a0ec9088	Keyspace1	Standard1	
377d73f0-07ae-11e4-9b36-abc3a0ec9088	system		
compactions_in_progress			
62b9c410-07a4-11e4-9b36-abc3a0ec9088	system	local	
d0566a40-07a5-11e4-9b36-abc3a0ec9088	system	schema_columns	
ba637930-07af-11e4-9b36-abc3a0ec9088	system		
compactions_in_progress			
cdbc1480-079e-11e4-9b36-abc3a0ec9088	system		
schema_columnfamilies			
e3456f80-07ae-11e4-9b36-abc3a0ec9088	Keyspace1	Standard1	
d086f020-07a5-11e4-9b36-abc3a0ec9088	system	schema_keyspaces	
d06118a0-07a5-11e4-9b36-abc3a0ec9088	system	local	
cdaafd80-079e-11e4-9b36-abc3a0ec9088	system	local	
640fde30-07a4-11e4-9b36-abc3a0ec9088	system		
compactions_in_progress			
37638350-07ae-11e4-9b36-abc3a0ec9088	Keyspace1	Standard1	

The four columns to the right of the table name show the timestamp, size of the SSTable before and after compaction, and the number of partitions merged. The notation means {tables:rows}. For example: {1:3, 3:1} means 3 rows were taken from one SSTable (1:3) and 1 row taken from 3 SSTables (3:1) to make the one SSTable in that compaction operation.

compacted_at	bytes_in	bytes_out	rows_merged
1404936947592	8096	7211	{1:3, 3:1}
1404936949540	144	144	{1:1}
1404941328243	1305838191	1305838191	{1:4647111}
1404770149323	5864	5701	{4:1}
1404940844824	573	148	{1:1, 2:2}
1404940700534	576	155	{1:1, 2:2}
1404941205282	766331398	766331398	{1:2727158}
1404936949462	8901649	8901649	{1:9315}
1404936336175	8900821	8900821	{1:9315}
1404936947327	223	108	{1:3, 2:1}
1404938642471	144	144	{1:1}
1404940804904	383020422	383020422	{1:1363062}
1404933936276	4889	4177	{1:4}
1404936334171	441	281	{1:3, 2:1}
1404936949567	379	79	{2:2}
1404936336248	144	144	{1:1}
1404940645958	307520780	307520780	{1:1094380}
1404938642319	8901649	8901649	{1:9315}
1404938642429	416	165	{1:3, 2:1}
1404933543858	692	281	{1:3, 2:1}
1404936334109	7760	7186	{1:3, 2:1}
1404936333972	4860	4724	{1:2, 2:1}
1404933936715	441	281	{1:3, 2:1}
1404941200880	1269180898	1003196133	{1:2623528, 2:946565}
1404940699201	297639696	297639696	{1:1059216}
1404940556463	592	148	{1:2, 2:2}
1404936334033	5760	5680	{2:1}
1404936947428	8413	5316	{1:2, 3:1}
1404941205571	429	42	{2:2}
1404933936584	7994	6789	{1:4}

```

. . . 1404940844664      306699417      306699417      {1:1091457}
. . . 1404936947746      601            281            {1:3, 3:1}
. . . 1404936947498      5840           5680           {3:1}
. . . 1404933936472      5861           5680           {3:1}
. . . 1404936336275      378            80             {2:2}
. . . 1404940556293      302170540      281000000      {1:924660, 2:75340}

```

nodetool compactionstats

Provide statistics about a compaction.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> compactionstats -H
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- data center is the name of an arbitrarily chosen data center from which to select sources for streaming.
- H converts bytes to a human readable form: kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The total column shows the total number of uncompressed bytes of SSTables being compacted. The system log lists the names of the SSTables compacted.

Example

```
C:\> %CASSANDRA_HOME%\bin\nodetool compactionstats
```

```

pending tasks: 5
      compaction type      keyspace      table      completed
      total      unit      progress
      302170540      bytes      93.43%      Compaction      Keyspace1      Standard1      282310680
      307520780      bytes      19.01%      Compaction      Keyspace1      Standard1      58457931
Active compaction remaining time : 0h00m16s

```

nodetool decommission

Deactivates a node by streaming its data to another node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> decommission
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Causes a live node to decommission itself, streaming its data to the next node on the ring. Use [netstats](http://wiki.apache.org/cassandra/NodeProbe#Decommission) to monitor the progress, as described on <http://wiki.apache.org/cassandra/NodeProbe#Decommission> and http://wiki.apache.org/cassandra/Operations#Removing_nodes_entirely.

nodetool describcluster

Provide the name, snitch, partitioner and schema version of a cluster

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> describcluster -- <data center>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- data center is the name of an arbitrarily chosen data center from which to select sources for streaming.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Describe cluster is typically used to validate the schema after upgrading. If a schema disagreement occurs, check for and [resolve schema disagreements](#).

Example

```
C:\> %CASSANDRA_HOME%\bin\nodetool describecluster
```

```
Cluster Information:
Name: Test Cluster
Snitch: org.apache.cassandra.locator.DynamicEndpointSnitch
Partitioner: org.apache.cassandra.dht.Murmur3Partitioner
Schema versions:
    65e78f0e-e81e-30d8-a631-a65dff93bf82: [127.0.0.1]
```

If a schema disagreement occurs, the last line of the output includes information about unreachable nodes.

```
C:\> %CASSANDRA_HOME%\bin\nodetool describecluster
```

```
Cluster Information:
Name: Production Cluster
    Snitch: org.apache.cassandra.locator.DynamicEndpointSnitch
    Partitioner: org.apache.cassandra.dht.Murmur3Partitioner
    Schema versions:
        UNREACHABLE: 1176b7ac-8993-395d-85fd-41b89ef49fbb:
[10.202.205.203]
```

nodetool describering

Provides the partition ranges of a keyspace.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> describering -- <keyspace>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option from an argument that could be mistaken for a option.
- keyspace is a keyspace name.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Example

This example shows the sample output of the command on a three-node cluster.

```
C:\> %CASSANDRA_HOME%\bin\nodetool describering demo_keyspace
```

```
Schema Version:1b04bd14-0324-3fc8-8bcb-9256d1e15f82
TokenRange:
    TokenRange(start_token:3074457345618258602,
    end_token:-9223372036854775808,
```



```

        endpoints:[127.0.0.1, 127.0.0.2, 127.0.0.3],
        rpc_endpoints:[127.0.0.1, 127.0.0.2, 127.0.0.3],
        endpoint_details:[EndpointDetails(host:127.0.0.1,
datacenter:datacenter1, rack:rack1),
        EndpointDetails(host:127.0.0.2, datacenter:datacenter1,
rack:rack1),
        EndpointDetails(host:127.0.0.3, datacenter:datacenter1,
rack:rack1)]]
TokenRange(start_token:-3074457345618258603,
end_token:3074457345618258602,
        endpoints:[127.0.0.3, 127.0.0.1, 127.0.0.2],
        rpc_endpoints:[127.0.0.3, 127.0.0.1, 127.0.0.2],
        endpoint_details:[EndpointDetails(host:127.0.0.3,
datacenter:datacenter1, rack:rack1),
        EndpointDetails(host:127.0.0.1, datacenter:datacenter1,
rack:rack1),
        EndpointDetails(host:127.0.0.2, datacenter:datacenter1,
rack:rack1)]]
TokenRange(start_token:-9223372036854775808,
end_token:-3074457345618258603,
        endpoints:[127.0.0.2, 127.0.0.3, 127.0.0.1],
        rpc_endpoints:[127.0.0.2, 127.0.0.3, 127.0.0.1],
        endpoint_details:[EndpointDetails(host:127.0.0.2,
datacenter:datacenter1, rack:rack1),
        EndpointDetails(host:127.0.0.3, datacenter:datacenter1,
rack:rack1),
        EndpointDetails(host:127.0.0.1, datacenter:datacenter1,
rack:rack1)]]

```

If a schema disagreement occurs, the last line of the output includes information about unreachable nodes.

```
C:\> %CASSANDRA_HOME%\bin\nodetool describecluster
```

```

Cluster Information:
Name: Production Cluster
Snitch: org.apache.cassandra.locator.DynamicEndpointSnitch
Partitioner: org.apache.cassandra.dht.Murmur3Partitioner
Schema versions:
    UNREACHABLE: 1176b7ac-8993-395d-85fd-41b89ef49fbb:
[10.202.205.203]

```

nodetool disableautocompaction

Disables autocompaction for a keyspace and one or more tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> disableautocompaction --
<keyspace> ( <table> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.

- `table` is one or more table names, separated by a space.
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The keyspace can be followed by one or more tables.

nodetool disablebackup

Disables incremental backup.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> disablebackup
```

Options are:

- (`-h` | `--host`) `<host name>` | `<ip address>`
- (`-p` | `--port`) `<port number>`
- (`-pw` | `--password`) `<password >`
- (`-u` | `--username`) `<user name>`
- (`-pwf` `<passwordFilePath>` | `--password-file` `<passwordFilePath>`)
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

nodetool disablebinary

Disables the native transport.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> disablebinary
```

Options are:

- (`-h` | `--host`) `<host name>` | `<ip address>`
- (`-p` | `--port`) `<port number>`
- (`-pw` | `--password`) `<password >`
- (`-u` | `--username`) `<user name>`
- (`-pwf` `<passwordFilePath>` | `--password-file` `<passwordFilePath>`)
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

Disables the binary protocol, also known as the native transport.

nodetool disablegossip

Disables the gossip protocol.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> disablegossip
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This command effectively marks the node as being down.

nodetool disablehandoff

Disables storing of future hints on the current node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> disablehandoff
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool disablehintsfordc

Disable hints for a data center.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] disablehintsfordc [--]
<datacenter>
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool disablehintsfordc` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.
- `[--]` can be used to separate command-line options from the list of arguments, when the list might be mistaken for options.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool disablehintsfordc` command is used to turn off hints for a data center. This can be useful if there is a downed data center, but hints should continue on other data centers. Another common case is during data center failover, when hints will put unnecessary pressure on the data center.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra
disablehintsfordc DC2
```

nodetool disablethrift

Disables the Thrift server.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] disablethrift [args]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool disablethrift` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

`nodetool disablethrift` will disable thrift on a node preventing the node from acting as a coordinator. The node can still be a replica for a different coordinator and data read at consistency level ONE could be stale. To cause a node to ignore read requests from other coordinators, `nodetool disablegossip` would also need to be run. However, if both commands are run, the node will not perform repairs, and the node will continue to store stale data. If the goal is to repair the node, set the read operations to a consistency level of QUORUM or higher while you run repair. An alternative approach is to delete the node's data and restart the Cassandra process.

Note that the `nodetool` commands using the `-h` option will not work remotely on a disabled node until `nodetool enablethrift` and `nodetool enablegossip` are run locally on the disabled node.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra disablethrift 192.168.100.1
```

nodetool drain

Drains the node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> drain
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>

- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Flushes all memtables from the node to SSTables on disk. Cassandra stops listening for connections from the client and other nodes. You need to restart Cassandra after running `nodetool drain`. You typically use this command before upgrading a node to a new version of Cassandra. To simply flush memtables to disk, use `nodetool flush`.

nodetool enableautocompaction

Enables autocompaction for a keyspace and one or more tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enableautocompaction --
<keyspace> ( <table> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.
- table is the name of one or more keyspaces, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The keyspace can be followed by one or more tables. Enables compaction for the named keyspace or the current keyspace, and one or more named tables, or all tables.

nodetool enablebackup

Enables incremental backup.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enablebackup
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool enablebinary

Re-enables native transport.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enablebinary
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Re-enables the binary protocol, also known as native transport.

nodetool enablegossip

Re-enables gossip.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enablegossip
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>

- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool enablehandoff

Re-enables the storing of future hints on the current node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enablehandoff
```

- options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- <dc-name>,<dc-name> means enable hinted handoff only for these data centers
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool enablehintsfordc

Enable hints for a data center.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] enablehintsfordc [--]
<datacenter>
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool enablehintsfordc` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.
- `[-]` can be used to separate command-line options from the list of arguments, when the list might be mistaken for options.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The `nodetool enablehintsfordc` command is used to turn on hints for a data center. The `cassandra.yaml` file has a parameter, `hinted_handoff_disabled_datacenters` that will blacklist data centers on startup. If a data center can be enabled later with `nodetool enablehintsfordc`.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra enablehintsfordc
DC2
```

nodetool enablethrift

Re-enables the Thrift server.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> enablethrift
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password >
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath | `--password-file` <passwordFilePath>)
- Angle brackets (`<` `>`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

nodetool flush

Flushes one or more tables from the memtable.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> flush -- <keyspace> (
    <table> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.
- table is the name of one or more tables, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

You can specify a keyspace followed by one or more tables that you want to flush from the memtable to SSTables on disk.

nodetool gcstats

Print garbage collection (GC) statistics.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] gcstats
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the cassandra-env.ps1 file for the host, then you must specify credentials.

- `nodetool gcstats` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The `nodetool gcstats` command will print garbage collection statistics that returns values based on all the garbage collection that has run since the last time `nodetool gcstats` was run. Statistics identify the interval time, some GC elapsed time measures, the disk space reclaimed (in MB), number of garbage collections that took place, and direct memory bytes.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra gcstats
```

nodetool getcompactionthreshold

Provides the minimum and maximum compaction thresholds in megabytes for a table.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> getcompactionthreshold --  
<keyspace> <table>
```

- Options are:
 - (`-h` | `--host`) `<host name>` | `<ip address>`
 - (`-p` | `--port`) `<port number>`
 - (`-pw` | `--password`) `<password >`
 - (`-u` | `--username`) `<user name>`
 - (`-pwf` `<passwordFilePath>` | `--password-file` `<passwordFilePath>`)
- `--` separates an option and argument that could be mistaken for a option.
- `keyspace` is the name of a keyspace.
- `table` is the name of a table.
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

nodetool getcompactionthroughput

Print the throughput cap (in MB/s) for compaction in the system.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] getcompactionthroughput
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool getcompactionthroughput` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

A semicolon that terminates CQL statements is not included in the synopsis.

Description

The `nodetool getcompactionthroughput` command prints the current compaction throughput.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra
getcompactionthroughput
```

nodetool getendpoints

Provides the IP addresses or names of replicas that own the partition key.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> getendpoints -- <keyspace>
<table> key
```

- Options are:
 - (-h | --host) <host name> | <ip address>

- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- table is a table name.
- key is the partition key of the end points you want to get.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Example

For example, which nodes own partition key_1, key_2, and key_3?

Note: The partitioner returns a token for the key. Cassandra will return an endpoint whether or not data exists on the identified node for that token.

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h 127.0.0.1 -p 7100 getendpoints myks
mytable key_1
```

```
127.0.0.2
```

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h 127.0.0.1 -p 7100 getendpoints myks
mytable key_2
```

```
127.0.0.2
```

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h 127.0.0.1 -p 7100 getendpoints myks
mytable key_2
```

```
127.0.0.1
```

nodetool getlogginglevels

Get the runtime logging levels.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> getlogginglevels
```

options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password>
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional

- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool getsstables

Provides the SSTables that own the partition key.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> getsstables [(-hf | --hex-format)] -- <keyspace> <table> <key>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- table is a table name.
- key is the partition key of the SSTables.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This command can be used to retrieve an SSTable.

Examples

An example of this command retrieves the SSTable for `cycling.cyclist_name` with the key argument `fb372533-eb95-4bb4-8685-6ef61e994caa` for one of the cyclists listed:

```
C:\> %CASSANDRA_HOME%\bin\nodetool getsstables cycling cyclist_name 'fb372533-eb95-4bb4-8685-6ef61e994caa'
```

The output is:

```
/homedir/datastax-ddc-3.6.0/data/data/cycling/
cyclist_name-612a64002ec211e6a92457e568fce26f/ma-1-big-Data.db
```

```
C:\> %CASSANDRA_HOME%\bin\nodetool getsstables keyspace1 standard1
3330394c344e35313730
```

nodetool getstreamthroughput

Provides the Mb (megabit) per second outbound throughput limit for streaming in the system.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> getstreamthroughput
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool gettimeout

Print the timeout value of the given type in milliseconds.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] gettimeout [--] <timeout_type>
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the cassandra-env.ps1 file for the host, then you must specify credentials.
- -- separates an option and argument that could be mistaken for a option.
- The timeout type:
 - read
 - range
 - write
 - counterwrite
 - cascontention
 - truncate
 - streamingsocket
 - misc, such as general rpc_timeout_in_ms

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal

- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool gettimeout` command prints the timeout value of the given type in milliseconds. Several timeouts are available.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra gettimeout read
```

nodetool gettraceprobability

Get the current trace probability.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> gettraceprobability
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- value is a probability between 0 and 1.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Provides the current trace probability. To set the trace probability, see [nodetool settraceprobability](#).

nodetool gossipinfo

Provides the gossip information for the cluster.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> gossipinfo
```

Options are:

- (-h | --host) <host name> | <ip address>

- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool help

Provides nodetool command help.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool help <command>
```

- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The help command provides a synopsis and brief description of each nodetool command.

Examples

Using nodetool help lists all commands and usage information. For example, `nodetool help netstats` provides the following information.

```
NAME
    nodetool netstats - Print network information on provided host
    (connecting node by default)

SYNOPSIS
    nodetool [(-h <host> | --host <host>)] [(-p <port> | --port <port>)]
    [(-pw <password> | --password <password>)]
    [(-u <username> | --username <username>)] netstats

OPTIONS
    -h <host>, --host <host>
        Node hostname or ip address

    -p <port>, --port <port>
        Remote jmx agent port number

    -pw <password>, --password <password>
        Remote jmx agent password

    -u <username>, --username <username>
        Remote jmx agent username
```

nodetool info

Provides node information, such as load and uptime.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> info ( -T | --tokens )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password>
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- T or --tokens means provide all token information.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Provides node information including the token and on disk storage (load) information, times started (generation), uptime in seconds, and heap memory usage.

nodetool invalidatecountercache

Invalidates the counter cache, and resets the global counter cache parameter, counter_cache_keys_to_save, to the default (not set), which saves all keys..

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] invalidatecountercache
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the cassandra-env.ps1 file for the host, then you must specify credentials.
- `nodetool invalidatecountercache` operates on a single node in the cluster if -h is not used to identify one or more other nodes. If the node from which you issue the command is the intended target,

you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

The `nodetool invalidatecountercache` command will invalidate the counter cache, and the system will start saving all counter keys.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra  
invalidatecountercache
```

nodetool invalidatekeycache

Resets the global key cache parameter to the default, which saves all keys.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> invalidatekeycache
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password >
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath> | `--password-file` <passwordFilePath>)
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

By default the `key_cache_keys_to_save` is disabled in the `cassandra.yaml`. This command resets the parameter to the default.

nodetool invalidaterowcache

Resets the global key cache parameter, `row_cache_keys_to_save`, to the default (not set), which saves all keys.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> invalidaterowcache
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool join

Causes the node to join the ring.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> join
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Causes the node to join the ring, assuming the node was initially *not* started in the ring using the - [Djoin_ring=false](#) cassandra utility option. The joining node should be properly configured with the desired options for seed list, initial token, and auto-bootstrapping.

nodetool listsnapshots

Lists snapshot names, size on disk, and true size.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> listsnapshots
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Example

```
Snapshot Details:
Snapshot Name    Keyspace    Column Family    True Size    Size on Disk
1387304478196    Keyspace1    Standard1        0 bytes      308.66 MB
1387304417755    Keyspace1    Standard1        0 bytes      107.21 MB
1387305820866    Keyspace1    Standard2        0 bytes      41.69 MB
                  Keyspace1    Standard1        0 bytes      308.66 MB
```

nodetool move

Moves the node on the token ring to a new token.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> move -- <new token>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- new token is a number in the range -2^{63} to $+2^{63}-1$.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Escape negative tokens using \ . For example: move \-123. This command moves a node from one token value to another. This command is generally used to shift tokens slightly.

nodetool netstats

Provides network information about the host.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> netstats -H
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password>
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- H converts bytes to a human readable form: kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The default host is the connected host if the user does not include a host name or IP address in the command. The output includes the following information:

- JVM settings
- Mode

The operational mode of the node: JOINING, LEAVING, NORMAL, DECOMMISSIONED, CLIENT
- Read repair statistics
- Attempted

The number of successfully completed [read repair operations](#)
- Mismatch (blocking)

The number of read repair operations since server restart that blocked a query.
- Mismatch (background)

The number of read repair operations since server restart performed in the background.
- Pool name

Information about client read and write requests by thread pool.
- Active, pending, and completed number of commands and responses

Example

Get the network information for a node 10.171.147.128:

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h 10.171.147.128 netstats
```

The output is:

```
Mode: NORMAL
Not sending any streams.
Read Repair Statistics:
```

```

Attempted: 0
Mismatch (Blocking): 0
Mismatch (Background): 0
Pool Name      Active   Pending   Completed
Commands       n/a      0         1156
Responses      n/a      0         2750

```

nodetool pausehandoff

Pauses the hints delivery process

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> pausehandoff
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool proxyhistograms

Provides a histogram of network statistics.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> proxyhistograms
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The output of this command shows the full request latency recorded by the coordinator. The output includes the percentile rank of read and write latency values for inter-node communication. Typically, you use the command to see if requests encounter a slow node.

Examples

This example shows the output from `nodetool proxyhistograms` after running 4,500 insert statements and 45,000 select statements on a three [ccm](#) node-cluster on a local computer.

```
C:\> %CASSANDRA_HOME%\bin\nodetool proxyhistograms
```

```
proxy histograms
Percentile      Read Latency      Write Latency      Range Latency
                (micros)         (micros)           (micros)
50%             1502.50           375.00             446.00
75%             1714.75           420.00             498.00
95%             31210.25          507.00             800.20
98%             36365.00          577.36             948.40
99%             36365.00          740.60            1024.39
Min              616.00           230.00             311.00
Max             36365.00          55726.00           59247.00
```

nodetool rangekeysample

Provides the sampled keys held across all keyspaces.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> rangekeysample
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password >
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath> | `--password-file` <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool rebuild

Rebuilds data by streaming from other nodes.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool options rebuild
[ -ks keyspace_name [ , keyspace_name ] [ . . . ] | --keyspace keyspace_name
[ , keyspace_name ] [ . . . ] ]
[ -ts token_spec | --tokens token_spec ]
```



```
[ -- src-dc-name ]
```

- options
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- *keyspace_name*
The name of the keyspace to rebuild. The `rebuild` command works with a single keyspace name or a comma-delimited list of keyspace names.
- *token_spec*
One or more tokens, and/or one or more ranges of tokens. The *token_spec* can be:
 - One specific token
 - A comma-delimited list of single tokens
 - A range of tokens, specified as (*start_token*, *end_token*)
 - A comma-delimited list of token ranges — for example, (*start_token1*, *end_token1*) , (*start_token2*, *end_token2*, . . .
 - A comma-delimited list of mixed single tokens and token ranges — for example, *token1*, (*start_token2*, *end_token2*) , (*start_token3*, *end_token3*) , *token4*, . . .
- -- separates an option and argument that could be mistaken for a option.
- *src-dc-name*
The name of the data center Cassandra uses as the source for streaming. Cassandra rebuilds from any data center. If the statement does not specify one, Cassandra chooses at random.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This command operates on multiple nodes in a cluster. Like [nodetool bootstrap](#), `rebuild` only streams data from a single source replica per range. Use this command to [add a new datacenter](#) to an existing cluster. If `bootstrap` fails because some token ranges cannot be retrieved, use the `-ts` or `--token` option to specify a list of tokens, or one or more token ranges.

nodetool rebuild_index

Performs a full rebuild of the index for a table

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> rebuild_index -- (
  <keyspace>.<table>.<indexName> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >

- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- table is a table name.
- indexName is an optional list of index names separated by a space.

The keyspace and table name followed by a list of index names. For example: `Standard3.IdxName`
`Standard3.IdxName1`

- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Fully rebuilds one or more indexes for a table.

nodetool refresh

Loads newly placed SSTables onto the system without a restart.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> refresh -- <keyspace> <table>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- table is a table name.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool refreshsizeestimates

Refreshes system.size_estimates table. Use when huge amounts of data are inserted or truncated which can result in size estimates becoming incorrect.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> refreshsizeestimates
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
 - (-u | --username) <user name>
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool reloadtriggers

Reloads trigger classes.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> reloadtriggers
```

options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool relocatesstables

In Cassandra 3.2 and later, rewrites any SSTable that contains tokens that should be in another data directory for JBOD disks. Basically, this commands relocates SSTables to the correct disk.

Synopsis

```
$ nodetool <options> relocatesstables -- <keyspace> <table>
```

- options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.

- `table` is a table name.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

This `nodetool` command can be used to manually rewrite the location of SSTables on disk. It is for use with JBOD disk storage. The command can also be used if you change the replication factor for the cluster stored on JBOD or if you add a new disk. If all the token are correctly stored in the data directories, `nodetool relocatesstables` will have no effect.

Examples

Text

```
$ nodetool relocatesstables cycling
```

nodetool removemode

Provides the status of current node removal, forces completion of pending removal, or removes the identified node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> removemode -- <status> | <force>
| <ID>
```

- Options are:
 - (`-h` | `--host`) `<host name>` | `<ip address>`
 - (`-p` | `--port`) `<port number>`
 - (`-pw` | `--password`) `<password >`
 - (`-u` | `--username`) `<user name>`
 - (`-pwf` `<passwordFilePath>` | `--password-file` `<passwordFilePath>`)
- `--` separates an option and argument that could be mistaken for a option.
- `status` provides status information.
- `force` forces completion of the pending removal.
- `ID` is the host ID, in UUID format.
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

This command removes a node, shows the status of a removal operation, or forces the completion of a pending removal. When the node is down and `nodetool decommission` cannot be used, use

`nodetool removenode`. Run this command only on nodes that are down. If the cluster does not use `vnodes`, before running the `nodetool removenode` command, [adjust the tokens](#).

Examples

Determine the UUID of the node to remove by running `nodetool status`. Use the UUID of the node that is down to remove the node.

```
C:\> %CASSANDRA_HOME%\bin\nodetool status
```

```
Datacenter: DC1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens   Owns (effective)  Host ID
   Rack
UN  192.168.2.101    112.82 KB    256      31.7%             420129fc-0d84-42b0-be41-ef7dd3a8ad06 RAC1
DN  192.168.2.103    91.11 KB     256      33.9%             d0844a21-3698-4883-ab66-9e2fd5150edd RAC1
UN  192.168.2.102    124.42 KB    256      32.6%             8d5ed9f4-7764-4dbd-bad8-43fddce94b7c RAC1
```

```
C:\> %CASSANDRA_HOME%\bin\nodetool removenode d0844a21-3698-4883-ab66-9e2fd5150edd
```

View the status of the operation to remove the node:

```
C:\> %CASSANDRA_HOME%\bin\nodetool removenode status
```

```
RemovalStatus: No token removals in process.
```

Confirm that the node has been removed.

```
C:\> %CASSANDRA_HOME%\bin\nodetool removenode status
```

```
Datacenter: DC1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address          Load          Tokens   Owns (effective)  Host ID
   Rack
UN  192.168.2.101    112.82 KB    256      37.7%             420129fc-0d84-42b0-be41-ef7dd3a8ad06 RAC1
UN  192.168.2.102    124.42 KB    256      38.3%             8d5ed9f4-7764-4dbd-bad8-43fddce94b7c RAC1
```

nodetool repair

Repairs one or more tables.

Synopsis

```
$ nodetool <options> repair <args> <--> <keyspace> <table> <.table>
<. . .> ;
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

args**-dc, or --in-dc, followed by *dc_name***

restrict repair to nodes in the named datacenter, which must be the local datacenter.

-dcpair, or --dc-parallel

repair data centers in parallel

-et, or --end-token followed by a token UUID

repair a range of nodes starting with the first token and ending with this token. Use -hosts to specify neighbor nodes.

-hosts *host_name* [, *host_name*] [. . .], or --in-hosts *host_name* [, *host_name*] [. . .]

repair specific hosts

-inc or --incremental

do an incremental repair.

-local or --in-local-dc

repair nodes only in the local datacenter.

-par or --parallel

perform repairs in parallel

-pr or --partitioner-range

repair only the first range returned by the partitioner

-st or --start-token followed by the UUID of a token

repair a range of nodes starting with this token

--

separates an option and argument that could be mistaken for a option

keyspace

the keyspace name. The default is `all`.

table

is a tablename or a space-delimited list of table names. If no tables are listed, the tool operates on all tables.

- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Performing an anti-entropy node repair on a [regular basis](#) is important, especially in an environment that deletes data frequently. The `repair` command repairs one or more nodes in a cluster, and provides options for restricting repair to a set of nodes. Anti-entropy node repair performs the following tasks:

- Ensures that all data on a replica is consistent.
- Repairs inconsistencies on a node that has been down.

By default, Cassandra 2.1 does a full, [sequential repair](#).

Using options

Use options to do these other types of repair:

- Use the `-hosts` option to list the good nodes to use for repairing the bad nodes. Use `-h` to name the bad nodes.
- Use the `-inc` option for an [incremental repair](#). An incremental repair persists already repaired SSTables and calculates the Merkle trees only for unrepaired SSTables. If you run repairs frequently, this repair process is more performant than the other types of repair even as datasets grow. Before doing an incremental repair for the first time, perform the [Incremental repair migration steps](#).
- Use the `-par` option for a parallel repair. Unlike [sequential repair](#), parallel repair constructs the Merkle trees for all nodes at the same time. Therefore, no snapshots are required (or generated). Use a parallel repair to complete the repair quickly or when you have operational downtime that allows the resources to be completely consumed during the repair.
- Use the `-pr` option to perform non-incremental [partitioner range repairs](#) across an entire cluster. Do not use this option for incremental repairs.

Examples

All `nodetool repair` arguments are optional. The following examples show the following types of repair:

```
# A full repair on a specific keyspace
$ nodetool repair <keyspace_name>

# An incremental, parallel repair of all keyspaces on the current node
$ nodetool repair -par -inc

# A partitioner range repair of the bad partition on current node using the
  good partitions on 10.2.2.20 or 10.2.2.21
$ nodetool repair -pr -hosts 10.2.2.20,10.2.2.21

# A start-point-to-end-point repair of all nodes between two nodes on the ring
$ nodetool repair -st a9fa31c7-f3c0-44d1-b8e7-a26228867840c -et f5bb146c-
db51-475ca44f-9facf2f1ad6e
```

To restrict the repair to the local data center, use the `-dc` option followed by the name of the datacenter. Issue the command from a node in the datacenter you specify in the command. If you issue the command from different datacenter, Cassandra returns an error. Do not use `-dc` and `-pr` together to repair only a local data center.

```
$ nodetool repair -dc DC1
```

```
[2014-07-24 21:59:55,326] Nothing to repair for keyspace 'system'
[2014-07-24 21:59:55,617] Starting repair command #2, repairing 490 ranges
  for keyspace system_traces (seq=true, full=true)
[2014-07-24 22:23:14,299] Repair session 323b9490-137e-11e4-88e3-
c972e09793ca
  for range (820981369067266915,822627736366088177] finished
[2014-07-24 22:23:14,320] Repair session 38496a61-137e-11e4-88e3-
c972e09793ca
  for range (2506042417712465541,2515941262699962473] finished
. . .
```

An inspection of the `system.log` shows repair taking place only on IP addresses in DC1.

```
. . . .
INFO [AntiEntropyStage:1] 2014-07-24 22:23:10,708 RepairSession.java:171
- [repair #16499ef0-1381-11e4-88e3-c972e09793ca] Received merkle tree
  for sessions from /192.168.2.101
INFO [RepairJobTask:1] 2014-07-24 22:23:10,740 RepairJob.java:145
- [repair #16499ef0-1381-11e4-88e3-c972e09793ca] requesting merkle trees
  for events (to [/192.168.2.103, /192.168.2.101])
. . . .
```

nodetool replaybatchlog

Replay batchlog and wait for finish.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> replaybatchlog
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

`nodetool replaybatchlog` is intended to force a batchlog replay. It also blocks until the batches have been replayed.

nodetool resetlocalschema

Reset the node's local schema and resynchronizes.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] resetlocalschema [args]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number

Short	Long	Description
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool resetlocalschema` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional
- The pipe (`|`) symbol means OR or AND/OR
- Ellipsis (`...`) means repeatable
- Orange (`and`) means not literal, indicates scope

Description

Normally, this command is used to rectify schema disagreements on different nodes. It can be useful if table schema changes have generated too many tombstones, on the order of 100,000s.

`nodetool resetlocalschema` drops the schema information of the local node and resynchronizes the schema from another node. To drop the schema, the tool truncates all the system schema tables. The node will temporarily lose metadata about the tables on the node, but will rewrite the information from another node. If the node is experiencing problems with too many tombstones, the truncation of the tables will eliminate the tombstones.

This command is useful when you have one node that is out of sync with the cluster. The system schema tables must have another node from which to fetch the tables. It is not useful when all or many of your nodes are in an incorrect state. If there is only one node in the cluster (replication factor of 1) – it does not perform the operation, because another node from which to fetch the tables does not exist. Run the command on the node experiencing difficulty.

nodetool resumehandoff

Resume hints delivery process.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> resumehandoff
```

options are:

- (`-h` | `--host`) `<host name>` | `<ip address>`
- (`-p` | `--port`) `<port number>`
- (`-pw` | `--password`) `<password>`
- (`-u` | `--username`) `<user name>`
- (`-pwf` `<passwordFilePath>` | `--password-file` `<passwordFilePath>`)
- Angle brackets (`< >`) mean not literal, a variable
- Italics mean optional

- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool ring

Provides node status and information about the ring.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> ring ( -r | --resolve-ip ) --
<keyspace>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -r, or --resolve-ip, means to provide node names instead of IP addresses.
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Displays node status and information about the ring as determined by the node being queried. This information can give you an idea of the load balance and if any nodes are down. If your cluster is not properly configured, different nodes may show a different ring. Check that the node appears the same way in the ring. If you use virtual nodes (vnodes), use `nodetool status` for succinct output.

- Address
The node's URL.
- DC (data center)
The data center containing the node.
- Rack
The rack or, in the case of Amazon EC2, the availability zone of the node.
- Status - Up or Down
Indicates whether the node is functioning or not.
- State - N (normal), L (leaving), J (joining), M (moving)
The state of the node in relation to the cluster.
- Load - updates every 90 seconds
The amount of file system data under the cassandra data directory after excluding all content in the snapshots subdirectories. Because all SSTable data files are included, any data that is not cleaned up, such as TTL-expired cell or tombstoned data) is counted.
- Token

The end of the token range up to and including the value listed. For an explanation of token ranges, see [Data Distribution in the Ring](#).

- Owns

The percentage of the data owned by the node per data center times the replication factor. For example, a node can own 33% of the ring, but show 100% if the replication factor is 3.

- Host ID

The network ID of the node.

nodetool scrub

Rebuild SSTables for one or more Cassandra tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> scrub <keyspace> -- ( -ns | --no-snapshot ) ( -s | --skip-corrupted ) ( <table> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.
- -ns, or --no-snapshot, triggers a snapshot of the scrubbed table first assuming snapshots are not disabled (the default).
- -s, or --skip-corrupted skips corrupted partitions even when scrubbing counter tables. (default false)
- table is one or more table names, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Rebuilds SSTables on a node for the named tables and snapshots data files before rebuilding as a safety measure. If possible use [nodetool upgradesstables](#). While scrub rebuilds SSTables, it also discards data that it deems broken and creates a snapshot, which you have to remove manually. If the -ns option is specified, snapshot creation is disabled. If scrub can't validate the column value against the column definition's data type, it logs the partition key and skips to the next partition. Skipping corrupted partitions in tables having counter columns results in under-counting. By default the scrub operation stops if you attempt to skip such a partition. To force the scrub to skip the partition and continue scrubbing, re-run `nodetool scrub` using the --skip-corrupted option.

nodetool setcachecapacity

Set global key and row cache capacities in megabytes.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setcachecapacity -- <key-cache-capacity> <row-cache-capacity>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- key-cache-capacity is the maximum size in MB of the key cache in memory.
- row-cache-capacity corresponds to the maximum size in MB of the row cache in memory.
- counter-cache-capacity corresponds to the maximum size in MB of the counter cache in memory.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The key-cache-capacity argument corresponds to the [key_cache_size_in_mb](#) parameter in the `cassandra.yaml`. Each key cache hit saves one seek and each row cache hit saves a minimum of two seeks. Devoting some memory to the key cache is usually a good tradeoff considering the positive effect on the response time. The default value is empty, which means a minimum of five percent of the heap in MB or 100 MB.

The row-cache-capacity argument corresponds to the [row_cache_size_in_mb](#) parameter in the `cassandra.yaml`. By default, row caching is zero (disabled).

The counter-cache-capacity argument corresponds to the [counter_cache_size_in_mb](#) in the `cassandra.yaml`. By default, counter caching is a minimum of 2.5% of Heap or 50MB.

nodetool setcachekeystosave

Sets the number of keys saved by each cache for faster post-restart warmup.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setcachekeystosave -- <key-cache-keys-to-save> <row-cache-keys-to-save>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- key-cache-keys-to-save is the number of keys from the key cache to save to the saved caches directory.

- row-cache-keys-to-save is the number of keys from the row cache to save to the saved caches directory.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This command saves the specified number of key and row caches to the saved caches directory, which you specify in the `cassandra.yaml`. The `key-cache-keys-to-save` argument corresponds to the `key_cache_keys_to_save` in the `cassandra.yaml`, which is disabled by default, meaning all keys will be saved. The `row-cache-keys-to-save` argument corresponds to the `row_cache_keys_to_save` in the `cassandra.yaml`, which is disabled by default.

nodetool setcompactionthreshold

Sets minimum and maximum compaction thresholds for a table.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setcompactionthreshold --  
<keyspace> <table> <minthreshold> <maxthreshold>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- keyspace is the name of a keyspace.
- table is a table name.
- minthreshold sets the minimum number of SSTables to trigger a minor compaction when using SizeTieredCompactionStrategy or DateTieredCompactionStrategy.
- maxthreshold sets the maximum number of SSTables to allow in a minor compaction when using SizeTieredCompactionStrategy or DateTieredCompactionStrategy.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

This parameter controls how many SSTables of a similar size must be present before a minor [compaction](#) is scheduled. The `max_threshold` table property sets an upper bound on the number of SSTables that may be compacted in a single minor compaction, as described in <http://wiki.apache.org/cassandra/MemtableSSTable>.

When using LeveledCompactionStrategy, maxthreshold sets the MAX_COMPACTING_L0, which limits the number of L0 SSTables that are compacted concurrently to avoid wasting memory or running out of memory when compacting highly overlapping SSTables.

nodetool setcompactionthroughput

Sets the throughput capacity for compaction in the system, or disables throttling.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setcompactionthroughput --
<value_in_mb>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- value_in_mb is the throughput capacity in MB per second for compaction.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Set value_in_mb to 0 to disable throttling.

nodetool sethintedhandoffthrottlekb

Sets hinted handoff throttle in kb/sec per delivery thread.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> sethintedhandoffthrottlekb
<value_in_kb/sec>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- value_in_kb/sec is the throttle time.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR

- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

When a node detects that a node for which it is holding hints has recovered, it begins sending the hints to that node. This setting specifies the maximum sleep interval per delivery thread in kilobytes per second after delivering each hint. The interval shrinks proportionally to the number of nodes in the cluster. For example, if there are two nodes in the cluster, each delivery thread uses the maximum interval; if there are three nodes, each node throttles to half of the maximum interval, because the two nodes are expected to deliver hints simultaneously.

Example

```
C:\> %CASSANDRA_HOME%\bin\nodetool sethintedhandoffthrottlekb 2048
```

nodetool setlogginglevel

Set the log level for a service.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setlogginglevel -- <
class_qualifier > < level >
```

options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password>
- (-u | --username) <user name>
- (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- class_qualifier is the logger class qualifier, a fully qualified domain name, such as org.apache.cassandra.service.StorageProxy.
- level is the logging level, for example DEBUG.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

You can use this command to set logging levels for services instead of modifying the logback-text.xml file. The following values are valid for the logger class qualifier:

- org.apache.cassandra
- org.apache.cassandra.db
- org.apache.cassandra.service.StorageProxy

The possible log levels are:

- ALL
- TRACE

- DEBUG
- INFO
- WARN
- ERROR
- OFF

If both class qualifier and level arguments to the command are empty or null, the command resets logging to the initial configuration.

Example

This command sets the StorageProxy service to debug level.

```
C:\> %CASSANDRA_HOME%\bin\nodetool setlogginglevel
org.apache.cassandra.service.StorageProxy DEBUG
```

Note: Cassandra 3.0 and later support extended logging for Compaction. This utility must be configured as part of the table configuration. The extended compaction logs are stored in a separate file. For details, see [Enabling extended compaction logging](#).

nodetool setstreamthroughput

Sets the throughput capacity in Mb (megabits) for streaming in the system, or disables throttling.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> setstreamthroughput --
<value_in_mb>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- -- separates an option and argument that could be mistaken for a option.
- value_in_mb is the throughput capacity in megabits per second for streaming.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Set value_in_mb to 0 to disable throttling.

nodetool settimeout

Set the specified timeout in ms, or 0 to disable timeout.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] settimeout [--] <timeout_type>
<timeout_in_ms>
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the cassandra-env.ps1 file for the host, then you must specify credentials.
- -- separates an option and argument that could be mistaken for a option.
- The timeout type:
 - read
 - range
 - write
 - counterwrite
 - cascontention
 - truncate
 - streamingsocket
 - misc, such as general rpc_timeout_in_ms

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool gettimeout` command sets the specified timeout in milliseconds. Use "0" to disable a timeout. Several timeouts are available.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra settimeout read
100
```

nodetool settraceprobability

Sets the probability for tracing a request.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> settraceprobability -- <value>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.
- value is a probability between 0 and 1.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Probabilistic tracing is useful to determine the cause of intermittent query performance problems by identifying which queries are responsible. This option traces some or all statements sent to a cluster. Tracing a request usually requires at least 10 rows to be inserted.

A probability of 1.0 will trace everything whereas lesser amounts (for example, 0.10) only sample a certain percentage of statements. Care should be taken on large and active systems, as system-wide tracing will have a performance impact. Unless you are under very light load, tracing all requests (probability 1.0) will probably overwhelm your system. Start with a small fraction, for example, 0.001 and increase only if necessary. The trace information is stored in a system_traces keyspace that holds two tables – sessions and events, which can be easily queried to answer questions, such as what the most time-consuming query has been since a trace was started. Query the parameters map and thread column in the system_traces.sessions and events tables for probabilistic tracing information.

To discover the current trace probability setting, use [nodetool gettraceprobability](#).

nodetool snapshot

Take a snapshot of one or more keyspaces, or of a table, to backup data.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> snapshot
( -cf <table> | --column-family <table> )
(-kc <ktlist> | --kc.list <ktlist> | -kt <ktlist> | --kt-list <ktlist>)
(-sf | --skip-flush)
(-t <tag> | --tag <tag> )
-- ( <keyspace> ) | ( <keyspace> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)

- -cf, or --column-family, followed by the name of the table to be backed up.
- -kc, --kc.list, -kt, or --kt-list, followed by a list of keyspace.table names to be back up, ktlist.
- -sf or --skip-flush, executes the snapshot without flushing the tables first (Cassandra 3.4 and later)
- -t or --tag, followed by the snapshot name.
- -- separates an option and argument that could be mistaken for a option.
- keyspace is a single keyspace name that is required when using the -cf option
- keyspace_list is one or more optional keyspace names, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Use this command to [back up data](#) using a snapshot. See the examples below for various options.

Cassandra [flushes](#) the node before taking a snapshot, takes the snapshot, and stores the data in the [snapshots directory](#) of each keyspace in the data directory. If you do not specify the name of a snapshot directory using the -t option, Cassandra names the directory using the timestamp of the snapshot, for example 1391460334889. Follow the procedure for [taking a snapshot](#) before upgrading Cassandra. When upgrading, backup all keyspaces. For more information about snapshots, see [Apache documentation](#).

Example: All keyspaces

Take a snapshot of all keyspaces on the node. On Linux, in the Cassandra bin directory, for example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool snapshot
```

The following message appears:

```
Requested creating snapshot(s) for [all keyspaces] with snapshot name
[1391464041163]
Snapshot directory: 1391464041163
```

Because you did not specify a snapshot name, Cassandra names snapshot directories using the timestamp of the snapshot. If the keyspace contains no data, empty directories are not created.

Example: Single keyspace snapshot

Assuming you created the keyspace cycling, took a snapshot of the keyspace and named the snapshot 2015.07.17.:

```
C:\> %CASSANDRA_HOME%\bin\nodetool snapshot -t 2015.07.17 cycling
```

The following output appears:

```
Requested creating snapshot(s) for [cycling] with snapshot name [2015.07.17]
Snapshot directory: 2015.07.17
```

Assuming the cycling keyspace contains two tables, cyclist_name and upcoming_calendar, taking a snapshot of the keyspace creates multiple snapshot directories named 2015.07.17. A number of .db files containing the data are located in these directories. For example, from the installation directory:

```
C:\> cd data\data\cycling\cyclist_name-
a882dca02aaf11e58c7b8b496c707234\snapshots\2015.07.17
```

```
C:\> dir
```

```
la-1-big-CompressionInfo.db  la-1-big-Index.db          la-1-big-TOC.txt
la-1-big-Data.db            la-1-big-Statistics.db     la-1-big-Digest.adler32
la-1-big-Filter.db          la-1-big-Summary.db        manifest.json
```

```
C:\> cd data\data\cycling\cyclist_name-a882dca02aaf11e58c7b8b496c707234/
snapshots/2015.07.17
c:\> dir
```

```
la-1-big-CompressionInfo.db  la-1-big-Index.db          la-1-big-TOC.txt
la-1-big-Data.db            la-1-big-Statistics.db     la-1-big-Digest.adler32
la-1-big-Filter.db          la-1-big-Summary.db        manifest.json
```

Example: Multiple keyspaces snapshot

Assuming you created a keyspace named mykeyspace in addition to the cycling keyspace, take a snapshot of both keyspaces.

```
C:\> %CASSANDRA_HOME%\bin\nodetool snapshot mykeyspace cycling
```

The following message appears:

```
Requested creating snapshot(s) for [mykeyspace, cycling] with snapshot name
[1391460334889]
Snapshot directory: 1391460334889
```

Example: Single table snapshot

Take a snapshot of only the cyclist_name table in the cycling keyspace.

```
C:\> %CASSANDRA_HOME%\bin\nodetool snapshot --table cyclist_name cycling
```

```
Requested creating snapshot(s) for [cycling] with snapshot name
[1391461910600]
Snapshot directory: 1391461910600
```

Cassandra creates the snapshot directory named 1391461910600 that contains the backup data of cyclist_name table in data/data/cycling/cyclist_name-a882dca02aaf11e58c7b8b496c707234/snapshots, for example.

Example: List of different keyspace.tables snapshot

Take a snapshot of several tables in different keyspaces, such as the cyclist_name table in the cycling keyspace and the sample_times table in the test keyspace. The keyspace.table list should be comma-delimited with no spaces.

```
C:\> %CASSANDRA_HOME%\bin\nodetool snapshot -kt
cycling.cyclist_name,test.sample_times
```

```
Requested creating snapshot(s) for [cycling.cyclist_name,test.sample_times]
with snapshot name [1431045288401]
Snapshot directory: 1431045288401
```

nodetool status

Provide information about the cluster, such as the state, load, and IDs.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> status ( -r | --resolve-ip ) -- <keyspace>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- r, or --resolve-ip, means to provide node names instead of IP addresses.
- separates an option and argument that could be mistaken for a option.
- keyspace is a keyspace name.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The status command provides the following information:

- Status - U (up) or D (down)
Indicates whether the node is functioning or not.
- State - N (normal), L (leaving), J (joining), M (moving)
The state of the node in relation to the cluster.
- Address
The node's URL.
- Load - updates every 90 seconds
The amount of file system data under the cassandra data directory after excluding all content in the snapshots subdirectories. Because all SSTable data files are included, any data that is not cleaned up, such as TTL-expired cell or tombstoned data) is counted.
- Tokens
The number of tokens set for the node.
- Owns
The percentage of the data owned by the node per data center times the replication factor. For example, a node can own 33% of the ring, but show 100% if the replication factor is 3.
Attention: If your cluster uses keyspaces having different replication strategies or replication factors, specify a keyspace when you run `nodetool status` to get meaningful ownership information.
- Host ID
The network ID of the node.
- Rack
The rack or, in the case of Amazon EC2, the availability zone of the node.

Example

This example shows the output from running `nodetool status`.

```
C:\> %CASSANDRA_HOME%\bin\nodetool status mykeyspace
```

```
Datacenter: datacenter1
```

```
=====
```

```
Status=Up/Down
```

```
|/ State=Normal/Leaving/Joining/Moving
```

```
-- Address      Load          Tokens   Owns    Host ID
```

```
  Rack
```

```
UN  127.0.0.1    47.66 KB      1         33.3%   aaalb7c1-6049-4a08-ad3e-3697a0e30e10
```

```
  rack1
```

```
UN  127.0.0.2    47.67 KB      1         33.3%   1848c369-4306-4874-afdf-5c1e95b8732e
```

```
  rack1
```

```
UN  127.0.0.3    47.67 KB      1         33.3%   49578bf1-728f-438d-b1c1-d8dd644b6f7f
```

```
  rack1
```

nodetool statusbackup

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> statusbackup
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password>
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath> | `--password-file` <passwordFilePath>)

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

A semicolon that terminates CQL statements is not included in the synopsis.

Description

Provides the status of backup.

nodetool statusbinary

Provide the status of native transport.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> statusbinary
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Provides the status of the binary protocol, also known as the native transport.

nodetool statusgossip

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> statusgossip
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Provides the status of gossip.

nodetool statushandoff

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> statushandoff
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Provides the status of hinted handoff.

nodetool statusthrift

Provide the status of the Thrift server.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> statusthrift
```

Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool stop

Stops the compaction process.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> stop -- <compaction_type>
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-id	--compaction-id	Compaction ID
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password

Short	Long	Description
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool stop` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.
- Valid compaction types: `COMPACTION`, `VALIDATION`, `CLEANUP`, `SCRUB`, `INDEX_BUILD`
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Stops all compaction operations from continuing to run. This command is typically used to stop a compaction that has a negative impact on the performance of a node. After the compaction stops, Cassandra continues with the remaining operations in the queue. Eventually, Cassandra restarts the compaction.

In Cassandra 2.2 and later, a single compaction operation can be stopped with the `-id` option. Run `nodetool compactionstats` to find the compaction ID.

nodetool stopdaemon

Stops the cassandra daemon.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> stopdaemon
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password >
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath> | `--password-file` <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool tablehistograms

Provides statistics about a table that could be used to plot a frequency function.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> tablehistograms --
      <keyspace>.<table>
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- separates an option from an argument that could be mistaken for a option.
- keyspace is the name of a keyspace.
- table is the name of a table.
- <keyspace>.<table> or <keyspace> <table> can be used to designate the table.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool tablehistograms` command provides statistics about a table, including read/write latency, partition size, column count, and number of SSTables. The report is incremental, not cumulative. It covers all operations since the last time `nodetool tablehistograms` was run in the current session. The use of the `metrics-core` library makes the output more informative and easier to understand.

Example

For example, to get statistics about the `libout` table in the `libdata` keyspace, use this command:

```
C:\> %CASSANDRA_HOME%\bin\nodetool.bat tablehistograms libdata libout
```

Output is:

libdata/libout histograms				
Percentile	SSTables	Write Latency	Read Latency	Partition Size
Cell Count		(micros)	(micros)	(bytes)
50%	0.00	39.50	36.00	1597
42				
75%	0.00	49.00	55.00	1597
42				
95%	0.00	95.00	82.00	8239
258				
98%	0.00	126.84	110.42	17084
446				
99%	0.00	155.13	123.71	24601
770				
Min	0.00	3.00	3.00	1110
36				
Max	0.00	50772.00	314.00	126934
3973				

The output shows the percentile rank of read and write latency values, the partition size, and the cell count for the table.

nodetool tablestats

Provides statistics about tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> tablestats -i
-- (<keyspace>.<table> ... ) -H
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Additional options:

- `--` separates an option from an argument that could be mistaken for a option.
- `-i` excludes the following list of tables from the tool's report. `tablestat` reports on all other tables in all other keyspaces.
- `table` specifies the table that the tool reports on. Use `keyspace` and a dot to specify the table's keyspace. to get stats on two or more tables, add more names (with optional keyspace names) separated by spaces.

If you run the command with no table names, `nodetool tablestats` reports on all tables in all keyspaces.

- `-H` converts bytes to a human readable form: kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB).
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool tablestats` command provides statistics about one or more tables. Cassandra uses the [metrics-core](#) library to make the output more informative and easier to understand.

This table lists the components of the `nodetool tablestats` output for a single table.

Table: nodetool tablestats output

Name of statistic	Example value	Brief description	Related information
Keyspace	libdata	Name of the keyspace	Keyspace and table
Table	libout	Name of this table	

Name of statistic	Example value	Brief description	Related information
SSTable count	3	Number of SSTables containing data for this table	How to use the SSTable counts metric
Space used (live)	9592399	Total number of bytes of disk space used by all active SSTables belonging to this table	Storing data on disk in SSTables
Space used (total)	9592399	Total number of bytes of disk space used by SSTables belonging to this table, including obsolete SSTables waiting to be GCd	Same as above.
Space used by snapshots (total):	0	Total number of bytes of disk space used by snapshot of this table's data	About snapshots on page 120
Off heap memory used (total)		Total number of bytes of off heap memory used for memtables, Bloom filters, index summaries and compression metadata for this table	
SSTable Compression Ratio	0.367. . .	Ratio of size of compressed SSTable data to its uncompressed size	Types of compression options.
Number of keys (estimate)	3	The number of partition keys for this table	Not the number of primary keys. This gives you the estimated number of partitions in the table.
Memtable cell count	1022550	Number of cells (storage engine rows x columns) of data in the memtable for this table	Cassandra memtable structure in memory
Memtable data size	32028148	Total number of bytes in the memtable for this table	Total amount of live data stored in the memtable, excluding any data structure overhead.
Memtable off heap memory used	0	Total number of bytes of off-heap data for this memtable, including column related overhead and partitions overwritten	The maximum amount is set in cassandra.yaml by the property memtable_offheap_space_in_mb .
Memtable switch count	3	Number of times a full memtable for this table was swapped for an empty one	Increases each time the memtable for a table is flushed to disk. See How memtables are measured article.
Local read count	11207	Number of requests to read tables in the keyspace since startup	

Name of statistic	Example value	Brief description	Related information
Local read latency	0.048 ms	Round trip time in milliseconds to complete the most recent request to read the table	Factors that affect read latency
Local write count	17598	Number of local requests to update the table since startup	
Local write latency	0.054 ms	Round trip time in milliseconds to complete an update to the table	Factors that affect write latency
Pending flushes	0	Estimated number of reads, writes, and cluster operations pending for this table	Important: Monitor this metric to watch for blocked or overloaded memtable flush writers. The nodetool tpstats tool does not report on blocked flushwriters.
Bloom filter false positives	0	Number of false positives reported by this table's Bloom filter	Tuning bloom filters
Bloom filter false ratio	0.00000	Fraction of all bloom filter checks resulting in a false positive from the most recent read	
Bloom filter space used, bytes	11688	Size in bytes of the bloom filter data for this table	
Bloom filter off heap memory used	8	The number of bytes of off heap memory used for Bloom filters for this table	
Index summary off heap memory used	41	The number of bytes of off heap memory used for index summaries for this table	
Compression metadata off heap memory used	8	The number of bytes of off heap memory used for compression offset maps for this table	
Compacted partition minimum	1110	Size in bytes of the smallest compacted partition for this table	
Compacted partition maximum bytes	126934	Size in bytes of the largest compacted partition for this table	
Compacted partition mean bytes	2730	The average size of compacted partitions for this table	

Name of statistic	Example value	Brief description	Related information
Average live cells per slice (last five minutes)	0.0	Average number of cells scanned by single key queries during the last five minutes	
Maximum live cells per slice (last five minutes)	0.0	Maximum number of cells scanned by single key queries during the last five minutes	
Average tombstones per slice (last five minutes)	0.0	Average number of tombstones scanned by single key queries during the last five minutes	
Maximum tombstones per slice (last five minutes)	0.0	Maximum number of tombstones scanned by single key queries during the last five minutes	
Dropped mutations	0.0	The number of mutations (INSERTs, UPDATEs or DELETEs) started on this table but not completed	A high number of dropped mutations can indicate an overloaded node.

Examples

An excerpt of the output of the command reporting on a library data table just flushed to disk.

```
C:\> %CASSANDRA_HOME%\bin\nodetool tablestats libdata.libout
Keyspace: libdata
Read Count: 11207
Read Latency: 0.047931114482020164 ms.
Write Count: 17598
Write Latency: 0.053502954881236506 ms.
Pending Flushes: 0
Table: libout
SSTable count: 3
Space used (live): 9088955
Space used (total): 9088955
Space used by snapshots (total): 0
Off heap memory used (total): 57
SSTable Compression Ratio: 0.8823529411764706
Number of keys (estimate): 3
Memtable cell count: 0
Memtable data size: 0
Memtable off heap memory used: 0
Memtable switch count: 3
Local read count: 11207
Local read latency: 0.048 ms
Local write count: 17598
Local write latency: 0.054 ms
Pending flushes: 0
Bloom filter false positives: 0
Bloom filter false ratio: 0.00000
Bloom filter space used: 11688
Bloom filter off heap memory used: 8
Index summary off heap memory used: 41
```

```

Compression metadata off heap memory used: 8
Compacted partition minimum bytes: 1110
Compacted partition maximum bytes: 126934
Compacted partition mean bytes: 2730
    Average live cells per slice (last five minutes): 0.0
Maximum live cells per slice (last five minutes): 0
Average tombstones per slice (last five minutes): 0.0
Maximum tombstones per slice (last five minutes): 0
Dropped Mutations: 0

```

Using the human-readable option

Use the human-readable `-H` option to get output in easier-to-read units. For example:

```

C:\> %CASSANDRA_HOME%\bin\nodetool tablestats cycling.calendar -H
Keyspace: cycling
Read Count: 0
Read Latency: NaN ms.
Write Count: 0
Write Latency: NaN ms.
Pending Flushes: 0
Table: calendar
SSTable count: 1
Space used (live): 13.75 MB
Space used (total): 13.75 MB
Space used by snapshots (total): 0 bytes
Off heap memory used (total): 32 bytes
SSTable Compression Ratio: 0.7606837606837606
Number of keys (estimate): 4
Memtable cell count: 0
Memtable data size: 0 bytes
Memtable off heap memory used: 0 bytes
Memtable switch count: 0
Local read count: 0
Local read latency: NaN ms
Local write count: 20050
Local write latency: 0.085 ms
Pending flushes: 0
Bloom filter false positives: 0
Bloom filter false ratio: 0.00000
Bloom filter space used: 16 bytes
Bloom filter off heap memory used: 8 bytes
Index summary off heap memory used: 16 bytes
Compression metadata off heap memory used: 8 bytes
Compacted partition minimum bytes: 1.87 KB
Compacted partition maximum bytes: 2.69 KB
Compacted partition mean bytes: 2.26 KB
Average live cells per slice (last five minutes): 0.0
Maximum live cells per slice (last five minutes): 0.0
Average tombstones per slice (last five minutes): 0.0
Maximum tombstones per slice (last five minutes): 0.0
Dropped Mutations: 0 bytes

```

nodetool toppartitions

Synopsis

```

C:\> %CASSANDRA_HOME%\bin\nodetool <options> toppartitions <keyspace> <table>
<duration> ...

```

- Options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password >
- (-u | --username) <user name>
- (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -a <samplers> comma separated list of samplers to use (default: all)
- -k <topCount> number of the top partitions to list (default: 10)
- -s <size> capacity of stream summary, closer to the actual cardinality of partitions will yield more accurate results (default: 256)
- keyspace is a keyspace name
- cfname is a column family name
- duration in milliseconds

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool toppartitions` command samples and prints the most active partitions during the duration specified. A keyspace and column family must be specified, as well as a duration in milliseconds.

Examples

Sample the most active partitions for the table `test.users` for 1,000 milliseconds

```
nodetool toppartitions test users 1000
```

Output is produced, similar to the following:


```

READS Sampler:
  Cardinality: ~0 (256 capacity)
  Top 10 partitions:
    Nothing recorded during sampling period...

WRITES Sampler:
  Cardinality: ~1 (256 capacity)
  Top 10 partitions:
    Partition      Count      +/-
    10             1          0
    11             1          0
    12             1          0
    13             1          0
    14             1          0
    15             1          0
    16             1          0
    17             1          0
    18             1          0
    19             1          0

```

nodetool tpstats

Provides usage statistics of thread pools.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> tpstats
```

options are:

- (-h | --host) <host name> | <ip address>
- (-p | --port) <port number>
- (-pw | --password) <password>
- (-u | --username) <user name>
- (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Cassandra is based on a Staged Event Driven Architecture (SEDA). Cassandra separates different tasks into stages connected by a messaging service. Each stage has a queue and a thread pool. although some

stages skip the messaging service and queue tasks immediately on a different stage if it exists on the same node. Cassandra can back up a queue if the next stage is too busy. This can lead to a performance bottlenecks.

The `nodetool tpstats` command reports on each stage of Cassandra operations by thread pool. For each thread pool, the command returns the number of Active, Pending and Completed tasks, the number of currently blocked tasks, and the total number of blocked tasks. A high number of pending tasks for any pool can indicate performance problems, as described in <http://wiki.apache.org/cassandra/Operations#Monitoring>.

Run the `nodetool tpstats` command on a local node for get thread pool statistics.

Run `nodetool tpstats` with appropriate options to check the thread pool statistics for a remote node. For setup instructions, see [Secure JMX Authentication](#).

nodetool tpstats pool names and tasks

This table describes the Cassandra task or property associated with each pool name reported in the `nodetool tpstats` output:

Pool Name	Associated tasks	Related information
AntiEntropyStage	Processing repair messages and streaming	For details, see Nodetool repair .
CacheCleanupExecutor	Clearing the cache	
CommitlogArchiver	Copying or archiving commitlog files for recovery	
CompactionExecutor	Running compaction	
CounterMutationStage	Processing local counter changes	Will back up if the write rate exceeds the mutation rate. A high pending count will be seen if consistency level is set to ONE and there is a high counter increment workload.
GossipStage	Distributing node information via Gossip	Out of sync schemas can cause issues. You may have to sync using <code>nodetool resetlocalschema</code> .
HintedHandoff	Sending missed mutations to other nodes	Usually symptom of a problem elsewhere. Use <code>nodetool disablehandoff</code> and run <code>repair</code> .
InternalResponseStage	Responding to non-client initiated messages, including bootstrapping and schema checking	
MemtableFlushWriter	Writing memtable contents to disk	May back up if the queue is overruns the disk I/O, or because of sorting processes. Warning: <code>nodetool tpstats</code> no longer reports blocked threads in the MemtableFlushWriter pool. Check the Pending Flushes metric reported by <code>nodetool tblestats</code> .

Pool Name	Associated tasks	Related information
MemtablePostFlushStage	Cleaning up after flushing the memtable (discarding commit logs and secondary indexes as needed)	
MemtableReclaimingStage	Making unused memory available	
MigrationStage	Processing schema changes	
MiscStage	Snapshotting, replicating data after node remove completed.	
MutationStage	Performing local inserts/updates, schema merges, commit log replays or hints in progress	A high number of Pending write requests indicates the node is having a problem handling them. Fix this by adding a node, tuning hardware and configuration, and/or updating data models.
Native-Transport-Requests	Processing CQL requests to the server	
PendingRangeCalculatorStage	Calculating pending ranges per bootstraps and departed nodes	Reporting by this tool is not useful — see Developer notes
ReadRepairStage	Performing read repairs	Usually fast, if there is good connectivity between replicas. If Pending grows too large, attempt to lower the rate for high-read tables by altering the table to use a smaller read_repair_chance value, like 0.11.
ReadStage	Performing local reads	Also includes deserializing data from row cache. Pending values can cause increased read latency. Generally resolved by adding nodes or tuning the system.
RequestResponseHandlingStage	Handling responses from other nodes	
ValidationExecutor	Validating schema	

nodetool tpstats droppable messages

Cassandra generates the messages listed below, but discards them after a timeout. The `nodetool tpstats` command reports the number of messages of each type that have been dropped. You can view the messages themselves using a JMX client.

Message Type	Stage	Notes
BINARY	n/a	Deprecated
_TRACE	n/a (special)	Used for recording traces (nodetool settraceprobability) Has a special executor (1 thread, 1000 queue depth) that throws

Message Type	Stage	Notes
		away messages on insertion instead of within the execute
MUTATION	MutationStage	If a write message is processed after its timeout (write_request_timeout_in_ms) it either sent a failure to the client or it met its requested consistency level and will relay on hinted handoff and read repairs to do the mutation if it succeeded.
COUNTER_MUTATION	MutationStage	If a write message is processed after its timeout (write_request_timeout_in_ms) it either sent a failure to the client or it met its requested consistency level and will relay on hinted handoff and read repairs to do the mutation if it succeeded.
READ_REPAIR	MutationStage	Times out after write_request_timeout_in_ms
READ	ReadStage	Times out after read_request_timeout_in_ms. No point in servicing reads after that point since it would of returned error to client
RANGE_SLICE	ReadStage	Times out after range_request_timeout_in_ms.
PAGED_RANGE	ReadStage	Times out after request_timeout_in_ms.
REQUEST_RESPONSE	RequestResponseStage	Times out after request_timeout_in_ms. Response was completed and sent back but not before the timeout

Example

Running `nodetool tpstats` on the host `labcluster`:

```
C:\> %CASSANDRA_HOME%\bin\nodetool -h labcluster tpstats
```

Example output is:

Pool Name	Active	Pending	Completed	Blocked	All
time blocked					
CounterMutationStage	0	0	0	0	
0					
ReadStage	0	0	103	0	
0					
RequestResponseStage	0	0	0	0	
0					

MutationStage	0	0	13234794	0
0				
ReadRepairStage	0	0	0	0
0				
GossipStage	0	0	0	0
0				
CacheCleanupExecutor	0	0	0	0
0				
AntiEntropyStage	0	0	0	0
0				
MigrationStage	0	0	11	0
0				
ValidationExecutor	0	0	0	0
0				
CommitLogArchiver	0	0	0	0
0				
MiscStage	0	0	0	0
0				
MemtableFlushWriter	0	0	126	0
0				
MemtableReclaimMemory	0	0	126	0
0				
PendingRangeCalculator	0	0	1	0
0				
MemtablePostFlush	0	0	1468	0
0				
CompactionExecutor	0	0	254	0
0				
InternalResponseStage	0	0	1	0
0				
HintedHandoff	0	0	0	
Message type	Dropped			
RANGE_SLICE	0			
READ_REPAIR	0			
PAGED_RANGE	0			
BINARY	0			
READ	0			
MUTATION	180			
_TRACE	0			
REQUEST_RESPONSE	0			
COUNTER_MUTATION	0			

nodetool truncatehints

Truncates all hints on the local node, or truncates hints for the one or more endpoints.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options>
truncatehints -- ( <endpoint> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath> | --password-file <passwordFilePath>)
- separates an option and argument that could be mistaken for a option.

- endpoint is one or more endpoint IP addresses or host names which hints are to be deleted.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

nodetool upgradesstables

Rewrites SSTables for tables that are not running the current version of Cassandra.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> upgradesstables
( -a | --include-all-sstables )
-- <keyspace> ( <table> ... )
```

- Options are:
 - (-h | --host) <host name> | <ip address>
 - (-p | --port) <port number>
 - (-pw | --password) <password >
 - (-u | --username) <user name>
 - (-pwf <passwordFilePath | --password-file <passwordFilePath>)
- -a or --include-all-sstables, followed by the snapshot name.
- -- separates an option and argument that could be mistaken for a option.
- keyspace a keyspace name.
- table is one or more table names, separated by a space.
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

Rewrites SSTables on a node that are incompatible with the current version. Use this command when upgrading your server or changing compression options.

nodetool verify

Verify (check data checksum for) one or more tables.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool [options] verify [(-e | --extended-verify)]
[--] [<keyspace> <tables>...]
```

Table: Options

Short	Long	Description
-h	--host	Hostname or IP address

Short	Long	Description
-p	--port	Port number
-pwf	--password-file	Password file path
-pw	--password	Password
-u	--username	User name

Note:

- If a username and password for RMI authentication are set explicitly in the `cassandra-env.ps1` file for the host, then you must specify credentials.
- `nodetool verify` operates on a single node in the cluster if `-h` is not used to identify one or more other nodes. If the node from which you issue the command is the intended target, you do not need the `-h` option to identify the target; otherwise, for remote invocation, identify the target node, or nodes, using `-h`.

In the synopsis section of each statement, formatting has the following meaning:

- Uppercase means literal
- Lowercase means not literal
- Italics mean optional
- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

Description

The `nodetool verify` command checks the data checksum for one or more specified tables. An optional argument, `-e` or `--extended-verify`, will verify each cell data, whereas without the option, only the SSTable checksums are verified.

Examples

```
C:\> %CASSANDRA_HOME%\bin\nodetool -u cassandra -pw cassandra verify cycling
cyclist_name
```

nodetool version

Provides the version number of Cassandra running on the specified node.

Synopsis

```
C:\> %CASSANDRA_HOME%\bin\nodetool <options> version
```

Options are:

- (`-h` | `--host`) <host name> | <ip address>
- (`-p` | `--port`) <port number>
- (`-pw` | `--password`) <password >
- (`-u` | `--username`) <user name>
- (`-pwf` <passwordFilePath> | `--password-file` <passwordFilePath>)
- Angle brackets (< >) mean not literal, a variable
- Italics mean optional

- The pipe (|) symbol means OR or AND/OR
- Ellipsis (...) means repeatable
- Orange (and) means not literal, indicates scope

The cassandra utility

You can run Cassandra 3.2 and later with start-up parameters by adding them to the `jvm.options` file or entering them at the command prompt.

Note: If you are using Cassandra 3.1, see the [Cassandra 3.0 documentation](#).

You can also add options such as maximum and minimum heap size to the `jvm.options` file to pass them to the Java virtual machine at startup, rather than setting them in the environment.

Usage

Add a parameter to the `jvm.options` file as follows:

```
$env:JVM_OPTS="$env:JVM_OPTS -D[PARAMETER]"
```

Example:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.load_ring_state=false"
```

The [Example section](#) contains more examples.

Command line only options

Option	Description
-f	Start the cassandra process in foreground. The default is to start as background process.
-h	Help.
-p <i>filename</i>	Log the process ID in the named file. Useful for stopping Cassandra by killing its PID.
-v	Print the version and exit.

Start-up parameters

The `-D` option specifies start-up parameters at the command line and in the `cassandra-env.ps1` file.

cassandra.auto_bootstrap=false

Sets [auto_bootstrap](#) to `false` on initial set-up of the cluster. The next time you start the cluster, you do not need to change the `cassandra.yaml` file on each node to revert to `true`.

cassandra.available_processors=number_of_processors

In a multi-instance deployment, each Cassandra instance independently assumes that all CPU processors are available to it. Use this setting to specify a smaller set of processors.

cassandra.boot_without_jna=true

Configures Cassandra to boot without JNA. If you do not set this parameter to `true`, and JNA does not initialize, Cassandra does not boot.

cassandra.config=directory

Sets the directory location of the `cassandra.yaml` file. The default location depends on the type of installation.

`cassandra.initial_token=token`

Use when Cassandra is not using virtual nodes (vnodes). Sets the initial partitioner token for a node the first time the node is started. (Default: disabled)

Note: Vnodes automatically select tokens.

`cassandra.join_ring=true/false`

When set to `false`, prevents the Cassandra node from joining a ring on startup. (Default: `true`) You can add the node to the ring afterwards using [nodetool join](#) and a JMX call.

`cassandra.load_ring_state=true/false`

When set to `false`, clears all gossip state for the node on restart. (Default: `true`)

`cassandra.metricsReporterConfigFile=file`

Enables pluggable metrics reporter. See [Pluggable metrics reporting in Cassandra 2.0.2](#).

`cassandra.native_transport_port=port`

Sets the port on which the CQL native transport listens for clients. (Default: 9042)

`cassandra.partitioner=partitioner`

Sets the partitioner. (Default: `org.apache.cassandra.dht.Murmur3Partitioner`)

`cassandra.replace_address=listen_address or broadcast_address of dead node`

To replace a node that has died, restart a new node in its place specifying the [listen_address](#) or [broadcast_address](#) that the new node is assuming. The new node must be in the same state as before bootstrapping, without any data in its data directory.

Note: The `broadcast_address` defaults to the `listen_address` except when the ring is using the [Ec2MultiRegionSnitch](#).

`cassandra.replayList=table`

Allows restoring specific tables from an archived commit log.

`cassandra.ring_delay_ms=ms`

Defines the amount of time a node waits to hear from other nodes before formally joining the ring. (Default: 1000ms)

`cassandra.rpc_port=port`

Sets the port for the Thrift RPC service, which is used for client connections. (Default: 9160).

`cassandra.ssl_storage_port=port`

Sets the SSL port for encrypted communication. (Default: 7001)

`cassandra.start_native_transport=true | false`

Enables or disables the native transport server. See [start_native_transport](#) in `cassandra.yaml`. (Default: `true`)

`cassandra.start_rpc=true | false`

Enables or disables the Thrift RPC server. (Default: `true`)

`cassandra.storage_port=port`

Sets the port for inter-node communication. (Default: 7000)

`cassandra.triggers_dir=directory`

Sets the default location for the triggers JARs.

`cassandra.write_survey=true`

Enables a tool for testing new compaction and compression strategies. `write_survey` allows you to experiment with different strategies and benchmark write performance differences without affecting the production workload. See [Testing compaction and compression](#) on page 147.

`consistent.rangemovement=true`

Set to `true`, makes bootstrapping behavior effective.

Example

Clearing gossip state when starting a node:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.load_ring_state=false"
```

Example

Starting a Cassandra node without joining the ring:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.join_ring=false"
```

Example

Replacing a dead node:

```
$env:JVM_OPTS="$env:JVM_OPTS -Dcassandra.replace_address=10.91.176.160"
```

The cassandra-stress tool

The `cassandra-stress` tool is a Java-based stress testing utility for basic benchmarking and load testing a Cassandra cluster.

Data modeling choices can greatly affect application performance. Significant load testing over several trials is the best method for discovering issues with a particular data model. The `cassandra-stress` tool is an effective tool for populating a cluster and stress testing CQL tables and queries. Use `cassandra-stress` to:

- Quickly determine how a schema performs.
- Understand how your database scales.
- Optimize your data model and settings.
- Determine production capacity.

The `cassandra-stress` tool also supports a YAML-based profile for defining specific schemas with various compaction strategies, cache settings, and types. Sample files are located in `Program Files\DataStax-DDC\apache-cassandra\tools`. The YAML file supports user-defined keyspace, tables, and schema. The YAML file can be used to design tests of reads, writes, and mixed workloads.

When started without a YAML file, `cassandra-stress` creates a keyspace, `keyspace1`, and tables, `standard1` or `counter1`, depending on what type of table is being tested. These elements are automatically created the first time you run a stress test and reused on subsequent runs. You can drop `keyspace1` using [DROP KEYSPACE](#). You cannot change the default keyspace and tables names without [using a YAML file](#).

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> cassandra-stress command [options]
```

`cassandra-stress options`

Command	Description
counter_read	Multiple concurrent reads of counters. The cluster must first be populated by a counter_write test.
counter_write	Multiple concurrent updates of counters.
help	Display help: <code>cassandra-stress help</code> Display help for an option: <code>cassandra-stress help [options]</code> For example: <code>cassandra-stress help -schema</code>
legacy	Legacy support mode.
mixed	Interleave basic commands with configurable ratio and distribution. The cluster must first be populated by a write test.
print	Inspect the output of a distribution definition.
read	Multiple concurrent reads. The cluster must first be populated by a write test.
user	Interleave user provided queries with configurable ratio and distribution.
write	Multiple concurrent writes against the cluster.

Important: Additional sub-options are available for each option in the following table. To get more detailed information on any of these, enter:

```
C:\> cassandra-stress help option
```

When entering the `help` command, be sure to precede the option name with a hyphen, as shown.

Cassandra-stress sub-options

Sub-option	Description
-col	Column details, such as size and count distribution, data generator, names, and comparator. Usage: <pre>-col names=? [slice] [super=?] [comparator=?] [timestamp=?] [size=DIST(?)] or -col [n=DIST(?)] [slice] [super=?] [comparator=?] [timestamp=?] [size=DIST(?)]</pre>
-errors	How to handle errors when encountered during stress testing. Usage: <pre>-errors [retries=?] [ignore]</pre>
-graph	Graph results of cassandra-stress tests. Multiple tests can be graphed together. Usage: <pre>-graph file=? [revision=?] [title=?] [op=?]</pre>
-insert	Insert specific options relating to various methods for batching and splitting partition updates. Usage:

Sub-option	Description
	<pre>-insert [revisit=DIST(?)] [visits=DIST(?)] partitions=DIST(?) [batchtype=?] select-ratio=DIST(?) row-population-ratio=DIST(?)</pre>
- log	<p>Where to log progress and the interval to use.</p> <p>Usage:</p> <pre>-log [level=?] [no-summary] [file=?] [interval=?]</pre>
- mode	<p>Thrift or CQL with options.</p> <p>Usage:</p> <pre>-mode thrift [smart] [user=?] [password=?] or -mode native [unprepared] cql3 [compression=?] [port=?] [user=?] [password=?] [auth-provider=?] [maxPending=?] [connectionsPerHost=?] or -mode simplenative [prepared] cql3 [port=?]</pre>
- node	<p>Nodes to connect to.</p> <p>Usage:</p> <pre>-node [whitelist] [file=?]</pre>
- pop	<p>Population distribution and intra-partition visit order.</p> <p>Usage:</p> <pre>-pop seq=? [no-wrap] [read-lookback=DIST(?)] [contents=?] or -pop [dist=DIST(?)] [contents=?]</pre>
- port	<p>Specify port for connecting Cassandra nodes. Port can be specified for Cassandra native protocol, Thrift protocol or a JMX port for retrieving statistics.</p> <p>Usage:</p> <pre>-port [native=?] [thrift=?] [jmx=?]</pre>
- rate	<p>Thread count, rate limit, or automatic mode (default is auto).</p> <p>Usage:</p> <pre>-rate threads=? [limit=?] or -rate [threads>=?] [threads<=?] [auto]</pre>
- sample	<p>Specify the number of samples to collect for measuring latency.</p> <p>Usage:</p> <pre>-sample [history=?] [live=?] [report=?]</pre>
- schema	<p>Replication settings, compression, compaction, and so on.</p> <p>Usage:</p>

Sub-option	Description
	<code>-schema [replication(?)] [keyspace=?] [compaction(?)] [compression=?]</code>
<code>-sendto</code>	Specify a stress server to send this command to. Usage: <code>-sendToDaemon <host></code>
<code>-transport</code>	Custom transport factories. Usage: <code>-transport [factory=?] [truststore=?] [truststore-password=?] [ssl-protocol=?] [ssl-alg=?] [store-type=?] [ssl-ciphers=?]</code>

Additional command-line parameters can modify how `cassandra-stress` runs:

Additional `cassandra-stress` parameters

Command	Description
<code>cl=?</code>	Set the consistency level to use during <code>cassandra-stress</code> . Options are ONE, QUORUM, LOCAL_QUORUM, EACH_QUORUM, ALL, and ANY. Default is LOCAL_ONE.
<code>clustering=DIS</code>	Distribution clustering runs of operations of the same kind.
<code>duration=?</code>	Specify the time to run, in seconds, minutes or hours.
<code>err<=?</code>	Specify a standard error of the mean; when this value is reached, <code>cassandra-stress</code> will end. Default is 0.02.
<code>n>=?</code>	Specify a minimum number of iterations to run before accepting uncertainly convergence.
<code>n<=?</code>	Specify a maximum number of iterations to run before accepting uncertainly convergence.
<code>n=?</code>	Specify the number of operations to run.
<code>no-warmup</code>	Do not warmup the process, do a cold start.
<code>ops(?)</code>	Specify what operations to run and the number of each. (only with the user option)
<code>profile=?</code>	Designate the YAML file to use with <code>cassandra-stress</code> . (only with the user option)
<code>truncate=?</code>	Truncate the table created during <code>cassandra-stress</code> . Options are never, once, or always. Default is never.

Simple read and write examples

```
# Insert (write) one million rows
C:\> cassandra-stress write n=1000000 -rate threads=50

# Read two hundred thousand rows.
C:\> cassandra-stress read n=200000 -rate threads=50

# Read rows for a duration of 3 minutes.
C:\> cassandra-stress read duration=3m -rate threads=50

# Read 200,000 rows without a warmup of 50,000 rows first.
```

```
C:\> cassandra-stress read n=200000 no-warmup -rate threads=50
```

View schema help

```
C:\> cassandra-stress help -schema
```

```
replication([strategy=?][factor=?][<option 1..N>=?]):          Define
  the replication strategy and any parameters
  strategy=? (default=org.apache.cassandra.locator.SimpleStrategy) The
  replication strategy to use
  factor=? (default=1)                                         The
  number of replicas
  keyspace=? (default=keyspace1)                               The
  keyspace name to use
compaction([strategy=?][<option 1..N>=?]):                    Define
  the compaction strategy and any parameters
  strategy=?                                                  The
  compaction strategy to use
compression=?
  Specify the compression to use for SSTable, default:no compression
```

Populate the database

Generally it is easier to let `cassandra-stress` create the basic schema and then modify it in [CQL](#):

```
#Load one row with default schema
C:\> cassandra-stress write n=1 cl=one -mode native cql3 -log
      file=create_schema.log

#Modify schema in CQL
C:\> cqlsh

#Run a real write workload
C:\> cassandra-stress write n=1000000 cl=one -mode native cql3 -schema
      keyspace="keyspace1" -log file=load_1M_rows.log
```

Change the replication strategy

Changes the replication strategy to `NetworkTopologyStrategy` and targets one node named `existing`.

```
C:\> cassandra-stress write n=500000 no-warmup -node existing -schema
      "replication(strategy=NetworkTopologyStrategy, existing=2)"
```

Run a mixed workload

When running a mixed workload, you must escape parentheses, greater-than and less-than signs, and other such things. This example invokes a workload that is one-quarter writes and three-quarters reads.

```
C:\> cassandra-stress mixed ratio="(write=1,read=3)" n=100000 cl=ONE
      -pop dist=UNIFORM"(1..1000000)" -schema keyspace="keyspace1" -mode
      native cql3 -rate threads">="16 threads"<="256 -log file=%HOMEPATH
      %\mixed_autorate_50r50w_1M.log
```

Notice the following in this example:

1. The `ratio` parameter requires quotes.

2. The value of `n` used in the read phase is different from the value used in write phase. During the write phase, `n` records are written. However in the read phase, if `n` is too large, it is inconvenient to read *all* the records for simple testing. Generally, `n` does not need be large when validating the persistent storage systems of a cluster.

The `-pop dist=UNIFORM"(1..1000000)"` portion says that of the `n=100,000` operations, select the keys uniformly distributed between 1 and 1,000,000. Use this when you want to specify more data per node than what fits in DRAM.

3. In the `rate` section, the greater-than and less-than signs are quoted. If not escaped, the shell attempts to use them for IO redirection: the shell tries to read from a non-existent file called `=256` and create a file called `=16`. The `rate` section tells `cassandra-stress` to automatically attempt different numbers of client threads and not test less than 16 or more than 256 client threads.

Standard mixed read/write workload keyspace for a single node

```
CREATE KEYSPACE "keyspace1" WITH replication = {
  'class': 'SimpleStrategy',
  'replication_factor': '1'
};
USE "keyspace1";
CREATE TABLE "standard1" (
  key blob,
  "C0" blob,
  "C1" blob,
  "C2" blob,
  "C3" blob,
  "C4" blob,
  PRIMARY KEY (key)
) WITH
  bloom_filter_fp_chance=0.010000 AND
  caching='KEYS_ONLY' AND
  comment='' AND
  dclocal_read_repair_chance=0.000000 AND
  gc_grace_seconds=864000 AND
  index_interval=128 AND
  read_repair_chance=0.100000 AND
  replicate_on_write='true' AND
  default_time_to_live=0 AND
  speculative_retry='99.0PERCENTILE' AND
  memtable_flush_period_in_ms=0 AND
  compaction={'class': 'SizeTieredCompactionStrategy'} AND
  compression={'class': 'LZ4Compressor'};
```

Split up a load over multiple cassandra-stress instances on different nodes

This example demonstrates loading into large clusters, where a single `cassandra-stress` load generator node cannot saturate the cluster. In this example, `$NODES` is a variable whose value is a comma delimited list of IP addresses such as 10.0.0.1, 10.0.0.2, and so on.

```
#On Node1
```

```
C:\> cassandra-stress write n=1000000 cl=one -mode native cql3 -schema
  keyspace="keyspace1" -pop seq=1..1000000 -log file=%HOMEPATH%\node1_load.log
  -node $NODES
```

```
#On Node2
```

```
C:\> cassandra-stress write n=1000000 cl=one -mode native cql3 -schema
keyspace="keyspace1" -pop seq=1000001..2000000 -log file=%HOMEPATH
%\node2_load.log -node $NODES
```

Run cassandra-stress with authentication

The following example shows using the `-mode` option to supply a username and password:

```
C:\> cassandra-stress -mode native cql3 user=cassandra password=cassandra no-
warmup cl=QUORUM
```

Note: Check the documentation of the [transport](#) option for SSL authentication.

Run cassandra-stress using the truncate option

This option must be inserted before the mode option, otherwise the cassandra-stress tool won't apply truncation as specified.

The following example shows the `truncate` command:

```
C:\>cassandra-stress write n=100000000 cl=QUORUM truncate=always -schema
keyspace=keyspace-rate threads=200 -log file=write_$NOW.log
```

Use a YAML file to run cassandra-stress

This example uses a YAML file named `cqlstress-example.yaml`, which contains the keyspace and table definitions, and a query definition. The keyspace name and definition are the first entries in the YAML file:

```
keyspace: perftesting

keyspace_definition:

    CREATE KEYSPACE perftesting WITH replication = { 'class':
'SimpleStrategy', 'replication_factor': 3};
```

The table name and definition are created in the next section using CQL:

```
table: users

table_definition:

    CREATE TABLE users (
        username text,
        first_name text,
        last_name text,
        password text,
        email text,
        last_access timeuuid,
        PRIMARY KEY(username)
    );
```

In the `extra_definitions` section you can add secondary indexes or materialized views to the table:

```
extra_definitions:
```



```
- CREATE MATERIALIZED VIEW perftesting.users_by_first_name AS SELECT *
FROM perftesting.users WHERE first_name IS NOT NULL and username IS NOT
NULL PRIMARY KEY (first_name, username);
- CREATE MATERIALIZED VIEW perftesting.users_by_first_name2 AS SELECT *
FROM perftesting.users WHERE first_name IS NOT NULL and username IS NOT
NULL PRIMARY KEY (first_name, username);
- CREATE MATERIALIZED VIEW perftesting.users_by_first_name3 AS SELECT *
FROM perftesting.users WHERE first_name IS NOT NULL and username IS NOT
NULL PRIMARY KEY (first_name, username);
```

The population distribution can be defined for any column in the table. This section specifies a uniform distribution between 10 and 30 characters for `username` values in generated rows, that the values in the generated rows will create, a uniform distribution between 20 and 40 characters for generated `startdate` over the entire Cassandra cluster, and a Gaussian distribution between 100 and 500 characters for `description` values.

```
columnspec:
- name: username
  size: uniform(10..30)
- name: first_name
  size: fixed(16)
- name: last_name
  size: uniform(1..32)
- name: password
  size: fixed(80) # sha-512
- name: email
  size: uniform(16..50)
- name: startdate
  cluster: uniform(20...40)
- name: description
  size: gaussian(100...500)
```

After the column specifications, you can add specifications for how each batch runs. In the following code, the `partitions` value directs the test to use the column definitions above to insert a fixed number of rows in the partition in each batch:

```
insert:
  partitions: fixed(10)
  batchtype: UNLOGGED
```

The last section contains a query, `read1`, that can be run against the defined table.

```
queries:
  read1:
    cql: select * from users where username = ? and startdate = ?
    fields: samerow # samerow or multirow (select arguments from the
    same row, or randomly from all rows in the partition)
```

The following example shows using the `user` option and its parameters to run `cassandra-stress` tests from `cqlstress-example.yaml`:

```
C:\> cassandra-stress user profile=C:\Program Files\DataStax-DDC\apache-
cassandra\tools\cqlstress-example.yaml" n=1000000 ops"(insert=3,read1=1)" no-
warmup cl=QUORUM
```

Notice that:

- The `user` option is required for the `profile` and `opt` parameters.
- The value for the `profile` parameter is the path and filename of the `.yaml` file.
- In this example, `-n` specifies the number of *batches* that run.

- The values supplied for `ops` specifies which operations run and how many of each. These values direct the command to `insert` rows into the database and run the `read1` query.

How many times? Each insert or query counts as one batch, and the values in `ops` determine how many of each type are run. Since the total number of batches is 1,000,000, and `ops` says to run three inserts for each query, the result will be 750,000 inserts and 250,000 of the `read1` query.

Use escaping quotes when specifying the `ops` value.

For more information, see [Improved Cassandra 2.1 Stress Tool: Benchmark Any Schema – Part 1](#).

Use the -graph option

In Cassandra 3.2 and later, the `-graph` option provides visual feedback for `cassandra-stress` tests. This option requires:

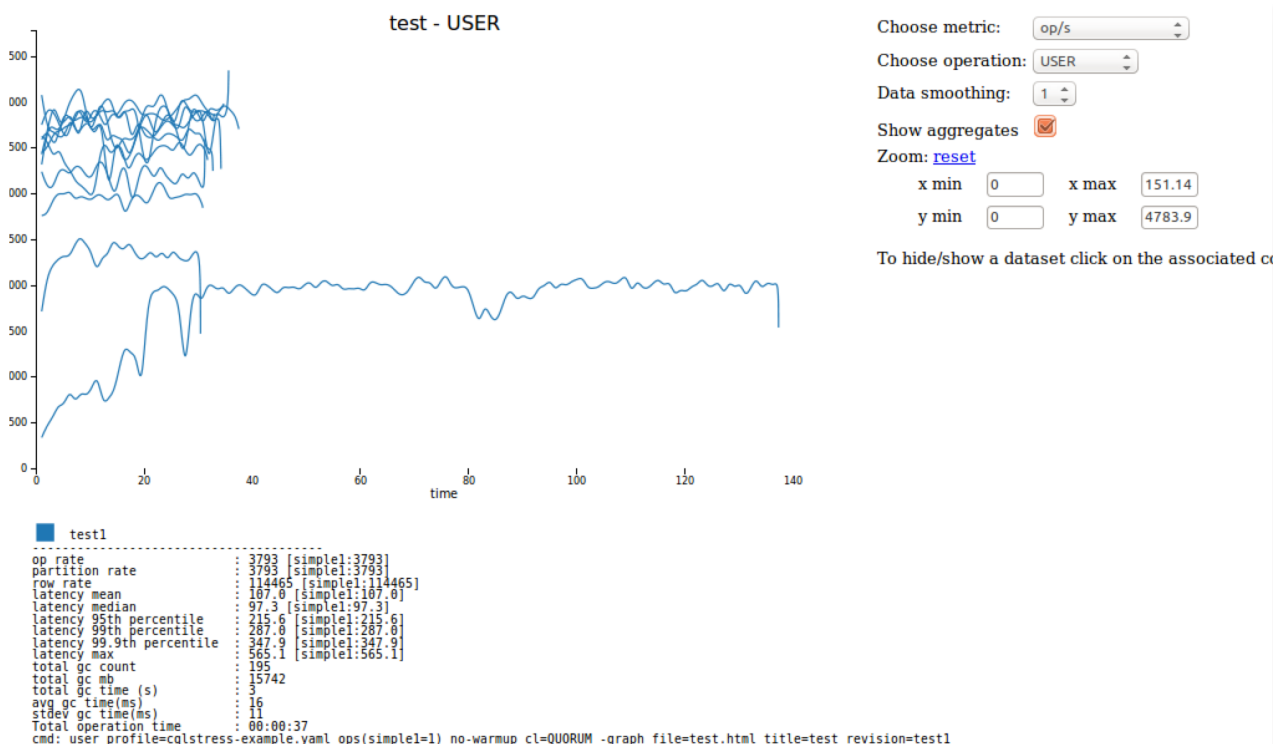
- A filename for the HTML file it builds (the value of the `file` parameter)
- A value for the `revision` parameter, if you graph multiple stress tests on the same output

The `title` and `op` parameters are optional.

Example:

```
C:\> cassandra-stress user profile=tools\cqlstress-example.yaml ops"(insert=1"
-graph file=test.html title=test revision=test1
```

This command generates interactive graph in a web browser tab or window:



Interpreting the output of cassandra-stress

Each line reports data for the interval between the last elapsed time and current elapsed time.

```
Created keyspaces. Sleeping 1s for propagation.
Sleeping 2s...
```

```

Warming up WRITE with 50000 iterations...
Running WRITE with 200 threads for 1000000 iteration
type      total ops,    op/s,    pk/s,    row/s,    mean,    med,
.95,      .99,      .999,      max,    time,    stderr, errors, gc: #, max ms,
sum ms,  sdv ms,    mb
total,      43148,    42991,    42991,    42991,    4.6,    1.5,
10.9, 106.1, 239.3, 255.4, 1.0, 0.00000, 0, 1, 49,
49, 0, 612
total,      98715,    43857,    43857,    43857,    4.6,    1.7,
8.5, 98.6, 204.6, 264.5, 2.3, 0.00705, 0, 1, 45,
45, 0, 619
total,      157777,    47283,    47283,    47283,    4.1,    1.4,
8.3, 70.6, 251.7, 286.3, 3.5, 0.02393, 0, 1, 59,
59, 0, 611

Results:
op rate           : 46751 [WRITE:46751]
partition rate    : 46751 [WRITE:46751]
row rate          : 46751 [WRITE:46751]
latency mean      : 4.3 [WRITE:4.3]
latency median    : 1.3 [WRITE:1.3]
latency 95th percentile : 7.2 [WRITE:7.2]
latency 99th percentile : 60.5 [WRITE:60.5]
latency 99.9th percentile : 223.2 [WRITE:223.2]
latency max       : 503.1 [WRITE:503.1]
Total partitions  : 1000000 [WRITE:1000000]
Total errors      : 0 [WRITE:0]
total gc count    : 18
total gc mb       : 10742
total gc time (s) : 1
avg gc time(ms)   : 73
stdev gc time(ms) : 16
Total operation time : 00:00:21

END

```

Table: Output of cassandra-stress

Data	Description
total ops	Running total number of operations during the run.
op/s	Number of operations per second performed during the run.
pk/s	Number of partition operations per second performed during the run.
row/s	Number of row operations per second performed during the run.
mean	Average latency in milliseconds for each operation during that run.
med	Median latency in milliseconds for each operation during that run.
.95	95% of the time the latency was less than the number displayed in the column.
.99	99% of the time the latency was less than the number displayed in the column.
.999	99.9% of the time the latency was less than the number displayed in the column.
max	Maximum latency in milliseconds.
time	Total operation time.

Data	Description
<code>stderr</code>	Standard error of the mean. It is a measure of confidence in the average throughput number; the smaller the number, the more accurate the measure of the cluster's performance.
<code>gc: #</code>	Number of garbage collections.
<code>max ms</code>	Longest garbage collection in milliseconds.
<code>sum ms</code>	Total of garbage collection in milliseconds.
<code>sdv ms</code>	Standard deviation in milliseconds.
<code>mb</code>	Size of the garbage collection in megabytes.

SSTable utilities

sstabledump

This tool outputs the contents of the specified SSTable in the JSON format.

Depending on your tasks, you may wish to flush the table to disk (using [nodetool flush](#)) before dumping its contents.

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstabledump [options] sstable_file
```

The file is located in the `data` directory and has a `.db` extension.

Table: Options

Flag	Description
<code>-d</code>	Outputs an internal representation, one CQL row per line.
<code>-e</code>	Limits output to the list of keys.
<code>-k key</code>	Limits output to information about the row

Flag	Description
	identified by the specified key.
-xkey	Excludes information about the row identified by the specified key from output.

sstableexpiredblockers

During compaction, Cassandra can drop entire SSTables if they contain only expired tombstones and if it is guaranteed to not cover any data in other SSTables. This diagnostic tool outputs all SSTables that are blocking other SSTables from being dropped.

Usage:

```
C:\> cd %CASSANDRA_HOME%
C:\> sstableexpiredblockers [--dry-run] keyspace table
```

Procedure

Choose a keyspace and table to check for any SSTables that are blocking the specified table from dropping.

```
C:\> %CASSANDRA_HOME%\tools\bin\sstableexpiredblockers cycling cyclist_name
```

What to do next

sstablekeys

The sstablekeys utility dumps table keys.

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstablekeys sstable_name
```

Procedure

1. If data has not been previously flushed to disk, manually flush it. For example:

```
C:\> %CASSANDRA_HOME%\bin\nodetool flush cycling cyclist_name
```

2. To list the keys in an SSTable, find the name of the SSTable file.

The file is located in the `data` directory and has a `.db` extension.

3. Look at keys in the SSTable data. For example, use `sstablekeys` followed by the path to the data. Use the path to data for your Cassandra installation:

```
C:\> sstablekeys %CASSANDRA_HOME%\data\data\cycling\cyclist_name-
a882dca02aaf11e58c7b8b496c707234\1a-1-big-Data.db
```

The output appears, for example:

```
e7ae5cf3-d358-4d99-b900-85902fda9bb0
5b6962dd-3f90-4c93-8f61-eabfa4a803e2
220844bf-4860-49d6-9a4b-6b5d3a79cbfb
6ab09bec-e68e-48d9-a5f8-97e6fb4c9b47
e7cd5752-bc0d-4157-a80f-7523add8dbcd
```

sstablelevelreset

Reset level to 0 on a given set of SSTables that use `LeveledCompactionStrategy`.

Usage:

```
C:\> cd %CASSANDRA_HOME%
C:\> sstablelevelreset [--really-reset] keyspace table
```

The option `--really-reset` is a warning that Cassandra is stopped before the tool is run.

Procedure

- Stop Cassandra on the node. Choose a keyspace and table to reset to level 0.

```
C:\> %CASSANDRA_HOME%\tools\bin\sstablelevelreset --really-reset cycling
cyclist_name
```

If the designated table is already at level 0, then no change occurs. If the SSTable is leveled, the metadata is rewritten to designate the level to 0.

Example

sstableloader (Cassandra bulk loader)

The Cassandra bulk loader, also called the `sstableloader`, provides the ability to:

- Bulk load external data into a cluster.
- Load existing SSTables into another cluster with a different number of nodes or replication strategy.
- Restore snapshots.

The `sstableloader` streams a set of SSTable data files to a live cluster. It does not simply copy the set of SSTables to every node, but transfers the relevant part of the data to each node, conforming to the replication strategy of the cluster. The table into which the data is loaded does not need to be empty.

Run `sstableloader` from the directory containing the SSTables, passing it the location of the target cluster.

Note: Bulkloading SSTables created in versions prior to Cassandra 3.0 is supported only in Cassandra 3.0.5 and later.

Note: Repairing tables that have been loaded into a different cluster does not repair the source tables.

Prerequisites

The source data loaded by `sstableloader` must be in SSTables.

Generating SSTables

When using `sstableloader` to load external data, you must first put the external data into SSTables.

Note: If using DataStax Enterprise, you can use [Sqoop](#) to migrate external data to Cassandra.

SSTableWriter is the API to create raw Cassandra data files locally for bulk load into your cluster. The Cassandra source code includes the `CQLSSTableWriter` implementation for creating SSTable files from external data without needing to understand the details of how those map to the underlying storage engine. Import the `org.apache.cassandra.io.sstable.CQLSSTableWriter` class, and define the schema for the data you want to import, a writer for the schema, and a prepared insert statement. For a complete example, see <http://www.datastax.com/dev/blog/using-the-cassandra-bulk-loader-updated>.

Restoring Cassandra snapshots

For information about preparing snapshots for `sstableloader` import, see [Restoring from centralized backups](#).

Importing SSTables from an existing cluster

Before importing existing SSTables, run [nodetool flush](#) on each source node to assure that any data in memtables is written out to the SSTables on disk.

Preparing the target environment

Before loading the data, you must define the schema of the target tables with [CQL](#) or Thrift.

Usage

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\bin"
C:\> sstableloader -d host_url (,host_url ...) [options] path_to_keyspace
```

The `sstableloader` bulk loads the SSTables found in the keyspace directory to the configured target cluster, where the parent directories of the directory path are used as the target keyspace/table name.

For more `sstableloader` options, see [sstableloader options](#)

Using sstableloader

1. If restoring snapshot data from some other source: make sure that the snapshot files are in a `keyspace/tablename` directory path whose names match those of the target `keyspace/tablename`. In this example, make sure the snapshot files are in `.`
2. Go to the location of the SSTables:

```
C:\> cd "Program Files\DataStax-DDC\data\data\Keyspace1\Standard1\"
```

3. To view the contents of the keyspace:

```
C:\> dir

Keyspace1-Standard1-jb-60-CRC.db
Keyspace1-Standard1-jb-60-Data.db
...
```

Keyspace1-Standard1-jb-60-TOC.txt

4. To bulk load the files, specify the path to `Keyspace1/Standard1/` in the target cluster:

```
C:\> sstableloader -d 110.82.155.1 "Program Files\DataStax-DDC\data\data
\Keyspace1\Standard1\"
```

This command bulk loads all files.

Note: To get the best throughput from SSTable loading, you can use multiple instances of `sstableloader` to stream across multiple machines. No hard limit exists on the number of SSTables that `sstableloader` can run at the same time, so you can add additional loaders until you see no further improvement.

Table: sstableloader options

Short option	Long option	Description
-alg	--ssl-alg <ALGORITHM>	Client SSL algorithm (default: SunX509).
-ap	--auth-provider <auth provider class name>	Allows the use of a third party auth provider. Can be combined with -u <username> and -pw <password> if the auth provider supports plain text credentials.
-ciphers	--ssl-ciphers <CIPHER-SUITES>	Client SSL. Comma-separated list of encryption suites.
-cph	--connections-per-host <connectionsPerHost>	Number of concurrent connections-per-host.
-d	--nodes <initial_hosts>	Required. Connect to a list of (comma separated) hosts for initial cluster information.
-f	--conf-path <path_to_config_file>	Path to the <code>cassandra.yaml</code> path for streaming throughput and client/server SSL.
-h	--help	Display help.
-i	--ignore <NODES>	Do not stream to this comma separated list of nodes.
-ks	--keystore <KEYSTORE>	Client SSL. Full path to the keystore.
-kspw	--keystore-password <KEYSTORE-PASSWORD>	Client SSL. Password for the keystore. Overrides the <code>client_encryption_options</code> option in cassandra.yaml
	--no-progress	Do not display progress.
-p	--port <rpc port>	RPC port (default: 9160 [Thrift]).
-prctl	--ssl-protocol <PROTOCOL>	Client SSL. Connections protocol to use (default: TLS). Overrides the <code>server_encryption_options</code> option in cassandra.yaml
-pw	--password <password>	Password for Cassandra authentication.
-st	--store-type <STORE-TYPE>	Client SSL. Type of store.
-t	--throttle <throttle>	Throttle speed in Mbits (default: unlimited). Overrides the <code>stream_throughput_outbound_megabits_per_sec</code> option in cassandra.yaml

Short option	Long option	Description
-tf	--transport-factory <transport factory>	Fully-qualified <code>ITransportFactory</code> class name for creating a connection to Cassandra.
-ts	--truststore <TRUSTSTORE>	Client SSL. Full path to truststore.
-tspw	--truststore-password <TRUSTSTORE-PASSWORD>	Client SSL. Password of the truststore.
-u	--username <username>	User name for Cassandra authentication.
-v	--verbose	Verbose output.

sstablemetadata

The `sstablemetadata` utility prints metadata about a specified `SSTable`, including:

- sstable name
- partitioner
- RepairedAt timestamp (for [incremental repairs](#) only)
- sstable level (for [Leveled Compaction](#) only)
- number of tombstones and Dropped timestamps (in epoch time)
- number of cells and size (in bytes) per row

Use this report to troubleshoot wide rows or performance-degrading tombstones.

Procedure

1. Switch to the `CASSANDRA_HOME` directory.
2. Enter the command `\tools\bin\sstablemetadata` followed by the filenames of one or more `SSTables`.

```
$ tools\bin\sstablemetadata <sstable_name filenames>
```

```
tools\bin\sstablemetadata data\data\autogeneratedtest
\transaction_by_retailer-f27e4d5078dc11e59d629d03f52e8a2b\ma-203-big-Data.db
SSTable: data\data\autogeneratedtest\transaction_by_retailer-
f27e4d5078dc11e59d629d03f52e8a2b\ma-203-big
Partitioner: org.apache.cassandra.dht.Murmur3Partitioner
Bloom Filter FP chance: 0.010000
Minimum timestamp: 1445871871053006
Maximum timestamp: 1445871953354005
SSTable max local deletion time: 2147483647
Compression ratio: -1.0
Estimated droppable tombstones: 0.0
SSTable Level: 0
Repaired at: 0
ReplayPosition(segmentId=1445871179392, position=18397674)
Estimated tombstone drop times:
2147483647: 7816721
Count          Row Size          Cell Count
1                0                0
2                0                0
3                0                0
4                0                0
5                0                0
```

6	0	0
7	0	0
8	0	0
10	0	0
12	0	710611
14	0	0
17	0	0
20	0	0
24	0	0
29	0	0
35	0	0
42	0	0
50	0	0
60	0	0
72	0	0
86	0	0
103	0	0
124	0	0
149	0	0
179	0	0
215	0	0
258	0	0
310	81	0
372	710530	0
446	0	0
535	0	0
642	0	0
770	0	0
924	0	0
1109	0	0
1331	0	0
1597	0	0
1916	0	0
2299	0	0
2759	0	0
3311	0	0
3973	0	0
4768	0	0
5722	0	0
6866	0	0
8239	0	0
9887	0	0
11864	0	0
14237	0	0
17084	0	0
20501	0	0
24601	0	0
29521	0	0
35425	0	0
42510	0	0
51012	0	0
61214	0	0
73457	0	0
88148	0	0
105778	0	0
126934	0	0
152321	0	0
182785	0	0
219342	0	0
263210	0	0
315852	0	0
379022	0	0
454826	0	0
545791	0	0

654949	0	0
785939	0	0
943127	0	0
1131752	0	0
1358102	0	0
1629722	0	0
1955666	0	0
2346799	0	0
2816159	0	0
3379391	0	0
4055269	0	0
4866323	0	0
5839588	0	0
7007506	0	0
8409007	0	0
10090808	0	0
12108970	0	0
14530764	0	0
17436917	0	0
20924300	0	0
25109160	0	0
30130992	0	0
36157190	0	0
43388628	0	0
52066354	0	0
62479625	0	0
74975550	0	0
89970660	0	0
107964792	0	0
129557750	0	0
155469300	0	0
186563160	0	0
223875792	0	0
268650950	0	0
322381140	0	0
386857368	0	0
464228842	0	0
557074610	0	0
668489532	0	0
802187438	0	0
962624926	0	0
1155149911	0	0
1386179893	0	0
1663415872	0	0
1996099046	0	0
2395318855	0	0
2874382626	0	
3449259151	0	
4139110981	0	
4966933177	0	
5960319812	0	
7152383774	0	
8582860529	0	
10299432635	0	
12359319162	0	
14831182994	0	
17797419593	0	
21356903512	0	
25628284214	0	
30753941057	0	
36904729268	0	
44285675122	0	
53142810146	0	
63771372175	0	

```

76525646610      0
91830775932      0
110196931118     0
132236317342     0
158683580810     0
190420296972     0
228504356366     0
274205227639     0
329046273167     0
394855527800     0
473826633360     0
568591960032     0
682310352038     0
818772422446     0
982526906935     0
1179032288322    0
1414838745986    0
Estimated cardinality: 722835

```

sstableofflinerelevel

This tool is intended to run in an offline fashion. When using the `LevelledCompactionStrategy`, it is possible for the number of SSTables in level L0 to become excessively large, resulting in read latency degrading. This is often the case when atypical write load is experienced (eg. bulk import of data, node bootstrapping). This tool will relevel the SSTables in an optimal fashion. The `--dry-run` flag can be used to run in test mode and examine the tools results.

Usage:

```

C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstableofflinerelevel [--dry-run] keyspace table

```

Procedure

Choose a keyspace and table to relevel.

```
C:\> %CASSANDRA_HOME%\tools\bin\sstableofflinerelevel cycling cyclist_name
```

sstablerepairedset

This tool is intended to mark specific SSTables as repaired or unrepaired. It is used to set the `repairedAt` status on a given set of SSTables. This metadata facilitates incremental repairs. It can take in the path to an individual sstable or the path to a file containing a list of SSTables paths.

Warning: Do not run this command until you have stopped Cassandra on the node.

Use this tool in the process of migrating a Cassandra installation to incremental repair. For details, see [Migrating to incremental repairs](#) on page 132

Usage:

- Package installations: `$ sstablerepairedset [--is-repaired | --is-unrepaired] [-f sstable-list | sstables]`
- Tarball installations:

```

$ cd install_location/tools
$ bin/sstablerepairedset [--is-repaired | --is-unrepaired] [-f sstable-list
| sstables]

```

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstablerepairedset [--is-repaired | --is-unrepaired] [-f sstable-list
| sstables]
```

Procedure

-
- Choose SSTables to mark as repaired.

```
C:\>sstablerepairedset --is-repaired data\data\cycling\cyclist_name-
a882dca02aaf11e58c7b8b496c707234\la-1-big-Data.db
```

- Use a file to list the SSTable to mark as unrepaired.

```
C:\> sstablerepairedset --is-unrepaired repairSetSSTables.txt
```

A file like `repairSetSSTables.txt` would contain a list of SSTable (.db) files, as in the following example:

```
\data\data\cycling\cyclist_by_country-82246fc065ff11e5a4c58b496c707234\ma-1-
big-Data.db
\data\data\cycling
\cyclist_by_birthday-8248246065ff11e5a4c58b496c707234\ma-1-big-Data.db
\data\data\cycling
\cyclist_by_birthday-8248246065ff11e5a4c58b496c707234\ma-2-big-Data.db
\data\data\cycling\cyclist_by_age-8201305065ff11e5a4c58b496c707234\ma-1-big-
Data.db
\data\data\cycling\cyclist_by_age-8201305065ff11e5a4c58b496c707234\ma-2-big-
Data.db
```

Use the following command to list all the Data .db files in a keyspace:

```
dir /s /q C:\Program Files\Datastax-ddc\data\data\keyspace1\*.db
```

sstablescrib

The `sstablescrib` utility is an offline version of [nodetool scrub](#). It attempts to remove the corrupted parts while preserving non-corrupted data. Because `sstablescrib` runs offline, it can correct errors that `nodetool scrub` cannot. If an SSTable cannot be read due to corruption, it will be left on disk.

If scrubbing results in dropping rows, new SSTables become unrepaired. However, if no bad rows are detected, the SSTable keeps its original `repairedAt` field, which denotes the time of the repair.

Procedure

1. Before using `sstablescrib`, try rebuilding the tables using `nodetool scrub`.

If `nodetool scrub` does not fix the problem, use this utility.

2. [Shut down the node](#).
3. Run the utility:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstablescrib [options] keyspace table
```

Table: Options

Flag	Option	Description
	--debug	Display stack traces.
-h	--help	Display help.
-m	--manifest-check	Only check and repair the leveled manifest, without actually scrubbing the SSTables.
-s	--skip-corrupted	Skip corrupt rows in counter tables.
-v	--verbose	Verbose output.

sstablesplit

Use this tool to split SSTables files into multiple SSTables of a maximum designated size. For example, if SizeTieredCompactionStrategy was used for a major compaction and results in a excessively large SSTable, it's a good idea to split the table because won't get compacted again until the next huge compaction.

Cassandra must be stopped to use this tool:

```
C:\> net stop DataStax-DDC_Server
```

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
```

```
C:\> sstablesplit [options] <filename> [<filename>]*
```

```
C:\> Program Files\DataStax-DDC\apache-cassandra\tools\bin\sstablesplit
[options] <filename> [<filename>]*
```

Example:

```
C:\> sstablesplit -s 40 "Program Files\DataStax-DDC\data\data
\Keyspace1\Standard1\*"
```

Table: Options

Flag	Option	Description
	--debug	Display stack traces.
-h	--help	Display help.
	--no-snapshot	Do not snapshot the SSTables before splitting.
-s	--size <size>	Maximum size in MB for the output SSTables (default: 50).
-v	--verbose	Verbose output.

sstableupgrade

This tool rewrites the SSTables in the specified table to match the currently installed version of Cassandra.

If restoring with [sstableloader](#), you must upgrade your snapshots before restoring for any snapshot taken in a major version older than the major version that Cassandra is currently running.

Troubleshooting

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\tools\bin"
C:\> sstableupgrade [options] keyspace table [snapshot]
```

The snapshot option only upgrades the specified snapshot.

Table: Options

Flag	Option	Description
	--debug	Display stack traces.
-h	--help	Display help.

sstableutil

The sstableutil will list the SSTable files for a provided table.

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\bin"
C:\> sstableutil [--cleanup | --debug | --help | --opslog | --type <arg> | --
verbose] keyspace | table
```

Note: Arguments for --type option are: all, tmp, or final.

Procedure

Choose a table for which to list SSTables files.

```
C:\> %CASSANDRA_HOME%\bin\sstableutil --all cycling cyclist_name
```

sstableverify

The sstableverify utility will verify the SSTable for a provided table and look for errors or data corruption.

Usage:

```
C:\> cd "Program Files\DataStax-DDC\apache-cassandra\bin"
C:\> sstableverify [--debug | --extended | --help | --verbose] keyspace
| table
```

Procedure

Choose a table to verify.

```
C:\> %CASSANDRA_HOME%\bin\sstableverify --verbose cycling cyclist_name
```

Troubleshooting

Troubleshooting has moved to [Troubleshooting for both Cassandra and DataStax Enterprise](#).

DataStax Distribution of Apache Cassandra 3.x for Windows release notes

Note: Cassandra is now releasing on a tick-tock schedule. For more information, see [Cassandra 2.2, 3.0, and beyond](#).

The latest version of DataStax Distribution of Apache Cassandra 3.x for Windows is 3.6.

The [CHANGES.txt](#) describes the changes in detail. You can view all version changes by branch or tag in the drop-down list on the changes page.

New features, improvements, and notable changes are described in [What's new?](#).