

WHAT IS CLAIMED IS:

1. A method, comprising:

performing, by one or more computing devices:

5 determining, for a particular data stream comprising a plurality of data records, a set of nodes configurable by one or more control components to perform stream management operations based on one or more policies including a stream partitioning policy;

10 providing data records in response to record retrieval requests received via one or more programmatic record retrieval interfaces, wherein the one or more programmatic record retrieval interfaces include a first retrieval interface enabling a non-sequential access pattern and a second retrieval interface enabling a sequential access pattern, and wherein a billing rate associated with a use of the first retrieval interface differs from a billing rate associated with a use of the second retrieval interface; and

15 generating a client billing amount associated with the particular data stream based at least in part on respective usage count metrics of the plurality of record retrieval interfaces.

20 2. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

25 assigning, in accordance with the partitioning policy, a particular data record of the particular data stream to a first partition of the particular data stream, based at least in part on a key associated with the particular data record, wherein the key is indicated by a write request corresponding to the particular data record.

3. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

30 selecting, based at least in part on a partition to which a particular data record is assigned, one or more of (a) a particular node of a record ingestion subsystem responsible for accepting the particular data record, (b) a particular node of a record storage subsystem responsible for storing at least one copy of the particular data record, and (c) a particular node of a retrieval subsystem responsible for obtaining the

particular data record from the record storage subsystem in response to a read request.

4. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

receiving data records submitted via one or more programmatic record submission interfaces, wherein the one or more programmatic record submission interfaces include a first submission interface supporting in-line submission of data records and a second submission interface enabling submission of data records by reference to one of: (a) an object address at a storage service implemented by a provider network (b) a universal record locator (c) a database record.

5. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

removing, from a particular node of a data storage subsystem, a particular data record based at least in part on one of: (a) a data de-duplication window configured for the particular data stream, (b) a data archival policy associated with the particular data stream, (c) a data retention policy indicated by a client, (d) a client request to remove the particular data record, or (e) an indication that the particular data record has been processed by one or more data consumers.

6. The method as recited in claim 1, wherein at least one subsystem of: (a) a record ingestion subsystem, (b) a record storage subsystem, or (c) a record retrieval subsystem configured for the particular data stream comprises a plurality of nodes configured by the one or more control components as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records of the stream and (b) one or more non-primary nodes configured to assume a primary role in response to one or more triggering events.

7. The method as recited in claim 6, wherein a particular primary node of the one or more primary nodes is instantiated at a particular data center, and wherein a particular non-primary node of the one or more non-primary nodes is instantiated at a different data center.

8. The method as recited in claim 6, further comprising performing, by the one or more computing devices:

detecting a triggering event of the one or more triggering events; and

notifying a particular non-primary node of the one or more non-primary nodes to assume the primary role.

9. The method as recited in claim 1, wherein the one or more control components comprise a plurality of control nodes configured as a redundancy group, comprising a primary control node configured to respond to requests for control-plane operations on one or more data streams including the particular data stream, and at least one non-primary control node configured to assume a primary role in response to one or more triggering events.

10. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

storing, at a network-accessible database of a provider network, metadata of the particular data stream including a partition map generated in accordance with the stream partitioning policy; and

accessing, from a record retrieval subsystem, the metadata to respond to a particular record retrieval request.

11. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

generating, corresponding to a particular data record of the data stream, a particular sequence number indicative of an order in which the particular data record was received at a record ingestion subsystem relative to other data records of the partition to which the particular data record belongs;

storing, by a record storage subsystem, a plurality of data records including the particular data record in an order based at least in part on respective timestamps generated for the data records; and

in response to receiving a read request invoking the first retrieval interface with the particular sequence number as a parameter, retrieving the particular data record from the record storage subsystem.

12. A system including one or more processors and one or more memories, the one or more memories including program instructions that when executed on one or more processors implement a control node of a multi-tenant stream management service, wherein the control node is configured to:

5 receive a request to initialize a particular data stream to be comprised of a plurality of data records generated by one or more data producers;

determine, based at least in part on a partitioning policy associated with the particular data stream, one or more parameters to be used to configure one or more subsystems for the particular data stream, including a record retrieval subsystem, wherein the one or more parameters comprise an initial number of nodes to be
10 instantiated in the record retrieval subsystem;

identify one or more resources to be used for a particular node of the record retrieval subsystem, wherein the particular node is to be configured to implement a plurality of programmatic record retrieval interfaces, including a first retrieval interface enabling a non-sequential access pattern and a second retrieval interface
15 enabling a sequential access pattern; and

configure the particular node of the record retrieval subsystem using the one or more resources.

20 13. The system as recited in claim 12, wherein the one or more subsystems include a record ingestion subsystem comprising one or more nodes configurable to receive data records of the particular data stream, and a record storage subsystem configurable to store data records of the stream at a selected set of storage locations.

25 14. The system as recited in claim 13, wherein at least one subsystem of the record ingestion subsystem, the record storage subsystem, and the record retrieval subsystem comprises a plurality of nodes configured as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records of the stream and (b) one or more non-primary nodes configured to assume a primary
30 role in response to one or more triggering events.

15. The system as recited in claim 13, at least one node of one of: the record ingestion subsystem, the record storage subsystem or the record retrieval subsystem comprises a

component of a compute instance of a virtualized computing service implemented at a provider network.

CLAIMS

1. A method, comprising:
performing, by one or more computing devices:
determining, for a particular data stream comprising a sequence of a plurality of data records, a set of nodes configurable by one or more control components to perform stream management operations based on one or more policies including a stream partitioning policy for partitioning the particular data stream that comprises the sequence of the plurality of data records into a plurality of partitions;
providing data records in response to record retrieval requests received via one or more programmatic record retrieval interfaces, wherein the one or more programmatic record retrieval interfaces include a first retrieval interface enabling a non-sequential access pattern and a second retrieval interface enabling a sequential access pattern, and wherein a billing rate associated with a use of the first retrieval interface differs from a billing rate associated with a use of the second retrieval interface; and
generating a client billing amount associated with the particular data stream based at least in part on respective usage count metrics of the plurality of record retrieval interfaces.
2. The method as recited in claim 1, further comprising performing, by the one or more computing devices:
assigning, in accordance with the partitioning policy, a particular data record of the particular data stream to a first partition of the plurality of partitions of the particular data stream, based at least in part on a key associated with the particular data record, wherein the key is indicated by a write request corresponding to the particular data record.
3. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

selecting, based at least in part on a partition to which a particular data record is assigned, one or more of (a) a particular node of a record ingestion subsystem responsible for accepting the particular data record, (b) a particular node of a record storage subsystem responsible for storing at least one copy of the particular data record, and (c) a particular node of a retrieval subsystem responsible for obtaining the particular data record from the record storage subsystem in response to a read request.

4. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

receiving data records submitted via one or more programmatic record submission interfaces, wherein the one or more programmatic record submission interfaces include a first submission interface supporting in-line submission of data records and a second submission interface enabling submission of data records by reference to one of: (a) an object address at a storage service implemented by a provider network (b) a universal record locator (c) a database record.

5. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

removing, from a particular node of a data storage subsystem, a particular data record based at least in part on one of: (a) a data de-duplication window configured for the particular data stream, (b) a data archival policy associated with the particular data stream, (c) a data retention policy indicated by a client, (d) a client request to remove the particular data record, or (e) an indication that the particular data record has been processed by one or more data consumers.

6. The method as recited in claim 1, wherein at least one subsystem of: (a) a record ingestion subsystem, (b) a record storage subsystem, or (c) a record retrieval subsystem configured for the particular data stream comprises a plurality of nodes configured by the one or more control components as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records

of the stream and (b) one or more non-primary nodes configured to assume a primary role in response to one or more triggering events.

7. The method as recited in claim 6, wherein a particular primary node of the one or more primary nodes is instantiated at a particular data center, and wherein a particular non-primary node of the one or more non-primary nodes is instantiated at a different data center.

8. The method as recited in claim 6, further comprising performing, by the one or more computing devices:

detecting a triggering event of the one or more triggering events; and

notifying a particular non-primary node of the one or more non-primary nodes to assume the primary role.

9. The method as recited in claim 1, wherein the one or more control components comprise a plurality of control nodes configured as a redundancy group, comprising a primary control node configured to respond to requests for control-plane operations on one or more data streams including the particular data stream, and at least one non-primary control node configured to assume a primary role in response to one or more triggering events.

10. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

storing, at a network-accessible database of a provider network, metadata of the particular data stream including a partition map generated in accordance with the stream partitioning policy; and

accessing, from a record retrieval subsystem, the metadata to respond to a particular record retrieval request.

11. The method as recited in claim 1, further comprising performing, by the one or more computing devices:

generating, corresponding to a particular data record of the data stream, a particular sequence number indicative of an order in which the particular data record was

received at a record ingestion subsystem relative to other data records of the partition to which the particular data record belongs;

storing, by a record storage subsystem, a plurality of data records including the particular data record in an order based at least in part on respective timestamps generated for the data records; and

in response to receiving a read request invoking the first retrieval interface with the particular sequence number as a parameter, retrieving the particular data record from the record storage subsystem.

12. A system including one or more processors and one or more memories, the one or more memories including program instructions that when executed on one or more processors implement a control node of a multi-tenant stream management service, wherein the control node is configured to:

receive a request to initialize a particular data stream to be comprised of a plurality of data records generated by one or more data producers;

determine, based at least in part on a partitioning policy for partitioning the particular data stream that comprises the sequence of the plurality of data records into a plurality of partitions, one or more parameters to be used to configure one or more subsystems for the particular data stream, including a record retrieval subsystem, wherein the one or more parameters comprise an initial number of nodes to be instantiated in the record retrieval subsystem;

identify one or more resources to be used for a particular node of the record retrieval subsystem, wherein the particular node is to be configured to implement a plurality of programmatic record retrieval interfaces, including a first retrieval interface enabling a non-sequential access pattern and a second retrieval interface enabling a sequential access pattern; and

configure the particular node of the record retrieval subsystem using the one or more resources.

13. The system as recited in claim 12, wherein the one or more subsystems include a record ingestion subsystem comprising one or more nodes configurable to receive data records of

the particular data stream, and a record storage subsystem configurable to store data records of the stream at a selected set of storage locations.

14. The system as recited in claim 13, wherein at least one subsystem of the record ingestion subsystem, the record storage subsystem, and the record retrieval subsystem comprises a plurality of nodes configured as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records of the stream and (b) one or more non-primary nodes configured to assume a primary role in response to one or more triggering events.

15. The system as recited in claim 13, wherein at least one node of one of: the record ingestion subsystem, the record storage subsystem or the record retrieval subsystem comprises a component of a compute instance of a virtualized computing service implemented at a provider network.

16. The system as recited in claim 13, wherein the one or more data producers comprise one or more of: (a) a logging component of a computing device, (b) a social media application, (c) a monitoring agent at a computing device, (d) a sensor device, (e) a mobile phone, or (f) a tablet computer.

17. The system as recited in claim 13, wherein at least one subsystem of the record ingestion subsystem, the record storage subsystem, and the record retrieval subsystem comprises a plurality of nodes configured as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records of the stream and (b) one or more non-primary nodes configured to assume a primary role in response to one or more triggering events, and wherein a particular primary node of the one or more primary nodes is instantiated at a particular data center, and wherein a particular non-primary node of the one or more non-primary nodes is instantiated at a different data center.

18. A system, comprising:

one or more computing devices configured to:

determine, by one or more control components of a multi-tenant stream management service, wherein the one or more control components are assigned to a particular data stream comprising a sequence of a plurality of data records generated by one or more data producers, a respective set of nodes of (a) a record ingestion subsystem, (b) a record storage subsystem, and (c) a record retrieval subsystem, wherein each subsystem of the record ingestion subsystem, the record storage subsystem, and the record retrieval subsystem comprises one or more nodes dynamically configurable by the one or more control components based on one or more policies including a partitioning policy for partitioning the particular data stream that comprises the sequence of the plurality of data records into a plurality of partitions;

receive data records submitted via one or more programmatic record submission interfaces implemented at the record ingestion subsystem, wherein the one or more programmatic record submission interfaces include a first submission interface supporting in-line submission of data records and a second submission interface enabling submission of data records by reference to network addresses at which data is stored;

provide contents of data records in response to data record retrieval requests received via one or more programmatic record retrieval interfaces implemented at the record retrieval subsystem, wherein the one or more programmatic record retrieval interfaces include a first retrieval interface enabling a non-sequential access pattern and a second retrieval interface enabling a sequential access pattern, and wherein a billing rate associated with a use of the first retrieval interface differs from a billing rate associated with a use of the second retrieval interface;

generate a client billing amount associated with the particular data stream based at least in part on respective usage count metrics of the plurality of record retrieval interfaces and the plurality of record submission interfaces.

19. The system as recited in claim 18, wherein the one or more computing devices are further configured to:

assign, in accordance with the partitioning policy, a particular data record of the particular data stream to a partition of the particular data stream, based at least in part on a key associated with the particular data record, wherein the key is indicated by a write request corresponding to the particular data record.

20. The system as recited in claim 18, wherein the one or more computing devices are further configured to:

select, based at least in part on a partition to which a particular data record is assigned, one or more of (a) a particular node of the record ingestion subsystem responsible for accepting the particular data record, (b) a particular node of the record storage subsystem responsible for storing at least one copy of the particular data record, and (c) a particular node of the retrieval subsystem responsible for obtaining the particular data record from the record storage subsystem in response to a read request.

21. The system as recited in claim 18, wherein at least one subsystem of the record ingestion subsystem, the record storage subsystem, and the record retrieval subsystem comprises a plurality of nodes configured by the one or more control components as members of a redundancy group, wherein the redundancy group comprises: (a) one or more primary nodes assigned to perform operations on a set of data records and (b) one or more non-primary nodes configured to assume a primary role in response to a detection of one or more triggering events.

22. The system as recited in claim 18, wherein the one or more computing devices are further configured to:

generate, corresponding to a particular data record, a particular sequence number indicative of an order in which the particular data record was received at the record ingestion subsystem relative to other data records of the partition to which the particular data record belongs;

store, by the record storage subsystem, a plurality of data records including the particular data record in an order based at least in part on respective sequence numbers generated for the data records; and

in response to a read request invoking the first retrieval interface with the particular sequence number as a parameter, retrieve the particular data record from the record storage subsystem.

23. A system, comprising:

one or more computing devices comprising one or more respective hardware processors and memory configured to:

determine a partitioning policy to be applied to distribute data records of a data stream among a plurality of nodes of a multi-tenant stream management service, wherein the partitioning policy comprises an initial mapping of data records to a plurality of partitions based at least in part on one or more attribute values associated with the data records;

identify, using the initial mapping, a first partition of which a particular data record of the data stream is to be designated a member, based at least in part on a particular attribute value;

generate, corresponding to the particular data record, a sequence number indicative of a position of the particular data record within a record acquisition sequence at an ingestion node of the stream management service, wherein the ingestion node is selected based at least in part on the initial mapping;

store a plurality of data records of the first partition at a data storage location of the stream management service in an order based at least in part on respective sequence numbers of the plurality of data records, wherein the data storage location is selected based at least in part on the initial mapping; and

in response to a determination that a triggering criterion for repartitioning the data stream has been met,

generate a modified mapping of data records to partitions,

initiate usage of the modified mapping without interrupting a flow of data record acquisitions of the data stream; and

select, for another data record with the particular attribute value, wherein the other data record is received subsequent to an initiation of usage of the modified mapping, at least one of: (a) a different ingestion node of the stream management service or (b) a different data storage location of the stream management service.

24. The system as recited in claim 23, wherein the sequence number comprises an indication of (a) a timestamp associated with ingestion of the particular data record, and (b) an additional subsequence value.

25. The system as recited in claim 24, wherein the one or more computing devices are further configured to:

select an initial timestamp value to be used for sequence numbers of data records to be mapped using the modified mapping;

in response to a data record retrieval request indicating a particular sequence number,

in response to a determination that a value of a particular timestamp indicated by the particular sequence number is lower than the initial timestamp value, utilize the initial mapping to retrieve one or more data records; and

in response to a determination that the value of the particular timestamp is not lower than the initial timestamp value, utilize the modified mapping to retrieve one or more data records.

26. The system as recited in claim 23, wherein the triggering criterion comprises one or more of: (a) a detection of an overload condition, (b) a detection of a workload imbalance, (c) a client request for repartitioning, (d) a determination of a change to a data durability requirement of the data stream, (e) a determination of a schedule of a software version change, (f) a detection of a change to a usage pattern of the data stream, (g) a determination of a pricing impact of repartitioning the data stream, or (h) a determination of a performance target associated with the data stream.

27. The system as recited in claim 23, wherein the one or more computing devices are further configured to:

receive a client request indicating one or more partitioning criteria to be used for the data stream; and

generate the initial mapping based at least in part on the client request.

28. A method, comprising:

performing, by one or more computing devices of a stream management service:

determining an initial mapping of data records of a data stream to a plurality of partitions based at least in part on one or more attribute values of the data records;

identifying, using the initial mapping, a first partition of which a particular data record of the data stream is to be designated a member, based at least in part on a particular attribute value;

storing the particular data record at a storage location selected based at least in part on the initial mapping; and

in response to determining that a triggering criterion has been met,

generating a modified mapping of data records to partitions, and

selecting, for another data record with the particular attribute value and without interrupting a flow of the data records of the data stream, wherein the other data record is received subsequent to an initiation of usage of the modified mapping, a different storage location.

29. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

executing, on the particular data record prior to said determining that the triggering criterion has been met, a processing operation at a worker node selected based at least in part on the initial mapping; and

executing, on a different data record with the particular attribute value, subsequent to said determining that the triggering criterion has been met, the processing operation at a different worker node selected based at least in part on the modified mapping.

30. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

generating, corresponding to the particular data record, a sequence number indicative of a position of the particular data record within a record acquisition sequence at an ingestion node of the stream management service, wherein the ingestion node is selected based at least in part on the initial mapping; and

storing data records of the first partition in an order corresponding to their sequence numbers.

31. The method as recited in claim 30, wherein the sequence number comprises an indication of (a) a timestamp associated with ingestion of the particular data record, and (b) an additional subsequence value.

32. The method as recited in claim 31, wherein the timestamp is indicative of a clock time at which the particular data record was ingested, wherein the method further comprises performing, by the one or more computing devices:

in response to a retrieval request requesting one or more data records to be retrieved based at least in part on a specified record ingestion time range, using sequence numbers associated with the one or more data records as index keys to retrieve the one or more data records.

33. The method as recited in claim 31, further comprising performing, by the one or more computing devices:

selecting an initial timestamp value to be used for sequence numbers of data records to be mapped using the modified mapping;

in response to receiving a data record retrieval request indicating a particular sequence number,

in response to determining that a value of a particular timestamp indicated by the particular sequence number is lower than the initial timestamp value, utilizing the initial mapping to retrieve one or more data records; and

in response to determining that the value of the particular timestamp is not lower than the initial timestamp value, utilizing the modified mapping to retrieve one or more data records.

34. The method as recited in claim 28, wherein said modified mapping uses at least one additional attribute value to determine the partition of a data record.

35. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

receiving a client request indicating one or more partitioning criteria to be used for the data stream; and

generating the initial mapping based at least in part on the client request.

36. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

receiving a client request indicating the triggering criterion.

37. The method as recited in claim 28, further comprising performing by the one or more computing devices:

receiving a client request to re-partition the data stream, wherein the client request indicates one or more parameters of the modified mapping.

38. The method as recited in claim 28, further comprising performing by the one or more computing devices:

receiving a client request indicating a problem state targeted for potential resolution via re-partitioning.

39. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

applying a hash function to at least a portion of contents of the particular data record to obtain a hash result expressed as a binary value comprising a selected number of bits;

determining a particular sub-range, of a range of binary values expressible using the selected number of bits, to which the hash result belongs; and

identifying the first partition based at least in part on the sub-range.

40. The method as recited in claim 28, wherein the one or more attribute values include at least one of: (a) a partition key supplied by a source of a data record, (b) an identification of a source of a data record, (c) at least a portion of contents of a data record, or (d) a network address of a source of the data record.

41. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

configuring, subsequent to the generation of the modified mapping, a different number of nodes of the stream management system to perform one or more of (a) data record ingestion (b) data record storage, or (c) data record retrieval for the data stream than were configured prior to the generation of the modified mapping.

42. The method as recited in claim 28, further comprising performing, by the one or more computing devices:

storing a combined data structure representing the initial mapping and the modified mapping, wherein the combined data structure comprises (a) a first entry indicating a first partition to which a particular data record attribute is mapped in accordance with the initial mapping, and a time range for which the initial mapping is applicable for the first partition, and (b) a second entry indicating a different partition to which the particular data record attribute is mapped in accordance with the modified mapping, and a different time range for which the modified mapping is applicable for the different partition.

43. The method as recited in claim 42, wherein the combined data structure comprises one of: (a) a tree, or (b) a directed acyclic graph.

44. The method as recited in claim 28, wherein the modified mapping comprises an indication of a merger of a pair of partitions indicated by the initial mapping.

45. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors cause the one or more processors to perform steps comprising:

determine a partitioning policy to be applied to distribute data records of a data stream among a plurality of nodes of a stream management service, wherein the partitioning policy comprises an indication of an initial mapping of data records to a plurality of partitions;

configure a first set of ingestion nodes of the stream management service to receive data records of the stream in accordance with the initial mapping, and a first set of data storage nodes of the stream management service to store data records in accordance with the initial mapping;

in response to a determination that a triggering criterion for dynamically repartitioning the data stream has been met,

generate a modified mapping of data records to a different plurality of partitions;

configure, without interrupting a flow of the data records of the data stream, a different set of ingestion nodes and a different set of data storage nodes for data records received subsequent to a generation of the modified mapping;
and

retain, for at least a particular time period during which arriving data records are stored in accordance with the modified mapping, data records stored at the first set of data nodes in accordance with the initial mapping.

46. The non-transitory computer-accessible storage medium as recited in claim 45, wherein the instructions when executed on the one or more processors:

configure an initial set of data retrieval nodes for the data stream in accordance with the initial mapping; and

in response to the determination that the triggering criterion has been met, configure a different set of data retrieval nodes for the data stream.

47. The non-transitory computer-accessible storage medium as recited in claim 45, wherein the triggering criterion comprises one or more of: (a) a detection of an overload condition, (b) a detection of a workload imbalance, (c) a client request for repartitioning, (d) a determination of a change to a data durability requirement of the data stream, (e) a determination of a schedule of a software version change, (f) a detection of a change to a usage pattern of the data stream, (g) a determination of a pricing impact of repartitioning the data stream, or (h) a determination of a performance target associated with the data stream.

48. The non-transitory computer-accessible storage medium as recited in claim 45, wherein the instructions when executed on the one or more processors:

receive a client request indicating one or more partitioning criteria to be used for the data stream; and

generate the initial mapping based at least in part on the client request.

49. The non-transitory computer-accessible storage medium as recited in claim 45, wherein the instructions when executed on the one or more processors:

receive a client request indicating the triggering criterion for re-partitioning the data stream.

50. A system, comprising:

one or more computing devices configured to:

implement one or more programmatic interfaces enabling a client of a multi-tenant stream processing service to indicate, corresponding to a particular

processing stage associated with a specified data stream, wherein the specified data stream comprises a plurality of data records received by the stream processing service over time: (a) a processing operation to be performed on the data records of the specified data stream in accordance with a partitioning policy configured to divide the data records of the specified data stream among worker nodes of the particular processing stage and (b) an output distribution descriptor for results of the processing operations;

receive, from a particular client via the one or more programmatic interfaces, an indication of a particular processing operation to be performed on data records of a particular data stream at the particular processing stage, and a particular output distribution descriptor for results of the particular processing operation;

determine, based at least in part on the partitioning policy and at least in part on an estimated performance capability of resources to be deployed as worker nodes for the processing stage, an initial number of worker nodes for the specified data stream;

configure a particular worker node of the initial number of worker nodes to (a) receive data records of one or more particular partitions of the particular data stream in accordance with the partitioning policy, (b) perform the particular processing operation on received data records, (c) store progress records indicating how far along in the particular data stream the particular worker node has processed a portion of the one or more partitions of the particular data stream, and (d) transfer results of the particular processing operations to one or more destinations in accordance with the particular output distribution descriptor;

monitor a health state of the particular worker node; and

in response to a determination that the particular worker node is in an undesired state, configure a replacement worker node to replace the particular worker node, wherein the replacement worker node accesses a progress record stored by the particular worker node being replaced to identify, by the replacement worker node, at least one data record of the one or more partitions on which the particular processing operation is to be performed by the replacement worker node.

51. The system as recited in claim 50, wherein the particular output distribution descriptor indicates that results of the particular processing operations are to be distributed, as data records of a different data stream, to one or more ingestion nodes configured for the different data stream, in accordance with a different partitioning policy.

52. The system as recited in claim 50, wherein the one or more computing devices are further configured to:

receive, from the particular client, an indication of another processing stage to which data records of the particular data stream are to be provided as input, wherein a different processing operation is to be performed at the other processing stage; and

configure an additional set of worker nodes for the other processing stage.

53. The system as recited in claim 50, wherein the one or more computing devices is further configured to:

in response to a determination that a different worker node configured to perform another processing operation for another processing stage is in an undesired state, configure a different replacement worker node to perform the other processing

operation on one or more subsequently-received data records without accessing a progress record.

54. The system as recited in claim 50, wherein the one or more computing devices is further configured to:

in response to a determination that a workload level at a different worker node of the processing stage meets a triggering criterion, implement a stage reconfiguration operation comprising one or more of: (a) a dynamic repartitioning of the particular data stream performed while additional data records of the stream continue to be processed, (b) an assignment of an alternate worker node to at least one partition previously being processed at the different worker node, (c) a change to a number of worker nodes configured for the processing stage, or (d) a transfer of a worker node from one server to another server.

55. A method, comprising:

performing, by one or more computing devices:

receiving, at a multi-tenant stream processing service from a particular client, an indication of a particular operation to be performed on data records of a particular data stream at a specified processing stage in accordance with a partitioning policy configured to divide the data records of the particular data stream among worker nodes of the specified processing stage, and a particular output distribution descriptor for results of the particular operation, wherein the particular data stream comprises a plurality of data records received by the stream processing service over time;

determining, based at least in part on the particular operation, an initial number of worker nodes to be configured for the specified processing stage in accordance with the partitioning policy;

configuring a particular worker node of the initial number of worker nodes to (a) perform the particular operation on received data records of one or more partitions of the particular data stream, (b) store progress records indicating how far along in the particular data stream the particular worker node has processed a portion of the one or more partitions of the particular data stream, and (c) transfer results of the particular operations to one or more destinations in accordance with the particular output distribution descriptor; and

in response to a determination that the particular worker node is in an unhealthy state, selecting a replacement worker node to replace the particular worker node, wherein the replacement worker node accesses a progress record stored by the particular worker node being replaced to identify, by the replacement worker node, at least one data record of the one or more partitions on which the particular operation is to be performed by the replacement worker node.

56. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

invoking one or more programmatic data record retrieval interfaces implemented by a multi-tenant stream management service to receive data records of the one or more partitions, including a particular programmatic data record retrieval interface that includes, as a parameter, an indication of a sequence number within a partition of a requested data record.

57. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

implementing one or more programmatic interfaces to enable clients of the stream processing service to specify a directed acyclic graph of processing stages for data records of one or more data streams.

58. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

obtaining, from a multi-tenant stream management service responsible for storage of the data records of the particular data stream, an indication of the partitioning policy being used for the particular data stream; and

determining the initial number of worker nodes based at least in part on the partitioning policy.

59. The method as recited in claim 55, wherein the particular output distribution descriptor indicates that results of the particular operations are to be distributed, as data records of a different data stream, to one or more ingestion nodes configured for the different data stream in accordance with a different partitioning policy.

60. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

in response to determining that a different worker node configured to perform another operation for another processing stage is in an undesired state, configuring a different replacement worker node to perform the other operation on one or more subsequently-received data records without accessing a progress record.

61. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

in response to determining that a workload level at a different worker node of the processing stage meets a triggering criterion, implementing one or more of: (a) a dynamic repartitioning of the particular data stream, (b) an assignment of an alternate worker node to at least one partition previously being processed at the different worker node, (c) a change to a number of worker nodes configured for the processing stage, or (d) a transfer of a worker node from one server to another server.

62. The method as recited in claim 55, wherein a result of the particular operation is formatted in accordance with an input format compatible with another stream processing system, and wherein a particular destination of the one or more destinations comprises an input node of the other stream processing system.

63. The method as recited in claim 55 wherein the particular worker node is configured to store, in a persistent data repository, an entry representing accumulated application state information corresponding to a plurality of data records that have been processed at the particular worker node, and to include an indication of the entry in a progress record.

64. The method as recited in claim 55, wherein the operation comprises one of: a log record analysis operation, a resource monitoring metric analysis, a billing amount computation, a sensor data analysis, a social media interaction analysis, a real-time ETL (Extract-Transform-Load) processing operation, or a transformation of a data record prior to its insertion into a data warehouse.

65. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

in response to a stream processing configuration request via an invocation of a client library component, registering, at the multi-tenant stream processing service, a specified resource as a worker node for a different processing stage.

66. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

in response to a stream processing configuration request via an invocation of a client library component, determining, at the multi-tenant stream processing service, one or more categories of control-plane functions to be implemented at a different processing stage.

67. The method as recited in claim 55, wherein the operation is an idempotent operation.

68. The method as recited in claim 55, further comprising performing, by the one or more computing devices:

receiving, at the multi-tenant stream processing service from the particular client, an indication of a particular non-idempotent operation to be performed on data records of a different data stream at a different processing stage; and

configuring a first worker node of the different processing stage to perform the non-idempotent operation on received data records.

69. The method as recited in claim 68, further comprising performing, by the one or more computing devices:

configuring the first worker node of the different processing stage to (a) perform a flush operation to store results of the non-idempotent operations to one or more destinations, and (b) save an indication of a flush operating timing at a persistent storage location; and

configuring a replacement worker node to replay, using the indication of the flush operation timing, the flush operation during recovery after a failure of the first worker node.

70. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors implement a control node of a multi-tenant stream processing service, wherein the control node is operable to:

receive, from a particular client via a programmatic interface, an indication of a particular operation to be performed on data records of a particular data stream, wherein the particular data stream comprises a plurality of data records received by the stream processing service over time;

determine, based at least in part on a partitioning policy associated with the particular data stream, an initial number of worker nodes for the specified data stream at a processing stage, wherein the partitioning policy is configured to divide the data records of the particular data stream among the worker nodes of the processing stage;

configure a particular worker node of the initial number of worker nodes to perform the particular operation on received data records of one or more partitions of the particular data stream and store progress records indicating how far along in the particular data stream the particular worker node has processed a portion of the one or more partitions of the particular data stream; and

in response to a determination that the particular worker node is in an unhealthy state, configure a replacement worker node to replace the particular worker node, wherein the replacement worker node accesses a progress record stored by the particular worker node being replaced to identify, by the replacement worker node, at least one data record of the one or more partitions on which the particular operation is to be performed by the replacement worker node.

71. The non-transitory computer-accessible storage medium as recited in claim 70, wherein the control node is operable to:

configure a redundancy group comprising a plurality of worker nodes to process data records of a different partition of a different data stream, wherein at least one worker node of the plurality of worker nodes is designated as a primary node to receive the data records of the different partition, and wherein at least another worker node of the plurality is configured as a standby node to assume responsibilities of a primary node in response to a triggering event.

72. The non-transitory computer-accessible storage medium as recited in claim 70, wherein the control node is operable to:

in response to a determination that a workload level at a different worker node of the processing stage meets a triggering criterion, implementing one or more of: (a) a dynamic repartitioning of the particular data stream, (b) an assignment of an alternate worker node to at least one partition previously being processed at the different worker node, (c) a change to a number of worker nodes configured for the processing stage, or (d) a transfer of a worker node from one server to another server.

73. The non-transitory computer-accessible storage medium as recited in claim 70, wherein the particular output distribution descriptor indicates that results of the particular operations are to be distributed, as data records of an ephemeral data stream for which storage to a persistent storage device is not a requirement, to one or more ingestion nodes configured for the ephemeral data stream in accordance with a different partitioning policy.

74. The non-transitory computer-accessible storage medium as recited in claim 70, wherein the control node is operable to:

implement one or more programmatic interfaces to enable clients of the stream processing service to specify a directed acyclic graph of processing stages for data records of one or more data streams.

75. A system, comprising:

one or more computing devices configured to:

implement a first set of programmatic interfaces enabling a client of a multi-tenant stream management service to select, for a particular data stream, a data ingestion policy from among a plurality of data ingestion policies, wherein the plurality of data ingestion policies includes an at-least-once ingestion policy in accordance with which a record submitter transmits an indication of a data record one or more times to the stream management service until a positive acknowledgement is received;

implement a second set of programmatic interfaces enabling the client to select, for the particular data stream, a data persistence policy from among a plurality of data persistence policies, wherein the plurality of data persistence policies comprises a multiple-replica persistence policy, in accordance with which multiple copies of the data record are to be stored at respective storage locations by the stream management service;

receive, at the stream management service via respective programmatic interfaces of the first and second set, a first indication that the client has selected the at-least-once ingestion policy for the particular data stream and a second indication that the client has selected the multiple-replica persistence policy for the particular data stream;

in response to a plurality of transmissions indicating a particular data record to the stream management service,

send at least one positive acknowledgement corresponding to the plurality of transmissions in accordance with the at-least-once ingestion policy; and

store, in response to a particular transmission of the plurality of transmissions, copies of the particular data record at a plurality of storage locations in accordance with the multiple-replica persistence policy.

76. The system as recited in claim 75, wherein the plurality of data ingestion policies comprises a best-effort ingestion policy, in accordance with which the stream management service is to accept and store at least some data records of a specified stream without providing corresponding positive acknowledgements to a record submitter.

77. The system as recited in claim 75, wherein the multiple-replica persistence policy selected by the client comprises an indication of a type of storage location to be used for storing copies of data records, wherein the type of storage location comprises one of: (a) magnetic disk-based storage, (b) solid state drive (SSD), (c) volatile RAM (random access memory), (d) non-volatile RAM, (e) a database management system, or (f) a storage node of a network-accessible storage service implemented by a provider network.

78. The system as recited in claim 75, wherein the multiple-replica persistence policy selected by the client comprises an indication of a requested data durability level, wherein the one or more computing devices are further configured to:

select the plurality of storage locations based at least in part on the requested data durability level.

79. The system as recited in claim 75, wherein the one or more computing devices are further configured to:

determine a billing amount that a particular client is to be charged for stream management operations based at least in part on one or more of: (a) a data ingestion policy selected by the particular client, and (b) a data persistence policy selected by the particular client.

80. A method, comprising:

performing, by one or more computing devices:

implementing a set of programmatic interfaces enabling a client of a stream management service to select, for a particular data stream, a data ingestion policy from among a plurality of data ingestion policies, wherein the plurality of data ingestion policies includes an at-least-once ingestion policy in accordance with which a record submitter is to transmit an indication of a data record one or more times to the stream management service until a positive acknowledgement is received;

receiving a request via a programmatic interface of the set, indicating that the client has selected the at-least-once ingestion policy for the particular data stream;

in response to receiving a plurality of transmissions indicating a particular data record at the stream management service,

sending respective positive acknowledgements corresponding to each transmission of the plurality of transmissions in accordance with the at-least-once ingestion policy; and

storing, in response to receiving a particular transmission of the plurality of transmissions, copies of the particular data record at a one or

more storage locations in accordance with a data persistence policy selected for the particular data stream.

81. The method as recited in claim 80, wherein the plurality of data ingestion policies comprises a best-effort ingestion policy, in accordance with which the stream management service is to accept and store at least some data records of a specified stream without providing corresponding positive acknowledgements to a record submitter.

82. The method as recited in claim 80, wherein in accordance with the at-least-once ingestion policy, the stream management service is configured to eliminate duplicated data records.

83. The method as recited in claim 80, wherein in accordance with the at-least-once ingestion policy, the stream management service is configured to store, corresponding to the plurality of transmissions, more than one copy of the particular data record.

84. The method as recited in claim 80, further comprising performing, by the one or more computing devices:

implementing a second set of programmatic interfaces enabling the client to select, for the particular data stream, the data persistence policy from among a plurality of data persistence policies.

85. The method as recited in claim 84, wherein the plurality of data persistence policies include a multiple-replica persistence policy and a single-replica persistence policy.

86. The method as recited in claim 84, wherein the data persistence policy comprises an indication of a type of storage location to be used for storing data records, wherein the type of storage location comprises one of: (a) magnetic disk-based storage, (b) solid state drive (SSD), (c) volatile RAM (random access memory), (d) non-volatile RAM, (e) a database management

system, or (f) a storage node of a network-accessible storage service implemented by a provider network.

87. The method as recited in claim 84, wherein the data persistence policy comprises an indication of a first type of storage location to be used for a first partition of the particular data stream, and an indication of a different type of storage location to be used for a second partition of the particular data stream.

88. The method as recited in claim 84, wherein the data persistence policy selected by the client does not include an indication of a type of storage location to be used for storing data records, further comprising performing, by the one or more computing devices:

selecting, by one or more components of the stream management service, a type of storage location to be used for storing data records.

89. The method as recited in claim 88, wherein said selecting a type of storage location comprises selecting a first type of storage location for a first partition of the particular data stream, and selecting a different type of storage location for a second partition of the particular data stream.

90. The method as recited in claim 84, wherein the data persistence policy includes an indication of a target latency, further comprising performing, by the one or more computing devices:

selecting, by one or more components of the stream management service, a type of storage location to be used for storing data records based at least in part on the target latency.

91. The method as recited in claim 84, wherein the data persistence policy selected by the client comprises an indication of a requested data durability level, further comprising performing, by the one or more computing devices:

selecting a plurality of storage locations at which data records of the particular data stream are to be stored based at least in part on the requested data durability level.

92. The method as recited in claim 80, further comprising performing, by the one or more computing devices:

determining a billing amount that a particular client is to be charged for stream management operations based at least in part on one or more of: (a) a data ingestion policy selected by the particular client, and (b) a data persistence policy selected by the particular client.

93. The method as recited in claim 80, further comprising performing, by the one or more computing devices:

determining a number of data ingestion nodes to be configured for the particular data stream based at least in part on a partitioning policy in accordance with which (a) the particular data record is designated as a member of a particular partition based on one or more attributes of the particular data record and (b) a data ingestion node of the number of data ingestion nodes is selected to ingest data records of the particular partition.

94. The method as recited in claim 80, further comprising performing, by the one or more computing devices:

determining a number of data storage nodes to be configured for the particular data stream based at least in part on a partitioning policy in accordance with which (a) the particular data record is designated as a member of a particular partition based on one or more attributes of the particular data record and (b) a data storage node of the number of data storage nodes is selected to store data records of the particular partition.

95. The method as recited in claim 80, further comprising performing, by the one or more computing devices:

storing, corresponding to each data record of a plurality of data records of the particular data stream, including the particular data record, a respective sequence number usable to respond to read requests for ordered sets of data records;

receiving, from a submitter of a different data record of the particular data stream, an indication of a minimum sequence number to be stored corresponding to the different data record; and

storing, corresponding to the different data record, a particular sequence number that is greater than or equal to the minimum sequence number.

96. A non-transitory computer-accessible storage medium storing program instructions that, when executed on one or more processors, cause the one or more processors to:

implement a set of programmatic interfaces enabling a client of a network-based data stream management service to select, for a particular data stream, a data persistence policy from among a plurality of data persistence policies, wherein the plurality of data persistence policies includes (a) a multiple-replica persistence policy in accordance with which multiple copies of a data record of the particular data stream are to be stored at respective storage locations and (b) a single-replica persistence policy in which a single copy of a data record of the particular data stream is to be stored, wherein data records for the particular data stream are ingested into the particular data stream based on a selected data ingestion policy;

receive, via a programmatic interface of the set, a request indicating that the client has selected the multiple-replica persistence policy for the particular data stream; and

configure a plurality of storage nodes to implement the multiple-replica persistence policy for data records of the particular data stream.

97. The non-transitory computer-accessible storage medium as recited in claim 96, wherein at least one data persistence policy of the plurality of data persistence policies comprises an indication of a type of storage location to be used for storing data records, wherein the type of storage location comprises one of: (a) magnetic disk-based storage, (b) solid state drive (SSD), (c) volatile RAM (random access memory), (d) non-volatile RAM, (e) a database management system, or (f) a storage node of a network-accessible storage service implemented by a provider network.

98. The non-transitory computer-accessible storage medium as recited in claim 96, wherein the multiple-replica persistence policy selected by the client comprises an indication of a requested data durability level, wherein the instructions, when executed on the one or more processors, cause the one or more processors to:

determine a number of storage nodes to be configured based at least in part on the requested data durability level.

99. The non-transitory computer-accessible storage medium as recited in claim 96, wherein the instructions, when executed on the one or more processors, cause the one or more processors to:

determine a number of data storage nodes to be configured for the particular data stream based at least in part on a partitioning policy in accordance with which (a) a particular data record is designated as a member of a particular partition based on one or more attributes of the particular data record and (b) a data storage node of the number of data storage nodes is selected to store data records of the particular partition.

100. The non-transitory computer-accessible storage medium as recited in claim 96, wherein the instructions, when executed on the one or more processors, cause the one or more processors to:

implement a different set of programmatic interfaces enabling a different client of the network-based stream service to select, for a different data stream, a data persistence policy from among the plurality of data persistence policies;

receive, via a different programmatic interface of the set, a different request indicating that a different client of the network-based stream service has selected a different data persistence policy for a different data stream; and

configure the plurality of storage nodes to implement the different data persistence policy for data records of the different data stream.

101. A system, comprising:

one or more hardware computing devices configured to:

implement a set of programmatic interfaces enabling clients of a provider network to select from among a plurality of security-related options for data records of a specified stream, wherein the plurality of security-related options include one or more placement destination type options for nodes of one or more functional categories of a plurality of functional categories that includes: (a) control nodes, (b) record ingestion nodes, (c) record storage nodes, (d) record retrieval nodes and (e) record processing nodes;

receive, via a programmatic interface of the set of programmatic interfaces, one or more requests from a client of the provider network, wherein one of the one or more requests from the client specifies one of the plurality of security-related options comprising at least one of the one or more

placement destination type options selected for a particular stream, wherein the at least one placement destination type option instructs that one or more nodes of a first functional category of the plurality of functional categories associated with the particular stream are to be configured at one or more data centers of the provider network, and instructs that one or more nodes of a second functional category of the plurality of functional categories associated with the particular stream are to be configured at a facility external to the provider network;

in response to the one or more requests from the client of the provider network:

configure one or more nodes of the first functional category at one or more hardware computing devices of one or more data centers of the provider network;

initiate a configuration of one or more nodes of the second functional category at one or more hardware computing devices of the facility external to the provider network; and

activate one or more record ingestion nodes assigned to the data stream to begin collecting data records of the particular stream.

102. The system as recited in claim 101, wherein the first functional category comprises record storage nodes, and the second functional category comprises record processing nodes.

103. The system as recited in claim 101, wherein the plurality of security-related options comprises an option to configure one or more nodes of a specified functional category within an isolated virtual network associated with the client and implemented at the provider network.

104. The system as recited in claim 101, wherein the provider network implements a multi-tenant computing service utilizing a plurality of instance hosts, wherein at least some

instance hosts of the plurality of instance hosts are each configurable to instantiate compute instances on behalf of a plurality of clients, and wherein the plurality of security-related options comprises an option to instantiate one or more nodes of a specified functional category of nodes on an instance host that hosts no more than one client.

105. The system as recited in claim 101, wherein the plurality of security-related options comprises an option to encrypt, at nodes of one or more functional categories, data records prior to transmission of the data records over a network link.

106. A method, comprising:

performing, by one or more hardware computing devices:

implementing a set of programmatic interfaces enabling a client of a data stream management service to select, for a specified stream, a placement option for one or more functional categories of nodes of the stream management service, wherein the stream management service utilizes nodes of a plurality of functional categories including at least (a) data ingestion nodes and (b) data processing nodes;

receiving, via a programmatic interface of the set of programmatic interfaces, a request from the client of the data stream management service, wherein the request specifies a placement option selected for a particular stream, wherein the placement option specified in the request from the client instructs the stream management service to configure one or more nodes of a first functional category of the plurality of functional categories using resources with a first security profile, and instructs the stream management service to configure one or more nodes of a second functional category of the plurality of functional categories using resources with a different security profile;

in response to the request from the client of the data stream management service:

initiating a configuration of one or more nodes of the first functional category at a first selected resource with the first security profile, wherein the first selected resource is implemented by one or more first hardware computing devices; and

initiating a configuration of one or more nodes of the second functional category at a second selected resource with the different security profile, wherein the second selected resource is implemented by one or more second hardware computing devices.

107. The method as recited in claim 106, wherein the plurality of functional categories include one or more of: (a) data storage nodes, (b) data retrieval nodes, and (c) control nodes.

108. The method as recited in claim 106, wherein in accordance with the request, the first selected resource is implemented at a data center of a provider network, and wherein the second selected resource is implemented at a facility external to the provider network.

109. The method as recited in claim 108, wherein the facility external to the provider network is linked to the provider network via an unshared physical network link dedicated for use by a particular client.

110. The method as recited in claim 108, wherein the first functional category comprises data ingestion nodes, and the second functional category of nodes comprises data processing nodes.

111. The method as recited in claim 106, wherein the second selected resource comprises one or more of: (a) a hardware device with a capability that is not supported at the provider network or (b) a software module with a capability that is not supported at the provider network.

112. The method as recited in claim 106, wherein in accordance with the request, the first selected resource is implemented at a first compute instance of a virtual computing service of the provider network, and wherein the second selected resource is implemented at a second compute instance of the virtual computing service, wherein operations of the first functional category are performed using a client-provided executable program whose execution at the first compute instance is managed by the stream management service, and wherein operations of the second functional category are managed by the client.

113. The method as recited in claim 106, wherein, in accordance with the request, the first selected resource is implemented within an isolated virtual network of the client implemented at the provider network.

114. The method as recited in claim 106, wherein the provider network implements a multi-tenant computing service utilizing a plurality of instance hosts, wherein at least some instance hosts of the plurality of instance hosts are each configurable to instantiate compute instances on behalf of a plurality of clients, wherein, in accordance with the request, the first selected resource comprises an instance host that is configured to instantiate compute instances on behalf of no more than one client.

115. The method as recited in claim 106, further comprising performing, by the one or more computing devices:

implementing a programmatic interface to enable a client to request an encryption, at nodes of one or more functional categories, of data records prior to transmission of the data records over a network link.

116. The method as recited in claim 106, further comprising performing, by the one or more computing devices:

providing a library of executable modules installable at one or more computing devices at a facility external to the provider network to implement at least a subset of

functionality of nodes of one or more functional categories of the plurality of functional categories.

117. The method as recited in claim 106, wherein said initiating the configuration of one or more nodes of the first functional category comprises initiating the configuration of at least one node at each of a plurality of data centers in accordance with an availability requirement.

118. A non-transitory computer-accessible storage medium storing program instructions of a service that when executed on one or more computer hardware processors:

receive, from a client of the service, a configuration request comprising a security option selected for a particular data stream for which nodes of a plurality of functional categories are to be configured, wherein the plurality of functional categories comprises at least a data ingestion category and a data retrieval category, wherein the security option indicates a security profile of a resource to be used for one or more nodes of at least one functional category of the plurality of functional categories;

in response to the request from the client of the service, configure, in accordance with the request comprising the selected security option, a node of a first functional category of the at least one functional category at a resource with a first security profile, wherein the resource is implemented by one or more hardware computing devices; and

initiate a configuration of a node of a second functional category of the plurality of functional categories at a different resource with a different security profile, wherein the different resource is implemented by one or more different hardware computing devices.

119. The non-transitory computer-accessible storage medium as recited in claim 118, wherein the plurality of functional categories include one or more of: (a) a data storage category, (b) a data processing category, or (c) a control category.

120. The non-transitory computer-accessible storage medium as recited in claim 118, wherein the resource used for the node of the first functional category is located within a provider network, and the resource used for the node of the second functional category is located outside the provider network.

121. The non-transitory computer-accessible storage medium as recited in claim 118, wherein in accordance with the configuration request, one or more nodes of the first functional category are configured at a computing device within an isolated virtual network implemented at a provider network.

122. The non-transitory computer-accessible storage medium as recited in claim 118, wherein in accordance with the configuration request, at least one node of the first functional category is instantiated at a particular instance host of a multi-tenant virtual computing service, wherein the particular instance host is configured to instantiate compute instances on behalf of no more than one client.