|  |
| --- |
| Home Start Realty |
| Security Checklist |

To: Brendan McAlister

From: Chad Ballay

As part of building our inhouse talent pool we’ve started capturing some best practices and lessons learned into a checklist for when we transition security for MySQL from third party vendors to ourselves.

Much of this starts with the National Checklist Program entry for securing MySQL. The National Checklist Program captures best practices at a broad level and socializes them for standardization. (<https://nvd.nist.gov/ncp/repository>) Specifically the MySQL checklist is provided by the Center for Internet Security. (<https://learn.cisecurity.org/l/799323/2020-07-14/216rx>)

This has been copied over verbatium and will be the beginning our own internal checklist.

1. Operating System Level Configuration
   1. Place Databases on Non-System Partitions
   2. Use Dedicated Least Privileged Account for MySQL Daemon/Service
   3. Disable MySQL Command History
   4. Verify That the MYSQL\_PWD Environment Variables Is Not In Use
   5. Disable Interactive Login
   6. Verify That 'MYSQL\_PWD' Is Not Set In Users' Profiles
2. Installation and Planning
   1. Backup and Disaster Recovery
      1. Backup policy in place
      2. Verify backups are good
      3. Secure backup credentials
      4. The backups should be properly secured
      5. Point in time recovery
      6. Disaster recovery plan
      7. Backup of configuration and related files
   2. Dedicate Machine Running MySQL
   3. Do Not Specify Passwords in Command Line
   4. Do Not Reuse Usernames
   5. Do Not Use Default or Non-MySQL-specific Cryptographic Keys
   6. Set a Password Expiry Policy for Specific Users
3. File System Permissions
   1. Ensure 'datadir' Has Appropriate Permissions
   2. Ensure 'log\_bin\_basename' Files Have Appropriate Permissions
   3. Ensure 'log\_error' Has Appropriate Permissions
   4. Ensure 'slow\_query\_log' Has Appropriate Permissions
   5. Ensure 'relay\_log\_basename' Files Have Appropriate Permissions
   6. Ensure 'general\_log\_file' Has Appropriate Permissions
   7. Ensure SSL Key Files Have Appropriate Permissions
   8. Ensure Plugin Directory Has Appropriate Permissions
4. General
   1. Ensure Latest Security Patches Are Applied
   2. Ensure the 'test' Database Is Not Installed
   3. Ensure 'allow-suspicious-udfs' Is Set to 'FALSE'
   4. Ensure 'local\_infile' Is Disabled
   5. Ensure 'mysqld' Is Not Started with '--skip-grant-tables'
   6. Ensure '--skip-symbolic-links' Is Enabled
   7. Ensure the 'daemon\_memcached' Plugin Is Disabled
   8. Ensure 'secure\_file\_priv' Is Not Empty
   9. Ensure 'sql\_mode' Contains 'STRICT\_ALL\_TABLES'
5. MySQL Permissions
   1. Ensure Only Administrative Users Have Full Database Access
   2. Ensure 'file\_priv' Is Not Set to 'Y' for Non-Administrative Users
   3. Ensure 'process\_priv' Is Not Set to 'Y' for Non-Administrative Users
   4. Ensure 'super\_priv' Is Not Set to 'Y' for Non-Administrative Users
   5. Ensure 'shutdown\_priv' Is Not Set to 'Y' for Non-Administrative Users
   6. Ensure 'create\_user\_priv' Is Not Set to 'Y' for Non-Administrative Users
   7. Ensure 'grant\_priv' Is Not Set to 'Y' for Non-Administrative Users
   8. Ensure 'repl\_slave\_priv' Is Not Set to 'Y' for Non-Slave Users
   9. Ensure DML/DDL Grants Are Limited to Specific Databases and Users
6. Auditing and Logging
   1. Ensure 'log\_error' Is Not Empty
   2. Ensure Log Files Are Stored on a Non-System Partition
   3. Ensure 'log\_error\_verbosity' Is Not Set to '1'
   4. Ensure Audit Logging Is Enabled
   5. Ensure 'log-raw' Is Set to 'OFF'
7. Authentication
   1. Ensure Passwords Are Not Stored in the Global Configuration
   2. Ensure 'sql\_mode' Contains 'NO\_AUTO\_CREATE\_USER'
   3. Ensure Passwords Are Set for All MySQL Accounts
   4. Ensure 'default\_password\_lifetime' Is Less Than Or Equal To '90'
   5. Ensure Password Complexity Is in Place
   6. Ensure No Users Have Wildcard Hostnames
   7. Ensure No Anonymous Accounts Exist
8. Network
   1. Ensure 'have\_ssl' Is Set to 'YES'
   2. Ensure 'ssl\_type' Is Set to 'ANY', 'X509', or 'SPECIFIED' for All Remote Users
9. Replication
   1. Ensure Replication Traffic Is Secured
   2. Ensure 'MASTER\_SSL\_VERIFY\_SERVER\_CERT' Is Set to 'YES' or '1'
   3. Ensure 'master\_info\_repository' Is Set to 'TABLE'
   4. Ensure 'super\_priv' Is Not Set to 'Y' for Replication Users
   5. Ensure No Replication Users Have Wildcard Hostnames