DATASTAX

FEATURE IN FOCUS

DataStax Enterprise – Advanced Security

Protecting the data collected by an enterprise is a top priority for CIO's, CTO's, database administrators, security administrators, and others in IT operations. DataStax Enterprise inherits the basic security feature set provided in open source Apache Cassandra and provides a set of commercial security extensions that enterprises need to protect critical data.

Search
Analytics
In-Memory
DSE
Expert Support
Visual Admin
Security
Cassandra Certified
Management Services

DataStax Enterprise delivers constant uptime and linear scale performance for online applications needing transactional, analytical, search, and in-memory workload support in a single platform.

Internal Authentication

DataStax Enterprise (DSE) supports internal-based authentication, which allows administrators to easily create users who can be authenticated to DSE database clusters. Those migrating to DataStax Enterprise from RDBMS's will find the authentication framework extremely familiar.

Administrators can use the CREATE USER command to create new users with passwords that will then be internally managed by Cassandra and used to authenticate into a database cluster. User accounts may also easily be altered and dropped.

External Authentication

Corporations and organizations that use external, 3rd party security packages to manage security in their environment can easily integrate DSE into their infrastructure. DSE supports widely used and trusted external security software such as Kerberos, LDAP, and Active Directory.

Permission Management/ Authorization

Once authenticated into a database cluster, using either internal or external authentication, the next security issue to be tackled is permission management; i.e. what the user can do inside the database. DataStax Enterprise supplies easy to use authorization capabilities for Cassandra that use the very familiar GRANT/REVOKE security paradigm from relational databases.

Control over DDL, DML, and SELECT operations are all handled via the granting and revoking of user privileges. The permissions that each user account possesses as well as what rights have been granted to certain objects may easily be determined by various Cassandra Query Language (CQL) commands.

Client-to-Node and Node-to-Node Data Encryption

DSE includes a secure form of communication from a client machine to a database cluster, as well as communication between nodes in a cluster. SSL ensures data in flight is not compromised and is securely transferred back/forth from client machines as well as between nodes in any cluster.

Transparent Data Encryption

Transparent Data Encryption (TDE) in DataStax Enterprise protects data at rest from being stolen and used in an authorized manner. TDE may be a good option for objects containing sensitive information such as social security numbers, credit card information, etc.

Administrators can encrypt tables via a CQL command with AES 128 being the default, although other encryption algorithms can be used. Tables may also be decrypted via the same CQL command.

Encryption is transparent to all end user activities. Data may be read, inserted, updated, etc., with nothing having to change from the application end. Encryption keys may be stored either on the database servers or on other servers that are external to the database cluster.

DATASTAX

3975 Freedom Circle
Santa Clara, CA 95054
(650) 389-6000

Data Auditing

DSE supports the ability to configure data auditing so an administrator can understand what user activities took place on a particular node or entire cluster. Data auditing allows for a "who looked at what/when, who changed what/when" type of documentation that many large-scale enterprises need to have in order to comply with various internal or external security policies.

Administrators have total flexibility and control over what gets audited and where audit information is written and stored. For example, all activity for an entire cluster may be tracked, only data modifications, only read operations, only login failures, etc.

In addition to standard user activity tracking, the auditing features of DSE provide a great way to detect and prevent data theft.

Uniform Security for Analytics and Search Data

DataStax Enterprise does away with the need to shard applications and use multiple data management providers for transactions, analytics, search, and in-memory workloads. Instead, DSE provides an easy way to run mixed workload operations on Cassandra data without resource contention (for either data or compute resources) occurring in a database cluster.

Where security is concerned, instead of administrators having to handle security on multiple systems and/or different database providers, DSE makes it easy as one set of security features covers all workloads on one platform.

SOX and PCI Compliance

DSE meets both SOX and PCI compliance standards for database systems. For more information on how DSE handles such security standards, see the specific white papers written for both SOX and PCI.

External Security Firm Validation

DataStax contracted with the security industry expert group iSECpartners to perform a review of the security implementation and feature set in DataStax Enterprise to ensure no key security holes existed in the platform. The conclusion of iSECpartner's review was that no major security concerns exist in the DSE platform.

Security Differences Between Open Source Cassandra / DataStax Enterprise

The following table summarizes the security feature differences between open source Cassandra and DataStax Enterprise.

Security Feature	Open Source Cassandra	DataStax Enterprise
Basic/Internal Authentication	Yes	Yes
Permission Management	Yes	Yes
Client-to-Node Encryption	Yes	Yes
Node-to-Node Encryption	Yes	Yes
External Authentication	No	Yes
Transparent Data Encryption	No	Yes
Data Auditing	No	Yes
Analytics/Search/In-Memory Security	No	Yes
PCI/SOX Compliant	No	Yes
External Security Firm Validation	No	Yes

Further Reading

The advanced security option of DataStax Enterprise provides the type of enterprise-class data protection needed by today's Web, mobile, and IoT applications. For more resources and downloads of DataStax Enterprise, visit www.datastax.com today.

DATASTAX

3975 Freedom Circle
Santa Clara, CA 95054
(650) 389-6000

DataStax delivers Apache Cassandra in a database platform purpose built for the performance and availability demands of Web, Mobile, and IOT applications, giving enterprises a secure always-on database that remains operationally simple when scaled in a single datacenter or across multiple datacenters and clouds.

DataStax has more than 500 customers in 38 countries including leaders such as Netflix, Rackspace, Pearson Education, and Constant Contact, and spans verticals including web, financial services, telecommunications, logistics, and government. Based in San Mateo, Calif., DataStax is backed by industry-leading investors including Lightspeed Venture Partners, Meritech Capital, and Crosslink Capital. For more information, visit DataStax.com or follow us @DataStax.