Center for Internet Security®

CIS MySQL Server 5.6 社区版安全基准

v1.1.0 2016-08-15
v1.1.0 2018-10-23 翻译

目 录

概览

本文档CIS Oracle MySQL5.6企业版基准，为MySQL Enterprise Edition 5.7建立安全配置状态提供了说明性指导。本指南针对在Ubuntu Linux 14.04上运行的MySQL Enterprise Edition 5.6进行了测试，但也适用于其他Linux发行版。要获取本指南的最新版本，请访问https://www.cisecurity.org/cis-benchmarks/。如果您有任何问题，意见或已找到改进本指南的方法，请发送电子邮件至feedback@cisecurity.org。

目标受众

本文档适用于计划开发，部署，评估或保护包含Oracle MySQL Enterprise Edition 5.7的解决方案的系统和应用程序管理员，安全专家，审计员，技术支持人员和平台部署人员。

共识指南

该基准是由学科专家使用协商审核流程创建的。参与者提供来自各自背景的视角，包括咨询，软件开发，审计和合规，安全研究，运营，政府和法律。

每个CIS基准都经历了两个阶段的协商审查。第一阶段发生在初始基准开发期间。在此阶段，学科专家召集会议讨论，创建和测试基准的工作草案。这一讨论一直持续到基准建议达成共识为止。第二阶段在基准发布后开始。在此阶段，互联网社区提供的所有反馈均由协商团队审核，以纳入基准。如果您有兴趣参与协商流程，请访问https://www.cisecurity.org/communities/。

排版约定

在本指南中使用了以下排版约定:

约定（格式）	意义
`Stylized Monospace font` 程式化的等宽字体	用于代码块、命令和脚本示例。文本应该完全按照所提供的解释。
等距字体	用于内联代码、命令或示例。文本应该完全按照所提供的解释。
<在方括号>中的斜体字体	尖括号中设置的斜体文本表示需要替换实际的变量。
斜体	用来表示一本书、一篇文章或其他出版物的标题。
注意	附加信息或警告

评分信息

评分状态是指对遵守给定的建议是否影响评估目标的基准评分。本基准测试使用以下评分状态:

Scored

不遵守“Scored”的建议将降低最终基准评分。遵守“Scored”的建议将提高最终基准评分。

Not Scored

不遵守“Not Scored”建议并不会降低最终基准评分。遵守“Not Scored”的建议也不会增加最终的基准评分。

概要定义

这个基准定义了以下配置文件：

- **Level 1 -MySQL RDBMS on Linux**

  本配置文件中的项目适用于运行在Linux上的MySQL Enterprise Edition 5.6并具有以下目的：
  - 务实而谨慎
  - 提供明确的安全收益
  - 不会超出可接受的手段来抑制技术的效用

- **Level 2 -MySQL RDBMS on Linux**

  这个配置文件扩展了"*Level 1 -MySQL RDBMS on Linux*"的内容，概要中的项目适用于运行在Linux上的MySQL Enterprise Edition 5.6，并具有以下一个或多个特征:
  - 适用于安全性至关重要的环境或用例
  - 充当深度防御措施
  - 可能会对技术的效用或性能产生负面影响

- **Level 1 -MySQL RDBMS**

  本概要中的项目适用于MySQL企业版5.6，并且：
  - 务实而谨慎
  - 提供明确的安全收益
  - 不会超出可接受的手段来抑制技术的效用

  注意:这个概要文件的目的是包括可以通过远程连接到MySQL RDBMS进行评估的检查。因此，此配置文件中不包含与文件系统相关的检查。

- **Level 2 -MySQL RDBMS**

  这个概要文件扩展了"*Level 1 -MySQL RDBMS*"具有以下一个或多个特点：
  - 适用于安全性至关重要的环境或用例
  - 充当深度防御措施
  - 可能会对技术的效用或性能产生负面影响

  注意:这个概要文件的目的是包括可以通过远程连接到MySQL RDBMS进行评估的检查。因此，此配置文件中不包含与文件系统相关的检查。

感谢

这个基准说明了一个由用户、供应商和学科专家组成的社区通过协商完成的伟大事情。独联体（CIS）社区感谢整个协商小组，特别感谢以下为编写本指南作出重大贡献的个人：

贡献者
Binod Bista
Daniël van Eeden

校订者
Adam Montville, *Center for Internet Security*
Timothy Harrison, *Center for Internet Security*
Sheryl Coppenger, *U.S. Government Accountability Office*
Karen Scarfone
Robert Warren Thomas
Neil Quiogue
Dan White, *CIS Community*

译者
Wei tao 汉武安全实验室研究员

建议

1 操作系统级配置

本节包含与运行MySQL数据库服务器的操作系统相关的建议。

1.1 存放系统库在非系统分区（Scored）

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

通常认为主机操作系统应包括用于不同目的不同文件系统分区。一组文件系统通常称为“系统分区”，通常保留用于主机系统/应用程序操作。另一组文件系统通常称为“非系统分区”，这些位置通常保留用于存储数据。

解释:

通常认为主机操作系统应包括用于不同目的不同文件系统分区。一组文件系统通常称为“系统分区”，通常保留用于主机系统/应用程序操作。另一组文件系统通常称为“非系统分区”，这些位置通常保留用于存储数据。

审计:

执行以下步骤来评估此建议：

- 通过执行以下SQL语句来检查datadir

```
show variables where variable_name = 'datadir';
```

- 使用上述查询中返回的datadir值，在系统终端中执行以下操作

```
df -h <datadir Value>
```

- 从上面的df命令返回的输出不应包括root（'/'）,"/var", 或者"/usr"。

修复：

执行以下步骤以修复此设置：

1. 为MySQL数据选择一个非系统分区的新位置
2. 使用如下命令停止mysqld：service mysql stop
3. 使用以下命令复制数据：cp -rp <datadir Value> <new location>
4. 将datadir位置设置为MySQL配置文件中的新位置
5. 使用如下命令启动mysqld：service mysql start

注意：在某些Linux发行版上，您可能需要另外修改apparmor设置。例如，在Ubuntu 14.04.1系统上编辑文件/etc/apparmor.d/usr.sbin.mysqld，以便数据库访问`datadir`是合适的。原文件内容可能如下所示：

```
# Allow data dir access
 /var/lib/mysql/ r,
 /var/lib/mysql/** rwk,
```

将这两条路径改为您在上面选择的新位置。例如，如果新位置是/media/mysql，则/etc/apparmor.d/usr.sbin.mysqld文件应包含以下内容：

```
# Allow data dir access
  /media/mysql/ r,
  /media/mysql/** rwk,
```

影响：

将数据库移动到非系统分区可能很困难，具体取决于在设置操作系统时是否只有一个分区以及是否有其他可用存储空间。

1.2 为MySQL守护进程/服务使用专用最小特权帐户(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

与主机上安装的其他服务一样，可以为其提供用户自己的上下文。为服务提供专用的用户，提供了在较大主机环境中精确约束服务的能力。

解释:

利用MySQL的最小权限帐户来运行，可以减少MySQL产生的漏洞的影响。受限帐户将无法访问与MySQL无关的资源，例如操作系统配置。

审计:

在终端提示符处执行以下命令以评估此建议：

```
ps -ef | egrep "^mysql.*$"
```

如果没有任何返回行，那么这是一个漏洞发现。

注意：假设MySQL的运行用户是`mysql`。此外，您可以考虑运行`sudo -l`作为MySQL用户检查sudoers文件。

修复:

创建一个仅用于运行MySQL数据库和直接相关进程的用户。此用户不得拥有系统的管理权限。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/changing-mysql-user.html
2. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_user

1.3 禁用MySQL命令历史记录(Scored)

适用性:

- Level 2 - MySQL RDBMS on Linux

描述:

在Linux/UNIX上，MySQL客户端将以交互方式执行的语句记录到历史文件中。默认情况下，此文件在用户的主目录中名为.mysql_history。在MySQL客户端应用程序中运行的大多数交互式命令都保存到历史文件中。应禁用MySQL命令历史记录。

解释:

禁用MySQL命令历史记录可降低泄露敏感信息（如密码和加密密钥）的可能性。

审计:

执行以下命令以评估此建议：

```
find /home -name ".mysql_history"
find /root -name ".mysql_history"
```

对于返回的每个文件，确定该文件是否符号链接(软链接)到 /dev/null。

修复:

执行以下步骤以修复此设置：

1. 删除.mysql_history（如果存在）。
2. 使用以下任一技术防止再次创建它：
    1. 将MYSQL_HISTFILE环境变量设置为/dev/null。这将需要放在shell的启动脚本中。
    2. 创建并将$HOME/.mysql_history 软链接到 /dev/null 。

```
> ln -s /dev/null $HOME/.mysql_history
```

默认值:

默认情况下，MySQL命令历史记录文件位于$HOME/.mysql_history文件。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/mysql-logging.html
2. http://bugs.mysql.com/bug.php?id=72158

1.4 验证“MYSQL_PWD”没有设置(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以从名为 `MYSQL_PWD` 的环境变量中读取默认数据库密码。避免使用此环境变量可以更好地保护MySQL凭据的机密性。

解释:

使用MYSQL_PWD环境变量意味着MySQL凭据的明文存储。 避免这种情况发生，保证MYSQL_PWD的机密性。

审计:

要评估此建议，使用/proc文件中确定当前是否为任何进程设置了MYSQL_PWD

```
grep MYSQL_PWD /proc/*/environ
```

这可能会返回执行grep命令的进程的一个条目。

修复:

检查哪些用户和(或)脚本设置了MYSQL_PWD，并使用更安全的方法更改它们。

默认值:

未设置。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/environment-variables.html
2. https://blogs.oracle.com/myoracklediary/entry/how_to_check_environment_variables

1.5 禁用交互式登录(Scored)

适用性:

- Level 2 - MySQL RDBMS on Linux

描述:

创建MySQL用户时可以对操作系统进行交互式访问，这意味着MySQL用户可以像任何其他用户一样登录到主机。

解释:

阻止MySQL用户以交互方式登录可以减少受害MySQL帐户的影响。访问MySQL服务器所在的操作系统将需要用户自己的帐户，因此还有更多的问责制。MySQL用户的交互式访问是不必要的，应该被禁用。

审计:

执行以下命令以评估此建议

```
getent passwd mysql | egrep "^.*[\/bin\/false|\/sbin\/nologin]$"
```

如果没有输出则意味着一个漏洞发现。

修复:

执行以下步骤以修复此设置:

- 在终端中执行以下命令之一

```
usermod -s /bin/false mysql
usermod -s /sbin/nologin mysql
```

影响:

此设置将阻止MySQL管理员使用MySQL用户以交互方式登录操作系统。相反，管理员需要使用自己的帐户登录。

1.6 验证用户配置文件中未设置“MYSQL_PWD”(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以从名为MYSQL_PWD的环境变量中读取默认数据库密码
解释:

使用MYSQL_PWD环境变量意味着MySQL凭据的明文存储。 避免这种情况可能会增加保证MySQL凭据的机密性得以保留。
审计:

使用以下命令检查登录脚本中是否设置了MYSQL_PWD：

```
grep MYSQL_PWD /home/*/.{bashrc,profile,bash_profile}
```

修复:

检查哪些用户和脚本正在设置MYSQL_PWD，并更改它们以使用更安全的方法。

默认值:

未设置

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/environment-variables.html
2. https://blogs.oracle.com/myoraclediary/entry/how_to_check_environment_variables

2 安装和规划

本节包含将MySQL服务部署到生产网络时需注意的重要事项。此处提出的建议不是从基准(CIS)角度进行评分，只是与通常大多数控制框架中的最佳实践保持一致。

另请注意，可以通过两种方式添加配置选项。首先使用MySQL配置文件（例如my.cnf）并在 [mysqld] 的正确部分下放置选项。放置在配置文件中的选项不应以双短划线“--”作为前缀。也可以通过修改MySQL启动脚本将选项放在命令行上。启动脚本取决于您的操作系统。

2.1 备份和恢复

本节包含与备份和恢复相关的建议

2.1.1 备份策略(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

应具备备份策略和恢复计划。

解释:

应该有一个备份策略。备份MySQL数据库，包括'mysql'，将有助于确保在发生事件时保证数据的可用性。

审计:

如果有备份计划，请使用“crontab -l”进行检查。

修复:

创建备份策略和备份计划。

影响:

没有备份，可能很难从事件中恢复。

2.1.2 验证备份是否正常(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

备份应定期验证。

解释:

验证备份是否正常进行将有助于确保在发生事件时数据的可用性。

审计:

检查备份验证测试的报告。

修复:

实施定期备份并检查。

影响:

如果备份的数据不正确，其中包含错误或不包含必需数据，则可能很难从事件中恢复。

2.1.3 安全备份凭据(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

应保护密码，证书和任何其他凭据。

解释:

备份需要具有执行备份所需的最少权限的数据库用户。 应保护此用户的凭据。

审计:

检查包含密码和 ssl密钥的文件的权限。

修复:

更改文件权限

影响:

如果备份凭据未得到适当保护，则可能会滥用它们以获取对服务器的访问权限。 备份用户需要具有许多权限的帐户，因此攻击者可以获得（几乎）完全访问服务器的权限。

2.1.4 应妥善保护备份(Not Scored)

适用性适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

备份文件将包含数据库中的所有数据。 应使用文件系统权限和/或加密来防止非授权用户获得对备份的访问权限。

解释:

备份应被视为敏感信息。

审计:

检查谁有权访问备份文件。

- 文件是否全员可读(e.g. rw-r--r-)
  - 它们是否存储在全员可读目录中?
- IMySQL备份组是否具体?
  - 如果不是：文件和目录不能是组可读的
- 备份是否异地存储
  - 谁有权访问备份?
- 备份是否加密?
  - 加密秘钥存储在哪?
  - 加密秘钥是否包含易猜解密码

修复:

实施加密或使用文件系统权限。

影响:

如果未经授权的用户可以访问备份，则他们可以访问数据库中的所有数据。 如果加密密钥与备份一起存储，则对于未加密的备份和加密备份都是如此。

2.1.5 时间点恢复(Not Scored)

适用性:

- Level 2 - MySQL RDBMS on Linux

描述:

使用binlogs可以实现时间点恢复。 这样就可以恢复上次完整备份和时间点之间的更

启用binlog是不够的，应该创建还原过程并且必须进行测试。

解释:

这可以减少丢失的信息量。

审计:

检查是否已启用binlog以及是否存在还原过程。

修复:

启用binlog并创建和测试还原过程。

影响:

如果没有时间点恢复，则在上次备份和灾难发生之间存储的数据可能无法恢复。

2.1.6 灾难恢复计划 (Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

应该创建灾难恢复计划。

可以使用不同数据中心或异地备份。 应该有关于恢复将花费多少时间以及恢复站点是否具有完整的信息。

解释:

应该具有灾难恢复计划

审计:

检查是否有灾难恢复计划

修复:

创建灾难恢复计划

影响:

如果没有经过充分测试的灾难恢复计划，可能无法及时恢复。

2.1.7 备份配置和相关文件(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

备份应包含以下文件:

- 配置文件 (`my.cnf` and included files)
- SSL 文件(certificates, keys)
- 用户定义函数 (UDFs)
- 自定义源代码

解释:

这些文件必须能够完全还原实例。

审计:

检查这些文件是否已被使用并保存在备份中。

修复:

把这些文件加入到备份计划

影响:

如果没有完整备份这些文件，可能无法完全恢复。

2.2 专用机器运行MySQL(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述性:

建议将MySQL Server软件安装在专用服务器上。这种架构考虑提供了灵活性，因为数据库服务器可以放置在单独的划分区域上，只允许从特定主机和特定协议进行访问。

解释:

在底层操作系统，或仅安装了MySQL服务器软件以及可能另外安装的任何安全或操作工具的服务器上减少了攻击面。较小的攻击面可以降低MySQL中数据被泄露的可能性。

审计:

验证确认没有为底层操作系统启用其他角色，并且没有安装与MySQL服务器软件正常运行无关的其他应用程序或服务。

修复:

删除多余的应用程序或服务和（或）从底层操作系统中删除不必要的角色。

影响:

必须注意，不删除操作系统正常运行所需的应用程序或服务。

可能需要修改自定义应用程序以适应网络上的数据库连接，而不是使用（例如，使用TCP/IP连接）。可能需要额外的硬件和操作系统许可证才能进行体系架构更改。

2.3 不在命令行中指定密码 (Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

在命令行上执行命令时，例如mysql -u admin - ppassword，密码可能在用户的shell / 命令历史记录或进程列表中可见。

解释:

如果密码在进程列表或用户的shell 命令历史记录中可见，则攻击者将能够使用被盗凭证访问MySQL数据库。

审计:

如果密码可见，请检查进程或任务列表。

如果密码可见，请检查shell或命令历史记录。

修复:
使用`-p`参数后不填写密码（`>mysql -u admin – p[无密码]`），然后在出现提示时输入密码，使用正确安全的`.my.cnf`文件，或者在`.mylogin.cnf`中以加密格式存储认证信息。

影响:

根据所选的补救措施，可以需要采取以下措施：

- 出现提示时输入密码;
- 确保.my.cnf上的文件权限受限制，但用户可以访问;
- 使用mysql_config_editor加密身份验证凭据.mylogin.cnf。

此外，并非所有脚本/应用程序都可以使用.mylogin.cnf。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/mysql-config-editor.html
2. http://dev.mysql.com/doc/refman/5.6/en/password-security-user.html

2.4 不重复使用用户帐户 (Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

不应将数据库用户帐户重用于多个应用程序或用户。

解释:

在应用程序中使用唯一的数据库帐户将减少受害MySQL帐户的影响。

审计:

每个用户都应链接到以下其中一个
- 系统账户
- 一个人
- 一个应用程序(或数据库)

修复:

添加/删除用户，以便每个用户仅用于一个特定目的。

影响:

如果用户被重用，则该用户的风险将危及系统和多个应用程序。

2.5 不要使用默认或非MySQL指定的加密密钥 (Not Scored)

适用性:

- Level 2 - MySQL RDBMS on Linux

描述:

MySQL使用的SSL证书和密钥只能用于MySQL，并且只能用于一个实例。不应使用默认加密元素，因为其他人可能拥有它们的副本。

解释:

如果攻击者获得对共享加密材料（包括默认元素）的访问权限，则攻击者可以重复使用该元素来模拟MySQL服务器或以其他方式破坏其操作。

审计:

检查证书是否只用于一个MySQL实例。

修复:

为每个MySQL实例生成新的证书/密钥。

影响:

如果在多个系统上使用相同的密钥，则对一个系统的危害会导致使用相同密钥的所有服务器受到损害。

3 文件权限和所有权

文件权限和所有权设置对于保持MySQL服务器的数据和配置安全至关重要。

3.1 确保'datadir'具有合适的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

此数据目录是MySQL数据库的存放位置。

解释:

限制这些文件对象的可访问权限将保护MySQL数据库的机密性，完整性和可用性。如果允许MySQL用户以外的其他人可以从数据目录中读取文件，则他（她）可能能够从包含密码的mysql.user表中读取数据。此外，可创建文件的权限可能导致拒绝服务，或者可能通过手动创建具有视图定义的文件来允许某人访问特定数据。

审计:

执行以下步骤以评估此建议：

- 执行以下SQL语句以确定datadir的值

```
show variables where variable_name = 'datadir';
```

- 在终端提示符处执行以下命令

```
ls -l <datadir>/.. | egrep "^d[r|w|x]{3}------\s*.\s*mysql\s*mysql\s*\d*.*mysql"
```

如果没有返回提示，则这是个漏洞发现。

修复:

在终端提示符处执行以下命令：

```
chmod 700 <datadir>
chown mysql:mysql <datadir>
```

3.2 确保'log_bin_basename'文件具有合适的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以使用各种日志文件进行取证操作，每个日志文件用于不同的目的。这些日志可能是二进制日志，错误日志，慢查询日志，中继日志和常规日志。因为这些是主机操作系统上的文件，所以它们受主机提供的权限和所有权结构的约束，并且可以由MySQL用户以外的用户访问。

解释:

限制对这些对象的可访问权限，将保护MySQL日志的机密性，完整性和可用性。

审计:

执行以下步骤以评估此建议：

- 执行以下SQL语句以确定log_bin_basename的值

```
show variables like 'log_bin_basename';
```

- 对于表单的每个日志文件，mysql：mysql的验证权限为660

修复:

对需要更正权限和所有权的每个日志文件位置执行以下命令：

```
 chmod 660 <log file>
 chown mysql:mysql <log file>
```

影响:

更改日志文件的权限和所有权可能会影响使用日志文件适配器的监控工具。

如果意外更改了用于运行MySQL服务的用户帐户的二进制日志文件的权限，则可能会破坏使用。

二进制日志文件可用于即时恢复，因此这也会影响备份、还原和灾难恢复过程。

3.3 确保'log_error'具有合适的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以使用各种日志文件进行取证操作，每个日志文件用于不同的目的。这些可能是二进制日志，错误日志，慢查询日志，中继日志，审核日志和常规日志。因为这些是主机操作系统上的文件，所以它们受主机提供的权限和所有权结构的约束，并且可以由MySQL用户以外的用户访问。

解释:

限制对这些对象的可访问权限，将保护MySQL日志的机密性，完整性和可用性。

审计:

P执行以下步骤以评估此建议：

- 执行以下SQL语句以确定log_error的值

```
show variables like 'log_error';
```

- 在终端提示符处执行以下命令以列出所有log_error.*文件

修复:

对于列出的每个文件，执行以下命令

```
 chmod 660 <log file>
 chown mysql:mysql <log file>
```

影响:

更改日志文件的权限可能会影响使用日志文件适配器的监视工具的正常工作。 此外，slow_query_log可用于应用程序开发人员的性能分析。

如果意外更改了中继日志和二进制日志文件的权限以排除用于运行MySQL服务的用户帐户，则可能会破坏复制。

二进制日志文件可用于即时恢复，因此这也会影响备份，还原和灾难恢复过程。

3.4 确保'slow_query_log'具有合适的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以使用各种日志文件进行操作，每个日志文件用于不同的目的。 这些是二进制日志，错误日志，慢查询日志，中继日志和常规日志。 因为这些是主机操作系统上的文件，所以它们受主机提供的权限结构的约束，并且可以由MySQL用户以外的用户访问。

解释:

限制对这些对象的可访问权限，将保护MySQL日志的机密性，完整性和可用性。

审计:

执行以下步骤以评估此建议：

- 执行以下SQL语句以确定slow_query_log_file的值

```
show variables like 'slow_query_log_file';
```

- 对于<slow_query_log_path>，验证权限为应为660

修复:

对需要更正权限和所有权的每个日志文件位置执行以下命令：

```
chmod 660 <log file>
chown mysql:mysql <log file>
```

影响:

更改日志文件的权限可能会影响使用日志文件适配器的监视工具。 此外，slow_query_log可用于应用程序开发人员的性能分析。

如果意外更改了中继日志和二进制日志文件的权限以排除用于运行MySQL服务的用户帐户，则可能会破坏复制。

二进制日志文件可用于即时恢复，因此这也会影响备份，还原和灾难恢复过程。

3.5 确保'relay_log_basename'文件具有适当的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以使用各种日志文件进行操作，每个日志文件用于不同的目的。 这些是二进制日志，错误日志，慢查询日志，中继日志和常规日志。 因为这些是主机操作系统上的文件，所以它们受主机提供的权限结构的约束，并且可以由MySQL用户以外的用户访问。

解释:

限制对这些对象的可访问权限，将保护MySQL日志的机密性，完整性和可用性。

审计:

执行以下步骤以评估此建议：

通过执行以下语句查找relay_log_basename值

```
show variables like 'relay_log_basename';
```

- 对于<Relay_log_path>，验证权限为应为660

修复:

对需要更正权限和所有权的每个日志文件位置执行以下命令：

```
chmod 660 <log file>
chown mysql:mysql <log file>
```

影响:

更改日志文件的权限可能会影响使用日志文件适配器的监视工具。 此外，slow_query_log可用于应用程序开发人员的性能分析。

如果意外更改了中继日志和二进制日志文件的权限以排除用于运行MySQL服务的用户帐户，则可能会破坏复制。

二进制日志文件可用于即时恢复，因此这也会影响备份，还原和灾难恢复过程。

3.6 确保'general_log_file'具有适当的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL可以使用各种日志文件进行取证操作，每个日志文件用于不同的目的。这些可能是二进制日志，错误日志，慢查询日志，中继日志，审核日志和常规日志。因为这些是主机操作系统上的文件，所以它们受主机提供的权限和所有权结构的约束，并且可以由MySQL用户以外的用户访问。

解释:

限制对这些对象的可访问权限，将保护MySQL日志的机密性，完整性和可用性。

审计:

执行以下步骤以评估此建议：

- 执行以下SQL语句以确定general_log_file的值

```
show variables like 'general_log_file';
```

- 对于<Relay_log_path>，验证权限为应为660

修复:

对需要更正权限和所有权的每个日志文件位置执行以下命令：

```
chmod 660 <log file>
chown mysql:mysql <log file>
```

影响:

更改日志文件的权限可能会影响使用日志文件适配器的监视工具。 此外，slow_query_log可用于应用程序开发人员的性能分析。

如果意外更改了中继日志和二进制日志文件的权限以排除用于运行MySQL服务的用户帐户，则可能会破坏复制。

二进制日志文件可用于即时恢复，因此这也会影响备份，还原和灾难恢复过程。

3.7 确保SSL密钥文件具有适当的权限和所有权 (Scored)

适用性：

- Level 1 - MySQL RDBMS on Linux

描述：

当配置为使用SSL/TLS时，MySQL依赖于密钥文件，这些密钥文件存储在主机的文件系统中。这些密钥文件受主机的权限和所有权结构的约束。

解释：

限制对这些对象的可访问权限，将保护MySQL数据库的机密性、完整性和可用性以及与客户端的通信。

如果攻击者知道SSL密钥文件的内容，则他或她可能会冒充服务器，用于中间人攻击。

根据SSL密码套件，密钥也可用于解密先前捕获的网络流量。

审计：

要评估此建议，请通过执行以下SQL语句找到正在使用的SSL密钥以获取ssl_key的值：

```
show variables where variable_name = 'ssl_key';
```

然后，执行以下命令以评估Value的权限：

```
 ls -l <ssl_key Value> | egrep "^-r--------[ \t]*.[ \t]*mysql[ \t]*mysql.*$"
```

如果没有任何返回行，那么这是一个漏洞发现。

修复：

在终端提示符处执行以下命令，以使用上述审计过程中的值修复这些设置：

```
 chown mysql:mysql <ssl_key Value>
 chmod 400 <ssl_key Value>
```

影响：

如果密钥文件的权限或所有权更改不正确，则可能导致在重新启动MySQL时禁用SSL，或者可能导致MySQL根本无法启动。

如果其他应用程序使用相同的密钥对，则更改密钥文件的权限或所有权将影响此应用程

序。如果是这种情况，则必须为MySQL生成新的密钥对。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/ssl-connections.html

3.8 确保插件目录具有适当的权限和所有权 (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

插件目录是MySQL插件的存储位置。插件是存储引擎或用户定义的函数（UDFs）

解释:

限制对这些对象的可访问权限，将保护MySQL数据库的机密性，完整性和可用性。如果有人可以修改插件，那么当服务器启动并且代码被执行时，可能会加载这些插件。

审计:

要评估此建议，请执行以下SQL语句以查找plugin_dir的值

```
show variables where variable_name = 'plugin_dir';
```

然后，在终端提示符下执行以下命令（使用查找的plugin_dir值）来确定权限和所有权。

```
ls -l <plugin_dir Value>/.. | egrep "^drwxr[-w]xr[-w]x[ \t]*[0-9][ \t]*mysql[
\t]*mysql.*plugin.*$"
```

没有输出返回行，则这是一个漏洞发现

注意:权限应为775或755。

修复:

要修复这些设置，请使用审计过程中的 `plugin_dir Value` 值在终端提示符处执行以下命令。

```
chmod 775 <plugin_dir Value> (or use 755)
chown mysql:mysql <plugin_dir Value>
```

影响:

mysql用户以外的用户将无法再更新和添加/删除插件，除非他们能够切换到mysql用户。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/install-plugin.html

4 通用

本节包含与数据库服务器相关的各个部分相关的建议。

4.1 确保应用最新安全补丁(Not Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

定期更新至发布的MySQL服务器新版本，以解决漏洞，缓解漏洞并提供新功能。建议MySQL及时安装最新的安全补丁。

解释:

使用MySQL补丁更新维护，将有助于降低与MySQL服务器中存在的已知漏洞相关的风险。

如果没有最新的安全补丁，MySQL会知道可能被攻击者用来获取访问权限的已知漏洞。

审计:

执行以下SQL语句以标识MySQL服务器版本：

```
SHOW VARIABLES WHERE Variable_name LIKE "version";
```

现在将版本与Oracle和（或）主机OS的安全公告进行比较（如果使用主机默认OS软件包）。

修复:

安装适用于您的版本的最新修补程序或升级到最新版本。

影响:

要更新MySQL服务器，需要重新启动。

参考文献:

1. http://www.oracle.com/technetwork/topics/security/alerts-086861.html
2. http://dev.mysql.com/doc/relnotes/mysql/5.6/en/
3. https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&query=mysql&search_type=all

4.2 确保未安装“test”数据库 (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

默认的MySQL安装附带一个名为test的未使用的数据库。建议删除测试数据库。

解释:

所有用户都可以访问测试数据库，并可以使用它来消耗系统资源。删除测试数据库将减少MySQL服务器的攻击面。

审计:

Execute the following SQL statement to determine if the test database is present:

```
SHOW DATABASES LIKE 'test';
```

The above SQL statement will return zero rows

修复:

执行以下SQL语句以确定测试数据库是否存在：

```
DROP DATABASE "test";
```

注意: mysql_secure_installation执行此操作以及其他与安全相关的活动。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/mysql-secure-installation.html

4.3 验证'allow-suspicious-udfs'设置为'FALSE' (Scored)

适用性:

- Level 2 - MySQL RDBMS

描述:

此选项通过检查至少一个名为`_init`, `_deinit`, `_reset`, `_clear`, 或 `_add`的相应方法，防止将任意共享库函数作为用户定义函数附加。

解释:

防止加载不包含用户定义函数的共享库将减少服务器的攻击面。

审计:

P执行以下操作以确定建议的状态是否到位:

- E确保在mysqld启动命令行中未指定 --allow-suspicious-udfs 。
- 确保在MySQL配置中将allow-suspicious-udfs设置为FALSE:
- `my_print_defaults mysqld | grep allow-suspicious-udfs`

  没有返回行证明配置无误。

修复:

执行以下操作以建立建议的状态:

- 从mysqld启动命令行中删除--allow-suspicious-udfs。
- 从MySQL选项文件中删除allow-suspicious-udfs。

默认值:

`FALSE`

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/udf-security.html
2. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_allow-suspicious-udfs

4.4 验证“local_infile”已禁用 (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

local_infile参数指示是否可以通过LOAD DATA INFILE或SELECT local_file加载或选择位于MySQL客户端计算机上的文件。

解释:

local_infile参数指示是否可以通过LOAD DATA INFILE或SELECT local_file加载或选择位于MySQL客户端计算机上的文件。

审计:

执行以下SQL语句并确保Value字段设置为OFF:

```
SHOW VARIABLES WHERE Variable_name = 'local_infile';
```

修复:

将以下行添加到MySQL配置文件的[mysqld]部分并重新启动MySQL服务:

```
local-infile=0
```

影响:

禁用local_infile将影响依赖它的解决方案的功能。

默认值:

ON

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/string-functions.html#function_load-file
2. http://dev.mysql.com/doc/refman/5.6/en/load-data.html

4.5 验证'mysqld'未启动--skip-grant-tables'(Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

此选项使mysqld在不使用权限系统的情况下启动。

解释:

如果使用此选项，则受影响服务器的所有客户端都将具有对所有数据库的不受限制的访问权限。

审计:

执行以下操作以确定建议的状态是否到位：

- 打开MySQL配置（例如`my.cnf`）文件并搜索`skip-grant-tables`
- 确保`skip-grant-tables`设置为FALSE

修复:

执行以下操作以建立建议状态：

- 打开MySQL配置（例如my.cnf）文件并设置：

```
skip-grant-tables = FALSE
```

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_skip-grant-tables

4.6 确保启用“--skip-symbolic-links”(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

MySQL的symbolic-links和skip-symbolic-links选项确定符号链接（软链）支持是否可用。启用符号链接时，它们具有不同的效果，具体取决于主机平台。禁用符号链接时，数据库不会使用存储在文件中的符号链接或表中的条目。

解释：

防止sym链接用于数据库文件。当MySQL以root身份执行时，这一点尤为重要，因为任意文件都可能被覆盖。symbolic-links选项可能允许某人将对MySQL服务器的操作指向其他文件和/或目录。

审计：

执行以下SQL语句来评估此建议：

```
SHOW variables LIKE 'have_symlink';
```

确保返回的值为DISABLED。

修复：

执行以下操作以修复此设置：

- 打开MySQL配置文件（my.cnf）
- 在配置中找到skip_symbolic_links
- 将skip_symbolic_links设置为YES

注意：如果skip_symbolic_links不存在，请将其添加到[mysqld]部分的配置文件中。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/symbolic-links.html
2. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_symbolic-links

4.7 确保禁用'daemon_memcached'插件 (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

InnoDB memcached插件允许用户使用memcached协议访问存储在InnoDB中的数据。

解释:

默认情况下，插件不进行身份验证，这意味着任何有权访问插件的TCP / IP端口的人都可以访问和修改数据。但是，并非所有数据都默认公开。

审计:

执行以下SQL语句来评估此建议：

```
SELECT * FROM information_schema.plugins WHERE PLUGIN_NAME='daemon_memcached'
```

确保没有返回

修复:

要修复此设置，请在MySQL命令行中执行以下命令：

```
uninstall plugin daemon_memcached;
```

这将从MySQL服务器卸载memcached插件。

默认值:

disabled

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/innodb-memcached-security.html

4.8 确保'secure_file_priv'不为空(Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

secure_file_priv选项限制为LOAD DATA INFILE或SELECT local_file使用的路径。建议将此选项设置为仅包含预期由MySQL加载的资源的文件系统位置。

解释:

设置secure_file_priv可降低攻击者通过SQL注入漏洞从受影响的服务器读取敏感文件的能力。

审计:

执行以下SQL语句并确保返回一行:

```
SHOW GLOBAL VARIABLES WHERE Variable_name = 'secure_file_priv' AND Value<>'';
```

注意: Value应包含有效路径。

修复:

将以下行添加到MySQL配置文件的[mysqld]部分并重新启动MySQL服务:

```
secure_file_priv=<path_to_load_directory>
```

影响:

依赖于从各个子目录加载数据的解决方案可能会受到此更改的负面影响。考虑在公共父目录下合并加载目录。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/server-system-variables.html#sysvar_secure_file_priv

4.9 确保'sql_mode'包含'STRICT_ALL_TABLES' (Scored)

适用性:

- Level 2 - MySQL RDBMS

描述:

当进行数据更改语句（即INSERT，UPDATE）时，MySQL可以不同地处理无效或缺失值，具体取决于是否启用了严格的SQL模式。启用严格SQL模式时，可能不会截断数据或以其他方式“调整”数据以使数据更改语句起作用。

解释:

如果没有严格模式，服务器会尝试在错误可能是更安全的选择时继续执行操作。例如，默认情况下，如果数据不适合某个字段，MySQL将截断数据，这可能导致未知行为，或者被攻击者利用来绕过数据验证。

审计:

要审核此建议，请执行以下查询：

```
SHOW VARIABLES LIKE 'sql_mode';
```

确保STRICT_ALL_TABLES位于返回的列表中。

修复:

执行以下操作以修复此设置：

1. 将STRICT_ALL_TABLES添加到服务器配置文件中的sql_mode

影响:

依赖于MySQL数据库的应用程序应该知道正在使用STRICT_ALL_TABLES，以便正确处理错误条件。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/server-sql-mode.html

5 MySQL 权限

本节包含有关用户权限的建议。

5.1 确保仅管理用户具有完全数据库访问权限(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

Mysql.user和mysql.db表列出了可以向MySQL用户授予（或拒绝）的各种权限。一些关注的特权包括：Select_priv，Insert_priv，Update_priv，Delete_priv，Drop_priv等。通常，这些权限不应该对每个MySQL用户可用，并且通常仅保留用于管理用途。

解释：

限制“mysql”数据库的可访问性将保护MySQL内部数据的机密性，完整性和可用性。直接访问mysql。*的用户可能会有意或无意地查看密码哈希，更改权限或更改或破坏信息。

审计：

执行以下SQL语句来评估此建议：

```
SELECT user, host
FROM mysql.user
WHERE (Select_priv = 'Y')
 OR (Insert_priv = 'Y')
 OR (Update_priv = 'Y')
 OR (Delete_priv = 'Y')
 OR (Create_priv = 'Y')
 OR (Drop_priv = 'Y');
```

```
SELECT user, host
FROM mysql.db
WHERE db = 'mysql'
  AND ((Select_priv = 'Y')
    OR (Insert_priv = 'Y')
    OR (Update_priv = 'Y')
    OR (Delete_priv = 'Y')
    OR (Create_priv = 'Y')
 OR (Drop_priv = 'Y'));
```

确保返回的所有用户都是管理用户。

修复：

执行以下操作以修复此设置：

1. 枚举审计程序产生的非管理用户
2. 对于每个非管理用户，请使用REVOKE语句根据需要删除权限

影响：

应考虑每个需要交互式数据库访问的用户需要哪些权限。

5.2 确保非管理用户的“file_priv”未设置为“Y”(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

Mysql.user表中的File_priv特权用于允许或禁止用户在服务器主机上读写文件。授予File_priv权限的任何用户都有能力：

- 从MySQL服务器读取本地文件系统中的文件（包括世界可读文件）
- 将文件写入MySQL服务器具有写访问权限的本地文件系统

解释：

File_priv权限允许mysql用户从磁盘读取文件并将文件写入磁盘。攻击者可能利用这一点来进一步破坏MySQL。应该注意，MySQL服务器不应该覆盖现有文件。

审计：

执行以下SQL语句以审核此设置

```
select user, host from mysql.user where File_priv = 'Y';
```

确保仅在结果集中返回管理用户。

修复：

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户：

```
REVOKE FILE ON *.* FROM '<user>';
```

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_file

5.3 确保非管理用户的“process_priv”未设置为“Y”(Scored)

适用性:

- Level 2 - MySQL RDBMS

描述:

mysql.user表中的PROCESS权限确定给定用户是否可以查看所有会话的语句执行信息。

解释:

PROCESS特权允许委托人查看当前正在执行的MySQL语句，包括用于管理密码的语句。攻击者可以利用这一点来破坏MySQL或获取对潜在敏感数据的访问权限。

审计:

执行以下SQL语句以审核此设置：

```
select user, host from mysql.user where Process_priv = 'Y';
```

确保仅在结果集中返回管理用户。

修复:

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户：

```
REVOKE PROCESS ON *.* FROM '<user>';
```

影响:

拒绝使用PROCESS权限的用户也可能被拒绝使用SHOW ENGINE。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_process

5.4 确保非管理用户的“super_priv”未设置为“Y” (Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

Mysql.user表中的SUPER权限控制着各种MySQL功能的使用。这些功能包括，CHANGE MASTER TO，KILL，mysqladmin kill选项，PURGE BINARY LOGS，SET GLOBAL，mysqladmin调试选项，日志记录控制等。

解释：

SUPER权限允许主体执行许多操作，包括查看和终止当前正在执行的MySQL语句（包括用于管理密码的语句）。此权限还提供配置MySQL的功能，例如启用/禁用日志记录，更改数据，禁用/启用功能。限制具有SUPER权限的帐户可以降低攻击者利用这些功能的可能性。

审计：

执行以下SQL语句以审核此设置：

```
select user, host from mysql.user where Super_priv = 'Y';
```

确保仅在结果集中返回管理用户。

修复：

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户：

```
REVOKE SUPER ON *.* FROM '<user>';
```

影响：

当SUPER权限被拒绝给定用户时，该用户将无法利用某些功能，例如某些mysqladmin选项。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_super

5.5 确保非管理用户的“shutdown_priv”未设置为“Y” (Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

SHUTDOWN权限只允许使用mysqladmin命令的shutdown选项，该命令允许具有SHUTDOWN权限的用户关闭MySQL服务器。

解释：

SHUTDOWN权限允许主体关闭MySQL。攻击者可能会利用这一点来对MySQL的可用性产生负面影响。

审计：

执行以下SQL语句以审核此设置：

```
SELECT user, host FROM mysql.user WHERE Shutdown_priv = 'Y';
```

确保返回结果中仅包含管理用户。

修复：

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户）：

```
REVOKE SHUTDOWN ON *.* FROM '<user>';
```

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_shutdown

5.6 确保非管理用户的“create_user_priv”未设置为“Y”(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

CREATE USER权限控制给定用户添加或删除用户，更改现有用户名称或撤消现有用户权限的权限。

解释：

减少授予CREATE USER权限的用户数量可以最大限度地减少能够添加/删除用户，更改现有用户名称和操纵现有用户权限的用户数量。

审计：

执行以下SQL语句以审核此设置：

```
SELECT user, host FROM mysql.user WHERE Create_user_priv = 'Y';
```

确保仅在结果集中返回管理用户。

修复：

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户）：

```
REVOKE CREATE USER ON *.* FROM '<user>';
```

影响：

被拒绝CREATE USER权限的用户不仅无法创建用户，而且他们可能无法删除用户，重命名用户或以其他方式撤消给定用户的权限。

5.7 确保非管理用户的“grant_priv”未设置为“Y”(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

GRANT OPTION权限存在于不同的上下文（mysql.user，mysql.db）中，目的是管理特权用户操纵其他用户权限的能力。

解释：

GRANT权限允许委托人授予其他委托人额外的权限。攻击者可能会使用它来破坏MySQL。

审计：

执行以下SQL语句以审核此设置：

```
SELECT user, host FROM mysql.user WHERE Grant_priv = 'Y';
SELECT user, host FROM mysql.db WHERE Grant_priv = 'Y';
```

确保仅在结果集中返回管理用户。

修复：

执行以下步骤以修复此设置：

1. 枚举审计过程结果集中的非管理用户
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为非管理用户：

```
REVOKE GRANT OPTION ON *.* FROM <user>;
```

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_grant-option

5.8 确保非从属用户'repl_slave_priv'未设置为'Y' (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

REPLICATION SLAVE特权控制给定用户（在主服务器的上下文中）是否可以请求在主服务器上进行的更新。

解释:

REPLICATION SLAVE特权允许主体获取包含所有数据更改语句和/或来自主数据库的表数据更改的binlog文件。攻击者可以使用它来从MySQL读取/获取敏感数据。

审计:

执行以下SQL语句以审核此设置：

```
SELECT user, host FROM mysql.user WHERE Repl_slave_priv = 'Y';
```

确保仅为从属用户指定的帐户被授予此权限。

修复:

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的非从属用户
2. 对于每个用户，发出以下SQL语句（将"<user>"替换为非从属用户）：

```
REVOKE REPLICATION SLAVE ON *.* FROM <user>;
```

使用REVOKE语句从不应拥有它的用户中删除SUPER权限。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_replication-slave

5.9 确保DML/DDL授权仅限于特定数据库和用户(Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

DML/DDL包括用于修改或创建数据结构的一组权限。这包括INSERT，SELECT，UPDATE，DELETE，DROP，CREATE和ALTER权限。

解释：

INSERT，SELECT，UPDATE，DELETE，DROP，CREATE和ALTER在任何数据库中具有强大权限。此类特权应仅限于需要此类权利的用户。通过限制具有这些权限的用户并确保它们仅限于特定数据库，减少了数据库的攻击面。

审计：

执行以下SQL语句以审核此设置：

```
SELECT User,Host,Db
FROM mysql.db
WHERE Select_priv='Y'
  OR Insert_priv='Y'
  OR Update_priv='Y'
  OR Delete_priv='Y'
  OR Create_priv='Y'
  OR Drop_priv='Y'
 OR Alter_priv='Y';
```

确保返回的所有用户都应在指定的数据库上具有这些权限。

修复：

执行以下步骤以修复此设置：

1. 枚举审计过程结果集中返回的未授权用户，主机和数据库
2. 对于每个用户，发出以下SQL语句（将“<user>”替换为未授权用户，将“<host>”替换为主机名，将“<database>”替换为数据库名称）：

```
 REVOKE SELECT ON <host>.<database> FROM <user>;
 REVOKE INSERT ON <host>.<database> FROM <user>;
 REVOKE UPDATE ON <host>.<database> FROM <user>;
 REVOKE DELETE ON <host>.<database> FROM <user>;
 REVOKE CREATE ON <host>.<database> FROM <user>;
 REVOKE DROP ON <host>.<database> FROM <user>;
 REVOKE ALTER ON <host>.<database> FROM <user>;
```

6 审计和记录

本节提供有关MySQL日志记录行为的指导。

6.1 确保'log_error'不为空(Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

错误日志包含有关事件的信息，例如mysqld启动和停止，需要检查或修复表时，以及根据主机操作系统，mysqld失败时的堆栈跟踪。

解释:

启用错误日志记录可以提高检测针对MySQL和其他关键消息的恶意企图的能力，例如，如果未启用错误日志，则可能不会注意到连接错误。

审计:

执行以下SQL语句以审核此设置：

```
SHOW variables LIKE 'log_error';
```

确保返回的值不为空。

修复:

执行以下操作以修复此设置：

1. 打开MySQL配置文件（my.cnf或my.ini）
2. 将log-error选项设置为错误日志的路径

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/error-log.html

6.2 确保日志文件存储在非系统分区上(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:

MySQL日志文件可以在MySQL配置中设置，以存在于文件系统的任何位置。通常的做法是确保系统文件系统不被应用程序日志整理。系统文件系统包括root，/var或/usr。

解释:

将MySQL日志从系统分区移出将通过耗尽操作系统的可用磁盘空间来降低拒绝服务的可能性。

审计:

执行以下SQL语句来评估此建议：

```
SELECT @@global.log_bin_basename;
```

确保返回的值不表示root（'/'），/var或/usr。

修复:

执行以下操作以修复此设置：

1. 打开MySQL配置文件（my.cnf）
2. 找到log-bin条目并将其设置为不在root（'/'），/ var或/ usr上的文件

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/binary-log.html
2. http://dev.mysql.com/doc/refman/5.6/en/replication-options-binary-log.html

6.3 确保'log_warnings'设置为'2' (Scored)

适用性:

- Level 2 - MySQL RDBMS

描述:

默认情况下启用的log_warnings系统变量为MySQL日志提供了附加信息。值1表示记录警告消息，较高的整数值倾向于启用更多日志记录。

注意：5.6.3及更早版本的变量范围是全局和会话，但对于5.6.4及更高版本，其范围是全局的。

解释:

这可能有助于通过记录通信错误和中止连接来检测恶意行为。

审计:

执行以下SQL语句来评估此建议:

```
SHOW GLOBAL VARIABLES LIKE 'log_warnings';
```

确保返回的值等于2。

修复:

执行以下操作以修复此设置:

- 打开MySQL配置文件（my.cnf）
- 确保在mysqld部分中找到以下行

```
log-warnings = 2
```

默认值:

默认情况下启用该选项为（1）。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_log-warnings

6.4 确保已启用审计日志记录(Not Scored)

适用性:

- Level 2 - MySQL RDBMS

描述:

审计日志并没有包含在MySQL的社区版中，只包含常规日志。 使用通用日志是可能的，但不实用，因为它会快速增长并对服务器性能产生负面影响。

尽管如此，启用审计日志记录是实际生产环境的需要重要考虑的因素，并且可以通过第三方工具来帮助实现这一点。 启用审计日志记录应包含以下内容

- 交互式用户会话
- 应用程序会话（可选）

解释:

审计日志有助于调查，确认事件发生的时间和由谁引发的事件。查看日志可以作为调查的证据。这也有助于确定攻击者造成了什么危害。

审计:

验证是否已安装并配置第三方工具以启用交互式用户会话和（可选）应用程序会话的日志记录。

修复:

从各种来源获取第三方MySQL日志记录解决方案，包括但不限于以下内容：

- 常规查询
- MySQL 企业 审计
- 适用于MySQL的MariaDB Audit插件
- McAfee MySQL 审计

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/query-log.html
2. http://dev.mysql.com/doc/refman/5.6/en/mysql-enterprise-audit.html
3. https://mariadb.com/kb/en/server_audit-mariadb-audit-plugin/
4. https://github.com/mcafee/mysql-audit

6.5 确保'log - raw'设置为OFF' (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

log-raw MySQL选项确定服务器是否重写密码，以便不以纯文本形式显示在日志文件中。如果启用了log-raw，则密码将以纯文本形式写入各种日志文件（通用查询日志，慢查询日志和二进制日志）。

解释:

通过密码的原始日志记录，有权访问日志文件的人可能会看到纯文本密码。

审计:

执行以下操作以评估此建议：

- 打开MySQL配置文件（my.cnf）
- 确保存在log-raw条目
- 确保将log-raw条目设置为OFF

修复:

执行以下操作以修复此设置：

- 打开MySQL配置文件（my.cnf）
- 查找log-raw条目并按如下所示进行设置

```
log-raw = OFF
```

默认值:

OFF

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/password-logging.html
2. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_log-raw

7 认证

本节包含与MySQL的身份验证机制相关的配置建议。

7.1 确保'old_passwords'未设置为'1' (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux

描述:
此变量控制PASSWORD（）函数使用的密码散列方法以及CREATE USER和GRANT语句的IDENTIFIED BY子句。
在5.6.6之前，该值可以是0（或OFF），或1（或ON）。 从5.6.6开始，以下值可以是以下值之一：

- 0 - 使用mysql_native_password插件进行身份验证
- 1 - 使用mysql_old_password插件进行身份验证
- 2 - 使用sha256_password插件进行身份验证

解释:

mysql_old_password插件利用了一种非常弱的哈希算法，可以使用离线字典攻击快速强制执行。有关其他详细信息，请参阅CVE-2003-1480。

审计:

执行以下SQL语句来评估此建议：

```
SHOW VARIABLES WHERE Variable_name = 'old_passwords';
```

确保返回值未设置为1或者on

修复:

配置mysql以利用mysql_native_password或sha256_password插件。有关更多信息，请参阅：

- http://dev.mysql.com/doc/refman/5.6/en/password-hashing.html
- http://dev.mysql.com/doc/refman/5.6/en/sha256-authentication-plugin.html

影响:

当old_passwords设置为1时，PASSWORD（）函数将使用非常弱的哈希算法创建密码哈希值，如果攻击者获得该哈希值可能很容易破解。

默认值：

0

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/server-system-variables.html#sysvar_old_passwords
2. CVE-2003-1480

7.2 确保'secure_auth'设置为'ON' (Scored)

适用性:

- Level 1 - MySQL RDBMS
- Level 2 - MySQL RDBMS

描述:

此选项指示服务器是否拒绝尝试使用以mysql_old_password格式存储其密码的帐户的客户端的连接。

解释:

启用此选项将阻止所有使用旧格式的密码（因此通过网络进行不安全的通信）。

审计:

执行以下SQL语句并确保Value字段未设置为ON： SHOW VARIABLES WHERE

Variable_name = 'secure_auth';

修复:

将以下行添加到MySQL选项文件的[mysqld]部分以建立建议状态：

```
secure_auth=ON
```

影响:

具有使用旧密码格式存储的凭据的帐户将无法登录。执行以下命令以标识将通过实施此设置而受影响的帐户：

```
SELECT User,Host FROM mysql.user WHERE plugin='mysql_old_password';
```

Default Value:

在MySQL 5.6.5之前，默认情况下禁用此选项。从MySQL 5.6.5开始，它默认启用;要禁用它，请使用`--skip-secure-auth`.

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/server-options.html#option_mysqld_secure-auth

7.3 确保全局配置中未存储密码(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux
- Level 2 - MySQL RDBMS on Linux

描述:

MySQL配置文件的[client]部分允许设置要使用用户和密码。验证全局配置文件（my.cnf）中未使用密码选项

解释:

密码参数的使用可能会对用户密码的机密性产生负面影响。

审计:

要评估此建议，请执行以下步骤：

- 打开MySQL配置文件（例如my.cnf）
- 检查MySQL配置文件的[client]部分，确保不使用密码。

修复:

使用mysql_config_editor以加密形式在.mylogin.cnf中存储身份验证凭据。

如果不可能，请使用特定于用户的选项文件.my.cnf。，并限制对用户标识的文件访问权限。

影响:

默认情况下，全局配置对系统上的所有用户都是可读的。这是全局默认值（提示，端口，套接字等）所必需的。如果此文件中存在密码，则系统上的所有用户都可以访问该密码。

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/mysql-config-editor.html

7.4 确保'sql_mode'包含'NO_AUTO_CREATE_USER' (Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux
- Level 2 - MySQL RDBMS on Linux
- Level 1 - MySQL RDBMS
- Level 2 - MySQL RDBMS

描述:

NO_AUTO_CREATE_USER是sql_mode的一个选项，可防止GRANT语句在未提供身份验证信息时自动创建用户。

解释:

空白密码否定了身份验证机制提供的好处。如果没有此设置，管理用户可能会在没有密码的情况下意外创建用户。

审计:

执行以下SQL语句来评估此建议：

```
SELECT @@global.sql_mode;
SELECT @@session.sql_mode;
```

确保每个结果包含NO_AUTO_CREATE_USER。

修复:

执行以下操作以修复此设置：

1. 打开MySQL配置文件（my.cnf）
2. 在[mysqld]区域中找到sql_mode设置
3. 将NO_AUTO_CREATE_USER添加到sql_mode设置

7.5 确保为所有MySQL帐户设置密码(Scored)

适用性：

- Level 1 - MySQL RDBMS
- Level 2 - MySQL RDBMS

描述：

空白密码允许用户在不使用密码的情况下登录。

解释：

如果没有密码，只知道用户名和允许的主机列表将允许某人连接到服务器并承担用户的身份。实际上，这绕过了认证机制。

审计：

执行以下SQL查询以确定是否有任何用户具有空密码：

```
SELECT User,host
FROM mysql.user
WHERE (plugin IN('mysql_native_password', 'mysql_old_password','')
 AND (LENGTH(Password) = 0
 OR Password IS NULL))
OR (plugin='sha256_password' AND LENGTH(authentication_string) = 0);
```

如果所有帐户都设置了密码，则不会返回任何行。

修复：

对于从审计过程返回的每一行，使用以下语句为给定用户设置密码（作为示例）：

```
SET PASSWORD FOR <user>@'<host>' = PASSWORD('<clear password>')
```

注意：使用适当的值替换<user>，<host>和<clear password>。

7.6 确保密码策略有效(Scored)

适用性:

- Level 1 - MySQL RDBMS on Linux
- Level 1 - MySQL RDBMS

描述:

密码复杂性包括密码特征如长度，大小写，长度和字符集。

解释:
复杂密码有助于缓解字典，暴力破解和其他密码攻击。此建议可防止用户选择容易被猜到的弱密码。

审计:

执行以下SQL语句来评估此建议:

```
SHOW VARIABLES LIKE 'validate_password%';
```

上述语句的结果集应显示:

- `validate_password_length` 应为14或更多
- `validate_password_mixed_case_count` 应为1或更多
- `validate_password_number_count` 应为1或更多
- `validate_password_special_char_count` 应为1或更多
- `validate_password_policy` 应为 `MEDIUM` 或 `STRONG`

全局配置中应包含:

```
plugin-load=validate_password.so
validate-password=FORCE_PLUS_PERMANENT
```

检查用户是否有与用户名相同的密码:

```
SELECT User,Password,Host FROM mysql.user
WHERE password=CONCAT('*', UPPER(SHA1(UNHEX(SHA1(user)))));
```

注意：此方法仅能够检查4.1之后的密码格式，该格式也被称为mysql_native_password。

修复:

添加到全局配置:

```
plugin-load=validate_password.so
validate-password=FORCE_PLUS_PERMANENT
validate_password_length=14
validate_password_mixed_case_count=1
validate_password_number_count=1
validate_password_special_char_count=1
validate_password_policy=MEDIUM
```

并为具有与其用户名相同的密码的用户更改密码。

影响：

此建议的修复需要重新启动服务器。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/validate-password-plugin.html

7.7 确保没有用户拥有通配符主机名(Scored)

适用性：

- Level 1 - MySQL RDBMS
- Level 2 - MySQL RDBMS

描述：

在向特定数据库上的用户授予权限时，MySQL可以使用主机通配符。例如，您可以将给定权限授予`'<user>'@'%'`。

解释：

避免在主机名中使用通配符有助于控制给定用户可以连接到数据库并与数据库交互的特定位置。

审计：

执行以下SQL语句来评估此建议：

```
SELECT user, host FROM mysql.user WHERE host = '%';
```

确保没有返回任何行。

修复：

执行以下操作以修复此设置：

1. 枚举运行审计程序后返回的所有用户
2. 将用户的主机更改为特定用户或DROP用户

7.8 确保没有匿名帐户存在(Scored)

适用性：

- Level 1 - MySQL RDBMS
- Level 2 - MySQL RDBMS

描述：

匿名帐户是具有空用户名（''）的用户。匿名帐户没有密码，因此任何人都可以使用它们连接到MySQL服务器。

解释：

删除匿名帐户有助于确保只有已识别和可信的主体才能与MySQL进行交互。

审计：

执行以下SQL查询以标识匿名帐户：

```
SELECT user,host FROM mysql.user WHERE user = '';
```

如果不存在匿名帐户，则上述查询将返回零行。

修复：

执行以下操作以修复此设置：

1. 枚举执行审计过程返回的匿名用户
2. 对于每个匿名用户，请DROP或为其指定名称

注意：作为替代方法，您可以执行mysql_secure_installation实用程序。

影响：

任何依赖于匿名数据库访问的应用程序都将受到此更改的不利影响。

默认值：

使用标准安装脚本mysql_install_db，它将创建两个匿名帐户：一个用于主机“localhost”，另一个用于网络接口的IP地址。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/mysql-secure-installation.html
2. https://dev.mysql.com/doc/refman/5.6/en/default-privileges.html

8 网络

本节包含有关MySQL服务器如何使用网络的建议。

8.1 确保'have_ssl'设置为'YES' (Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

在不受信任的网络上漫游时，所有网络流量都必须使用SSL / TLS。

解释：

受SSL / TLS保护的MySQL协议有助于防止窃听和中间人攻击。

审计：

执行以下SQL语句来评估此建议：

```
SHOW variables WHERE variable_name = 'have_ssl';
```

确保返回的值为YES。

注意：从MySQL 5.0.38开始，have_openssl是have_ssl的别名。MySQL可以使用OpenSSL或YaSSL构建。

修复：

按照MySQL 5.6参考手册中记录的步骤设置SSL。

影响：

启用SSL将允许客户端加密网络流量并验证服务器的身份。这可能会对网络流量检查产生影响。

默认值：

DISABLED

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/ssl-connections.html
2. http://dev.mysql.com/doc/refman/5.6/en/ssl-options.html

8.2 确保所有远程用户的'ssl_type'设置为'ANY'，'X509'或'SPECIFIED' (Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

在不受信任的网络上漫游时，所有网络流量都必须使用SSL / TLS。

对于通过网络进入系统的用户，应该基于每个用户强制执行SSL / TLS。

解释：

受SSL / TLS保护的MySQL协议有助于防止窃听和中间人攻击。

审计：

执行以下SQL语句来评估此建议：

```
SELECT user, host, ssl_type FROM mysql.user
WHERE NOT HOST IN ('::1', '127.0.0.1', 'localhost');
```

确保返回的每个用户的ssl_type等于ANY，X509或SPECIFIED。

注意：从MySQL 5.0.38开始，have_openssl是have_ssl的别名。MySQL可以使用OpenSSL或YaSSL构建。

修复：

使用GRANT语句要求使用SSL：

```
GRANT USAGE ON *.* TO 'my_user'@'app1.example.com' REQUIRE SSL;
```

请注意，REQUIRE SSL仅强制执行SSL。REQUIRE X509，REQUIRE ISSUER，REQUIRE SUBJECT等选项可用于进一步限制连接选项。

影响：

强制执行SSL / TLS时，不使用SSL的客户端将无法连接。如果服务器未配置SSL / TLS，则必须连接SSL / TLS的帐户

默认值：

未强制执行 (`ssl_type` 为空)

参考文献:

1. http://dev.mysql.com/doc/refman/5.6/en/ssl-connections.html
2. http://dev.mysql.com/doc/refman/5.6/en/grant.html

9 同步

一切都与将数据从一台服务器同步到另一台服务器有关。

9.1 确保同步流量安全(Not Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

应保护服务器之间的同步流量。安全措施应包括确保流量的机密性和完整性，以及在执行复制之前在服务器之间执行相互身份验证。

解释:

应该保护同步流量，因为它可以访问所有传输的信息并可能泄漏密码。

审计:

检查同步流量是否正在使用以下保护措施：、

- 专用网络
- VPN
- SSL/ TLS
- SSH隧道

修复:

保护网络流量

影响:

当同步流量不受保护时，攻击者可能会在同步到从属设备时捕获密码和其他敏感信息。

9.2 确保'master_info_repository'设置为'TABLE' (Scored)

适用性：

- Level 2 - MySQL RDBMS

描述：

master_info_repository设置确定从站记录主站状态和连接信息的位置。 选项包含FILE或TABLE。另请注意，此设置也与sync_master_info设置相关联。

解释：

客户端使用的密码存储在主信息存储库中，默认情况下是一个纯文本文件。 TABLE主信息存储库更安全一些，但是通过文件系统访问，仍然可以访问从属设备使用的密码。

审计：

执行以下SQL语句来评估此建议：

```
SHOW GLOBAL VARIABLES LIKE 'master_info_repository';
```

结果应该是TABLE而不是FILE。

注意：datadir中也不应该有master.info文件。

修复：

执行以下操作以修复此设置：

1. 打开MySQL配置文件（my.cnf）
2. 找到master_info_repository
3. 将master_info_repository值设置为TABLE

注意：如果master_info_repository不存在，请将其添加到配置文件中。

默认值：

FILE

References:

1. http://dev.mysql.com/doc/refman/5.6/en/replication-options-slave.html#sysvar_master_info_repository

9.3 确保'MASTER_SSL_VERIFY_SERVER_CERT'设置为'YES'或'1' (Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

在MySQL从属上下文中，设置MASTER_SSL_VERIFY_SERVER_CERT指示从属设备是否应验证主服务器的证书。此配置项可以设置为“是”或“否”，除非在从站上启用了SSL，否则将忽略该值。

解释:

使用SSL时，证书验证对于验证正在建立连接的一方非常重要。在这种情况下，从服务器（客户端）应验证主服务器（服务器）的证书，以便在继续连接之前对主服务器进行身份验证。

审计:

要评估此建议，请查找以下声明：

```
select ssl_verify_server_cert from mysql.slave_master_info;
```

验证ssl_verify_server_cert的值是否为1。

修复:

要修复此设置，必须使用CHANGE MASTER TO命令。

```
STOP SLAVE; -- required if replication was already running
CHANGE MASTER TO MASTER_SSL_VERIFY_SERVER_CERT=1;
START SLAVE; -- required if you want to restart replication
```

影响:

使用CHANGE MASTER TO时，请注意以下事项：

- 在执行CHANGE MASTER TO之前，需要停止从属进程
- 使用CHANGE MASTER来启动新的中继日志而不保留旧的中继日志，除非明确告知保留它们
- 调用CHANGE MASTER TO时，会将一些信息转储到错误日志中（MASTER_HOST，

MASTER_PORT，MASTER_LOG_FILE和MASTER_LOG_POS的先前值）

- 调用CHANGE MASTER TO将隐式提交任何正在进行的事务

参考文献:

1. https://dev.mysql.com/doc/refman/5.6/en/change-master-to.html

9.4 确保同步用户的'super_priv'未设置为'Y' (Scored)

适用性：

- Level 1 - MySQL RDBMS

描述：

mysql.user表中的SUPER权限控制着各种MySQL功能的使用。这些功能包括，CHANGE MASTER TO，KILL，mysqladmin kill选项，PURGE BINARY LOGS，SET GLOBAL，mysqladmin调试选项，日志记录控制等。

解释：

SUPER权限允许主体执行许多操作，包括查看和终止当前正在执行的MySQL语句（包括用于管理密码的语句）。此权限还提供配置MySQL的功能，例如启用/禁用日志记录，更改数据，禁用/启用功能。限制具有SUPER权限的帐户可以降低攻击者利用这些功能的可能性。

审计：

执行以下SQL语句以审核此设置：

```
select user, host from mysql.user where user='repl' and Super_priv = 'Y';
```

不应返回任何行。

注意：在上面的查询中用repl替换复制用户的名称。The 'repl' user can be在

SHOW SLAVE STATUS中找到：

Master_User:

修复：

执行以下步骤以修复此设置：

1. 枚举在审计过程的结果集中找到的复制用户
2. 对于每个复制用户，发出以下SQL语句（将“repl”替换为复制用户的名称）：

```
REVOKE SUPER ON *.* FROM 'repl';
```

影响：

当SUPER权限被拒绝给定用户时，该用户将无法利用某些功能，例如某些mysqladmin选项。

参考文献：

1. http://dev.mysql.com/doc/refman/5.6/en/privileges-provided.html#priv_super
2. https://dev.mysql.com/doc/refman/5.6/en/show-slave-status.html

9.5 确保没有同步用户具有通配符主机名(Scored)

适用性:

- Level 1 - MySQL RDBMS

描述:

在向特定数据库上的用户授予权限时，MySQL可以使用主机通配符。例如，您可以将给定权限授予`'<user>'@'%'`。

解释:

避免在主机名中使用通配符有助于控制给定用户可以连接到数据库并与数据库交互的特定位置。

审计:

执行以下SQL语句来评估此建议：

```
SELECT user, host FROM mysql.user WHERE user='repl' AND host = '%';
```

确保没有返回行

修复:

执行以下操作以修复此设置：

1. 枚举运行审计程序后返回的所有用户
2. 将用户的主机更改为特定用户或DROP用户

附录A：评估记录表

控制项		正确设置	
		是	否
1	**操作系统级配置**		
1.1	将数据库放在非系统分区上	☐	☐
1.2	为MySQL守护进程/服务使用专用最小特权帐户	☐	☐
1.3	禁用MySQL命令历史记录	☐	☐
1.4	验证“MYSQL_PWD”没有设置	☐	☐
1.5	禁用交互式登录	☐	☐
1.6	验证用户配置文件中未设置“MYSQL_PWD”	☐	☐
2	**安装和规划**		
2.1	**备份和恢复**		
2.1.1	备份策略	☐	☐
2.1.2	验证备份是否正常	☐	☐
2.1.3	安全备份凭据	☐	☐
2.1.4	应妥善保护备份	☐	☐
2.1.5	时间的恢复	☐	☐
2.1.6	灾难恢复计划	☐	☐
2.1.7	备份配置和相关文件	☐	☐
2.2	专用平台允许Mysql	☐	☐
2.3	不在命令行中指定密码	☐	☐
2.4	不重复使用用户账户	☐	☐
2.5	不要使用默认或非Mysql指定的加密密钥	☐	☐
3	**文件权限和所有权**		
3.1	确保’datadir’具有合适的权限和所有权	☐	☐
3.2	确保"log_bin_basename'文件具有合适的权限和所有权	☐	☐
3.3	确保'log_error'具有合适的权限和所有权	☐	☐

3.4	确保'slow_query_log'具有合适的权限和所有权	☐	☐
3.5	确保'general_log_file'具有适当的权限和所有权	☐	☐
3.6	确保'general_log_file'具有适当的权限和所有权	☐	☐
3.7	确保SSL密钥文件具有适当的权限和所有权	☐	☐
3.8	确保插件目录具有适当的权限和所有权	☐	☐
4	**通用**		
4.1	确保应用最新安全补丁	☐	☐
4.2	确保应用最新安全补丁	☐	☐
4.3	验证'allow-suspicious-udfs'设置为'FALSE'	☐	☐
4.4	验证“local_infile”已禁用	☐	☐
4.5	确保启用“--skip-symbolic-links”	☐	☐
4.6	确保启用“--skip-symbolic-links”	☐	☐
4.7	确保禁用'daemon_memcached'插件	☐	☐
4.8	确保'secure_file_priv'不为空	☐	☐
4.9	确保'sql_mode'包含'STRICT_ALL_TABLES'	☐	☐
5	**MySQL 权限**		
5.1	确保仅管理用户具有完全数据库访问权限	☐	☐
5.2	确保非管理用户的“file_priv”未设置为“Y”	☐	☐
5.3	确保非管理用户的“process_priv”未设置为“Y”	☐	☐
5.4	确保非管理用户的“super_priv”未设置为“Y”	☐	☐
5.5	确保非管理用户的“shutdown_priv”未设置为“Y”	☐	☐
5.6	确保非管理用户的“create_user_priv”未设置为“Y”	☐	☐
5.7	确保非管理用户的“grant_priv”未设置为“Y”	☐	☐
5.8	确保非从属用户'repl_slave_priv'未设置为'Y'	☐	☐
5.9	确保DML/DDL授权仅限于特定数据库和用户	☐	☐
6	**审计和记录**		
6.1	确保'log_error'不为空	☐	☐
6.2	确保日志文件存储在非系统分区上	☐	☐

6.3	确保'log_warnings'设置为'2'	☐	☐
6.4	确保已启用审计日志记录	☐	☐
6.5	确保'log - raw'设置为'OFF'	☐	☐
7	**认证**		
7.1	确保'old_passwords'未设置为'1'	☐	☐
7.2	确保'secure_auth'设置为'ON'	☐	☐
7.3	确保全局配置中未存储密码	☐	☐
7.4	确保'sql_mode'包含'NO_AUTO_CREATE_USER'	☐	☐
7.5	确保为所有MySQL帐户设置密码	☐	☐
7.6	确保密码策略有效	☐	☐
7.7	确保没有用户拥有通配符主机名	☐	☐
7.8	确保没有匿名帐户存在	☐	☐
8	**网络**		
8.1	确保'have_ssl'设置为'YES'	☐	☐
8.2	确保所有远程用户的'ssl_type'设置为'ANY'，'X509'或'SPECIFIED'	☐	☐
9	**同步**		
9.1	确保同步流量安全	☐	☐
9.2	确保'master_info_repository'设置为'TABLE'	☐	☐
9.3	确保'MASTER_SSL_VERIFY_SERVER_CERT'设置为'YES'或'1'	☐	☐
9.4	确保同步用户的'super_priv'未设置为'Y'	☐	☐
9.5	确保没有同步用户具有通配符主机名	☐	☐

附录B：更改记录

时间	版本	版本更改
2016-08-15	1.1.0	
2018-10-23	1.1.0	首次翻译