MySQL服务器内部安全数据目录访问 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/138/2021_2022_MySQL_E6_9C_8D_E5_8A_c98_138162.htm 作为MySQL管理员的您，在维护MySQL安装的安全性和完整性方面能够做些什么。在本文中，我们将更详细地讨论以下与安全性相关的问题： 为什么说安全性是重要的，应该警惕哪些攻击？ 从服务器主机中的用户那里您将面临什么风险（内部安全性），能做什么？ 从在网络上连接到服务器的客户机那里您将面临什么风险（外部安全性），能做什么？ MySQL管理员有责任保护数据库内容的安全，使得记录只能由经过严格认证的那些用户访问。这包括内部安全性和外部安全性。 内部安全性关心文件系统级的问题，如保护MySQL数据目录免遭拥有运行服务器的机器账号的用户的攻击。但是，如果数据目录内容的文件许可权过分随意，有人可以将对应这些表的文件进行简单的替换的话，内部安全性就不能很好地确保适当建立对网络上客户机访问的授权表的控制。 外部安全性关心客户机从外部连接的问题，如防止MySQL服务器免遭通过网络进来的通过服务器的连接请求对数据库内容访问的攻击。要建立MySQL授权表使得它们不允许对服务器所管理的数据库的访问（除非提供了有效的名字和口令）。 本文提供了应该了解的有关问题的指导，并说明如何防止内部和外部级别中未认证的访问。MySQL服务器提供了一个通过mysql数据库中的授权表来实现的灵活的权限系统。可以设置这些表的内容来允许或拒绝数据库对客户机的访问。这提供了关于未认证的网络访问数据的安全性。但是，如果服务器主机上的其他用户具有对该数

据目录内容的直接访问权，则将不能对访问数据的网络建立良好的安全性。除非知道您是曾在运行MySQL服务器的机器上注册的惟一的一个人，否则需要关心在该机器上的其他用户获得对数据目录访问的可能性。 以下是您想要保护的内容：数据库文件。显然想要维护由服务器维护的数据库的保密性。数据库的所有者通常要考虑数据库内容的专有性。即使他们不考虑，也最多是使数据库的内容公共化，而不会使那些内容因数据库目录安全性低而被泄露。 日志文件。常规和更新日志必须安全，因为它们包含了查询文本。这有相当的利害关系，因为具有日志文件访问的任何人都可以监控发生在数据库中的事务处理。 与日志文件有关的更为特殊的安全性问题是，像GRANT 和SET PASSWORD 这样的查询被记录在日志中了。常规和更新日志文件包含敏感的查询文本，其中包括了口令（MySQL使用口令加密，但这只适用于在口令设置之后的连接建立。设置口令的过程包含在GRANT 、INSERT 或SET PASSWORD 这样的查询中，但这些查询以纯文本的形式被记录。）如果一个攻击者具有对日志的读访问权，那他只需在日志中对GRANT 或PASSWORD 这样的词运行grep 就能找到敏感信息。 显然，您不想让服务器主机上的其他用户拥有对数据目录文件的写访问权，因为那样的话，他们就可以在状态文件或数据库表上肆意践踏。但读访问也很危险。如果表文件可读取，那么窃取文件并使MySQL自己以纯文本的形式显示表的内容是微不足道的事。可按下列步骤进行： 1) 在服务器主机上安装您的MySQL服务器，但使用与正式服务器不同的端口、套接字和数据文件。 2) 运行mysql_install_db 初始化您的数据目录。这将允许您作

为MySQL的root 用户访问服务器，因此您将具有完全控制服务器访问机制的权利。它还建立了一个test 数据库。 3) 将您想窃取的表的相应文件拷贝到服务器数据目录下的test 子目录中。4) 启动作案服务器。您可以随意访问这些表。SHOW TABLES FROM test 将显示您拥有一个被窃取表的备份，SELECT * 将显示任何这些表的全部内容。 5) 如果更坏一点，打开服务器的匿名用户账号的许可权，使任何人都能从任何地方连接到该服务器来访问您的test 数据库。现在，您已经向全世界公布了这些被偷窃的表。 考虑一下刚才的情况，然后颠倒过来想。您希望有人对您这样做吗？当然不要。 通过在数据目录中执行ls -l 可以确定数据目录中是否包含非安全的文件或目录。应查看具有以开启的“ 组 ”或“ 其他 ”许可权的文件或目录。以下是一个非安全数据目录的部分列表，是该数据目录中的一部分数据库目录： 正如您所看到的，有些数据库目录有正确的许可权，而有些则不是这样。本例中的情况是由于时间引起的。较老的服务器创建了限制较少的许可权，且较老的服务器与较新的服务器相比，在设置许可权方面不严格（请注意，有更多限制的目录， menager 和t m p，都有更为新的日期）。MySQL当前的版本确保这些文件只对服务器运行的用户可读。 让我们来安排这些许可权，使得只有服务器的用户才能访问它们。主要的保护手段来自由UNIX文件系统本身提供的工具，这些工具可设置文件和目录的所有权及方式。操作步骤如下： 1) 定位到数据目录中：% cd DATADIR 2) 设置该数据目录下所有文件的所有权为运行该服务器的账号所拥有（必须以root 身份执行这一步）。在本书中，笔者对此账号的用户名和组名使用mysqladm 和mysqlg r

p。可以用下列命令之一修改所有权： # chown -R mysqladmin.mysqlgrp # find . -follow -type d -print | xargs chown mysqladmin.mysqlgrp3) 修改数据目录和数据库目录的方式，使得它们仅对于mysqladm 是可读的。这样防止了其他用户访问数据目录的内容。可以利用下列命令之一来进行，这些命令或者以root 或者以mysqladm 运行（后者更好，可以使作为root 运行的命令数量最小化）： % chmod -R go-rwx % find . -follow -type d -print | xargs chmod go -rwx4) 对mysqladm 用户设置数据目录内容的所有权和方式。现在，您应该确保总是以mysqladm 运行，因为它现在是唯一拥有该数据目录访问权的用户。 在上述步骤之后，将拥有以下许可权： 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com