Janis Gonzalez

WEB 335 Introduction to NoSQL

Discussion 7.1 Database Security

April 27,2023

Bellevue University

A user administrator should be created first in a MongoDB database. Then the additional unique MongoDB users should be added for each person and application that will have access to the database system. MongoDB data can also be encrypted with the help of the WiredTiger storage engine’s native Encryption at Rest (2021). Encryption at Rest is data that is stored and is protected by an anti-virus software or a firewall (2021). If this is not being used, then the data can be encrypted on each host using filesystem, device, or physical encryption. Encryption in Transit is when the encrypted data is active and moving around between networks and devices (2021). For example, when a user logs into their e-mail, the password is sent to a third-party application for validation. Collecting logs into a central log store can also be useful since these logs contain database authentication attempts which include source IP addresses (Security Checklist). Ensuring that MongoDB runs on a trusted network environment is also important. Controlling inbound and outbound traffic by configuring firewall or security groups is also essential for the MongoDB instances (7 best practices for mongodb security). Direct SSH root access should also be disabled to limit the database’s network exposure. The MongoDB database should also have audit records where system events such as connection events and user operations can be recorded since these allow forensic analysis and administrators to exercise proper controls (Security Checklist). MongoDB should also be run using a dedicated operating system user account that has permissions to access the data, but no additional permissions that are not needed (7 best practices for mongodb security. Since MongoDB supports the execution of JavaScript code for some server-side operations, if some of these operations are not needed, they should be disabled using –noscripting (Security Checklist). Input validation should also be enabled since this makes sure all documents are stored by the mongod instance. Multi-factor authentication is also something that should be kept in mind when protecting sensitive information from being easily stolen, copied and shared. This requires a user to login with something only they know (for example a username) and has the user combine it with something they own (like their mobile device) (7 best practices for mongodb security. Once both of these factors are authenticated, the user will have access to the data. MongoDB’s recommended password policy is that it should contain at least eight characters that contain unique characters, numbers, or symbols (Manage Your MongoDB Atlas Account). The password should exclude the username and email address. The password should also be different than the four last passwords used and should not be the same as other commonly used passwords (Manage Your MongoDB Atlas Account).

References:

*7 best practices for mongodb security*. MongoDB. (n.d.). Retrieved from <https://www.mongodb.com/features/security/best-practices>

*Encryption: Understanding data at rest vs. in transit*. DataLocker Inc. (2021, September 24). Retrieved from <https://datalocker.com/blog/technology/encryption/encryption-at-rest-vs-in-transit-effectively-encrypt-identifiable-information/>

*Manage Your MongoDB Atlas Account*. MongoDB Atlas. (n.d.). Retrieved from <https://www.mongodb.com/docs/atlas/security/manage-your-mongodb-atlas-account/#:~:text=Atlas%20Password%20Policy,characters%2C%20numbers%2C%20or%20symbols>.

*Security Checklist*. MongoDB Manual. (n.d.). Retrieved from <https://www.mongodb.com/docs/manual/administration/security-checklist/>