数据库安全：DB2数据库安全性全面介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022__E6_95_B0_E6_8D_AE_E5_BA_93_E5_c98_454837.htm 简介 我们面对的这个问题是：数据库安全性话题还没有象测定最短宕机时间世界记录和报告那么引人瞩目。您是在什么时候最后一次读到有关安全令牌和加密的睿智文章的呢？但正如去年大肆宣传的从一些电子商务企业中盗窃信用卡号码的事件所表明的，安全性缺口的确引人瞩目 而且能削弱顾客的信心。即便安全性不是最令人激动的主题，对于任何使用数据库管理系统的企业来说，它也是重要顾虑。同时，随着越来越多的企业参与电子空间，把私有数据从公共数据中分离变得尤为重要。 任何给定的公司的数据库系统可能要收集、存储和分析成千上万行信息，这些信息本质上有公共的，也有私有的。由于有这项责任在身，数据库必须使数据库管理员能适当的授权和限制访问。此外，数据库还必须提供防止未授权用户存取机密数据的方法。 但是有时候，数据库安全信息难以获得或理解。尽管您常听说 DB2 通用数据库（DB2 Universal Database，UDB）是多么可扩展、多么健壮，但您多久才会听到一次有关 DB2 的安全特性的细节呢？ 因为保护数据库安全是 DBA 最重要的职责之一，所以您不应当试图通过反复试验来学习数据库安全性。保护您的数据库安全涉及： 防止任何人在企业无需知道的情况下对机密数据进行未授权的存取 防止未授权用户恶意删除进行破坏或擅自改变数据 采用审核技术监视用户存取数据 本文中，我将带您浏览 Windows、Unix 和 OS/2 版本的 DB2 UDB v.7.1 中的安全特性，并描述一些可以帮助您

最大化安全性的内部控制。 验证 数据库安全性中最基本的概念之一就是验证，这是一个相当简单的过程，系统通过这个过程来证实用户身份。用户可以通过提供身份证明或验证令牌来响应验证请求。 很可能您已经熟悉这个概念了。如果您曾经被要求出示带照片的 ID（例如，在银行新开帐户时），那么已经有人向您提出过验证请求了。您出示了驾驶执照（或其它带照片的 ID）从而证明自己的身份。在这种情况下，您的驾驶执照就充当了验证令牌。 图 1. DB2 授权角色 不管您在电影里看到些什么，大部分软件程序不能把未来系统（比如面部识别）用于验证。相反，大多数验证请求要求您提供用户标识和密码。您的用户标识表示您声称自己是被授权可访问该环境的人，密码则将提供您个人的验证证据。当然，这种验证假定您的密码受到很好的保护，而且您是唯一一个知道这个密码的人。 用户验证由 DB2 之外的安全性工具完成，这个工具通常是操作系统的一部分或独立产品。事实上，安全性不仅是数据库问题；操作系统厂商也要花费很多的时间、金钱和心思确保他们的产品是安全的。但是，包括 Microsoft Windows 95 和 98 在内的一些操作系统并没有本地安全机制。如果您使用的是没有安全机制的操作系统，那您可以把环境配置成依靠在更安全的系统上运行的 DB2 服务器来提供这种安全性。例如，您可以使用可靠的客户端选项，我将在文章的后面部分更多的讨论这些选项。（如想获得更多信息，请参阅 DB2 Administration Guide。） 您也可以使用第三方产品（如由 Open Group 定义的分布式计算环境安全服务（Distributed Computing Environment（DCE）Security Services）来给您的环境添加一层安全层。DB2 可以协调这些外部安

全工作与其安全主动性来保护事务或分析环境。一旦用户身份验证成功，DB2 记下用户的身份标识和其它相关的安全信息，如用户组列表。用户必须使用 SQL 授权名（authorization name）或授权标识（authid）以被 DB2 识别，授权名或授权标识可以与用户标识或映射值相同。这一连接信息将在用户连接期间保留。