第8章 数据安全技术

在数字化和信息化高度发展的当今时代，数据已成为企业和个人最重要的资产之一。然而数据在存储、传输和使用过程中可能面临多种威胁，如数据丢失、篡改、泄露或破坏。数据安全技术作为保护数据资产的关键手段，不仅关注数据的完整性、可用性和保密性，还为数据在灾难性事件后的恢复提供了强有力的保障。通过本章内容的学习，读者将全面掌握数据安全技术的基本理论、应用实践以及最新发展趋势，为应对现代信息社会的数据安全挑战奠定坚实基础。

要点难点

- 数据完整性保护
- 数据容错技术
- 数据容灾技术
- 数据灾难恢复技术
- 数据库安全技术

8.1 数据完整性保护技术

随着网络空间安全需求的不断提高，数据完整性保护技术成为信息安全领域的一个重要分支。对于个人用户、企业以及政府机构来说，数据完整性至关重要，因为它直接关系到数据的可信性和系统的正常运行。

在实际应用中，数据完整性保护技术通过一系列算法、协议和工具，确保数据从创建到使用的全生命周期内保持一致性和准确性。

8.1.1 数据完整性保护简介

数据完整性保护是确保数据在传输、存储和处理过程中不被篡改、损坏或丢失的一种安全措施。数据完整性保护旨在确保数据的原始性和可信性，以防止未经授权的修改或损坏，从而保障数据的可靠性和准确性。数据完整性是信息安全的重要组成部分，涉及以下几方面。

- **防止未授权的修改：**数据完整性保证数据在存储、处理和传输过程中不被未授权的用户篡改或修改。
- **确保数据的准确性和一致性：**包括数据的内容、格式和结构，确保数据在各种操作后仍然保持一致的状态。
- **维护数据的隐私性：**数据完整性的保障有助于保护个人和企业信息的隐私性，防止数据泄露和滥用。
- **组织文化和政策：**组织应建立一种质量文化，确保所有形式的数据（如纸质版和电子版）都是完整和一致的。此外，数据治理政策应得到组织最高层的认可和支持。

8.1.2 消息认证技术

消息认证技术主要用于保护数据的完整性，是确保数据在传输或存储过程中未被篡改的重要手段。

1. 认识消息认证技术

消息认证是一种用于验证通信中消息真实性和完整性的技术，也被称为报文鉴别或报文认证。它通常用于确认消息的发送者和内容是可信的，并且消息在传输过程中未被篡改。消息认证技术是网络安全和信息安全中的重要组成部分，常用于保护通信数据的安全。

2. 消息认证技术的功能

消息认证技术的主要功能如下。

（1）消息内容认证

消息内容认证是消息认证的核心，旨在确保消息在传输过程中未被篡改。通常通过消息认证码（MAC）或数字签名实现。消息认证码是一种通过对消息内容进行特定算法处理后生成的一段代码，它可以验证消息是否完整且未经修改。

（2）身份认证

身份认证涉及确认消息的来源确实是声称的发送者，而不是其他人伪装的。可以通过数字签名实现，因为数字签名不仅提供了消息的完整性验证，还能验证发送者的身份。

（3）序号和时间认证

在某些情况下，消息的顺序和发送时间也是重要的安全因素。例如，防止重放攻击，即攻击者截获并重新发送一条旧消息以企图欺骗系统。在消息中包含序列号和时间戳，可以防止这类攻击。

（4）加密与签名

消息认证技术通常与加密和数字签名技术结合使用。加密确保了即使消息被截获，未授权的第三方也无法读取其内容。数字签名则提供了一种验证消息来源和内容完整性的方法。

3. 消息认证技术的原理

消息认证技术的基本原理是使用密钥和消息认证码（MAC）对消息进行认证。发送方使用密钥和消息计算MAC，并将MAC与消息一起发送给接收方。接收方使用相同的密钥和消息计算MAC，并将得出的MAC与接收到的MAC进行比较。如果两个MAC相同，则表示消息没有被篡改，并且来自可信的发送方。

8.1.3 报文摘要技术

报文摘要也称为消息摘要或数字指纹，是一种对报文进行压缩的算法，其目的是生成报文的唯一标识，用于验证报文的完整性。报文摘要通常是报文的一部分，可以用来验证报文是否被篡改。报文摘要算法使用Hash函数将报文转换为固定长度的摘要。报文摘要技术的特点如下。

- **不可逆性**：报文摘要是通过Hash函数生成的，具有不可逆性，即无法从摘要反推出原始消息内容。
- **固定长度**：报文摘要的长度是固定的，不受原始消息长度的影响。常见的摘要长度包括128位、160位、256位等。
- **唯一性**：对于不同的消息内容，生成的摘要是唯一的，即使原始消息内容只有微小的改变，生成的摘要也会大不相同。
- **敏感性**：原始消息内容的任何改变都会导致生成的摘要发生变化，从而可以检测到消息的篡改。

1. 报文摘要技术用法

发送方在发送消息之前，使用Hash函数对消息内容进行摘要计算，生成一个固定长度的摘要，并将摘要附加到消息中一起发送。接收方接收到消息后，重新计算收到消息的摘要，并将计算得到的摘要与接收到的摘要进行比较。如果两者相同，则说明消息完整且未被篡改；如果不同，则表示消息可能已被篡改或损坏。

2. 报文摘要技术的优势和局限性

报文摘要技术有如下优势。

- **安全性高**：报文摘要使用Hash函数进行计算，具有较高的安全性。
- **效率高**：报文摘要的计算效率较高，可以满足实时性要求。
- **易于实现**：报文摘要技术的实现方法比较简单，易于应用。

同时报文摘要技术也存在一定的局限性。

- **报文摘要不能防止重放攻击：**攻击者可以截获原始报文，并在将来重新发送该报文，以欺骗接收方。
- **报文摘要不能防止抵赖攻击：**发送方可以否认发送过某个报文，即使该报文包含其摘要。

8.1.4 Hash函数

Hash函数将任意长度的输入数据映射为固定长度的输出数据，通常称为Hash值或摘要。这个过程是确定性的，即给定相同的输入，Hash函数总是生成相同的输出。8.1.3节介绍的报文摘要的生成，其实就是使用了Hash函数。

如果对一段明文使用Hash算法，哪怕只更改该段落的一个字母，随后的Hash值都将产生不同的值。要找到Hash值为同一个值的两个不同的输入，在计算上是不可能的，所以数据的Hash值可以检验数据的完整性。

知识拓展

Hash函数的特性

如果两个Hash值是不相同的（根据同一函数），那么这两个Hash值的原始输入也是不相同的。这个特性是Hash函数具有确定性的结果。另一方面，Hash函数的输入和输出不是一一对应的，如果两个Hash值相同，两个输入值很可能是相同的，但不确定二者一定相等（可能出现Hash碰撞）。输入一些数据计算出Hash值，然后部分改变输入值，一个具有强混淆特性的Hash函数会产生一个完全不同的Hash值。

1. Hash 函数的特性

Hash函数在数据完整性保护中的功能与其特性是分不开的，Hash函数的特性如下。

- **一致性：**相同的输入数据应该产生相同的Hash值。
- **唯一性：**不同的输入数据应该产生不同的Hash值，以尽可能减少Hash碰撞的可能性。
- **高效性：**Hash函数的计算应该是高效的，以便在实际应用中能够快速地生成Hash值。
- **不可逆性：**理想情况下，Hash函数是不可逆的，即从Hash值无法推导出原始的输入数据。
- **抗碰撞性：**Hash函数应该具有良好的抗碰撞性，即对于不同的输入数据，其生成的Hash值应该尽可能不同。
- **扩展性：**Hash函数应该具有良好的扩展性，即能够处理任意长度的输入数据，并且生成固定长度的输出。

知识拓展

Hash函数的构造

Hash函数通常由两部分组成：压缩函数和初始向量。压缩函数负责将输入数据压缩为固定长度的输出；初始向量是用于初始化压缩函数的参数，以确保输出的随机性和不可预测性。

2. Hash 值的计算方式

根据获取Hash值的计算方法，Hash函数常使用以下四种方法获取到Hash值。

- **余数法：**先估计整个Hash表中的表项目数目大小。然后用这个估计值作为除数去除每个原始值，得到商和余数。用余数作为Hash值。因为这种方法产生冲突的可能性相当大，

因此任何搜索算法都应该能够判断冲突是否发生，并提出取代算法。

- **折叠法：**这种方法针对原始值为数字时使用，将原始值分为若干部分，然后将各部分叠加，得到的最后四个数字（或者取其他位数的数字都可以）作为Hash值。
- **基数转换法：**当原始值是数字时，可以将原始值的数值基数转为一个不同的数字。例如，可以将十进制的原始值转为十六进制的Hash值。为了使Hash值的长度相同，可以省略高位数字。
- **数据重排法：**这种方法只是简单地将原始值中的数据打乱排序。例如可以将第3～6位的数字逆序排列，然后利用重排后的数字作为Hash值。

3. Hash 函数的主要应用

Hash函数被广泛应用到多个应用场景。

（1）数据完整性校验

Hash函数可以用来校验数据的完整性。例如，在下载文件时，可以使用Hash函数验证下载的文件是否完整无损。

（2）数字签名

Hash函数可以用来生成数字签名。数字签名可以用来验证数据的真实性和完整性。

（3）密码存储

Hash函数可以用来存储用户密码。将用户密码进行Hash处理后存储，可防止密码泄露。

（4）数据索引

Hash函数可以用来快速查找数据。例如，在数据库中，可以使用Hash函数快速找到指定的数据记录。

（5）网络安全

Hash函数可以用于网络协议的认证和加密。例如，在SSL/TLS协议中，可以使用Hash函数验证服务器的身份和加密通信数据。

4. Hash 函数的安全性

Hash函数的安全性是其最重要的特性之一。Hash函数的安全性主要取决于其碰撞性。碰撞是指不同的输入数据产生相同的输出数据。如果Hash函数存在碰撞攻击，则攻击者可以构造不同的输入数据，使其产生相同的Hash值，从而伪造数据或破解密码。

目前，常用的Hash函数算法具有较高的安全性。然而，随着计算能力的不断提高，Hash函数的安全性也面临着挑战。因此，需要不断研究和开发新的Hash函数算法，以提高其安全性。

5. 常见的 Hash 函数算法

常见的Hash函数算法包括MD5以及SHA系列算法。

1）MD5算法

MD5（Message Digest Algorithm 5）是一种广泛使用的Hash函数，用于将任意长度的消息（字符串或二进制数据）转换成固定长度的128位（16字节）Hash值。虽然在当今的密码学中不再建议使用MD5，因为它存在一些已知的安全漏洞，但它仍然被广泛应用于数据完整性校验、数字签名和随机数生成等领域。MD5算法具有以下特点。

- **固定长度输出**：无论输入消息的长度如何，MD5算法的输出始终是128位。
- **快速性**：MD5算法的实现通常很快，适合需要快速计算Hash值的应用。
- **不可逆性**：由于MD5是单向Hash函数，从Hash值推导出原始消息几乎是不可能的。这使得MD5广泛用于密码Hash等领域。
- **雪崩效应**：即使输入数据发生微小变化，也会导致输出的MD5值发生显著变化。
- **碰撞可能性**：MD5算法存在碰撞的可能性，即不同的输入可能会产生相同的Hash值。这一问题已经被广泛证实，因此MD5算法在许多安全领域已经不再建议使用。

2）SHA系列算法

SHA（Secure Hash Algorithm，安全哈希算法）是一系列密码学Hash函数。SHA算法的设计目标是产生固定长度的Hash值，使得对输入数据的任何细微变化都会导致输出Hash值的大幅度变化，同时尽可能地减小碰撞的可能性。SHA算法通常采用迭代的方式对输入数据进行处理，通过多轮的复杂运算混淆输入数据的比特位，从而增加反向推导原始数据的难度。SHA算法家族包括多个版本，其中SHA-1、SHA-2和SHA-3的使用较广泛。

（1）SHA-1算法

SHA-1产生160位（20字节）的Hash值，它是SHA算法家族中的第一个版本，于1995年发布。由于SHA-1存在严重的安全漏洞，尤其是碰撞攻击的可行性，因此它不再适合用于安全应用。因此，SHA-1在许多场景中已经被淘汰。

（2）SHA-2算法

SHA-2是SHA算法家族的第二个版本，它包括一系列Hash函数，产生的Hash值长度可以是224位、256位、384位或512位。SHA-256和SHA-512是SHA-2家族中最常用的两个Hash函数。SHA-2被广泛认为是安全的，目前仍然被广泛使用，尤其在数字签名、数据完整性校验和密码学证明等领域。

（3）SHA-3算法

SHA-3是SHA算法家族中的第三个版本，与SHA-1和SHA-2不同，SHA-3不是在SHA-2的基础上设计的，而是由Keccak算法家族中的一个成员进行了改进和标准化。SHA-3也产生不同长度的Hash值，最常见的是SHA3-256和SHA3-512。

6. Hash 算法的应用实例

Hash算法在实际中使用的较多，主要用在保证完整性和数据加密两方面。保证数据的完整性就是防止数据被篡改。实际使用中，数据、文件、软件都是以二进制存储在计算机中，都可以使用MD5算法进行完整性校验。如对一个文件或软件进行MD5计算后，将文件或软件以及计算出的MD5值发布到网上，如图8-1所示。

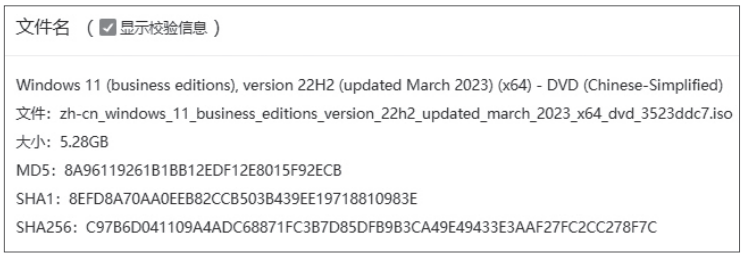

图 8-1

下载后再次对文件进行MD5值的计算，将结果与发布时的MD5值进行对比，如果完全一致，说明软件未经过任何篡改，如图8-2所示。

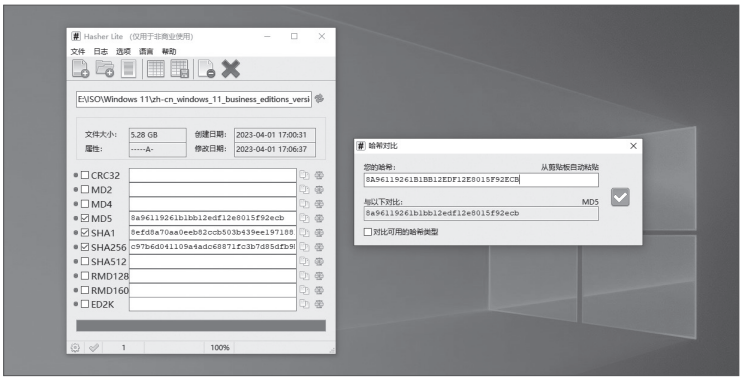

图 8-2

知识拓展

其他的Hash计算工具

除了使用工具，如Hasher计算文件的Hash值外，在操作系统，如Windows中，可以使用命令计算文件的Hash值。除了计算文件的Hash值外，这些工具还可以计算程序以及文本的Hash值。有些人还会对一些密码进行Hash计算，并存储在数据库中，通过网站提供Hash值的反查询来达到破解Hash的目的。

8.2 数据容错技术

在现代网络空间中，数据是企业运营、决策制定和个人生活的重要支柱。为了最大程度地减少各种错误对数据可靠性的影响，数据容错技术应运而生。数据容错技术是一种通过冗余设计、自动校正和恢复机制确保数据在受损情况下依然可用的关键手段。它的核心理念是“预防为主，恢复为辅”，即在系统设计中增加冗余组件，以提高系统的容错能力，并在出现问题时快速恢复数据。

8.2.1 数据容错技术简介

数据容错技术是计算机系统和存储设备中用于提高可靠性的重要技术。其主要目标是通过冗余存储和自动恢复机制，确保在硬件或软件出现故障时，数据的完整性和可用性不受影响。

1. 基本原理

数据容错技术依赖于冗余机制提供故障保护。例如，通过复制数据或将数据分片存储到多个设备中，可以在其中一个设备发生故障时，从冗余设备中恢复丢失的数据。此外，校验技术和错误检测机制能够实时发现数据错误并进行纠正。

2. 技术特点

数据容错技术的特点如下。

- **冗余设计：**通过冗余副本或校验信息提高系统的可靠性。
- **实时监控：**对系统运行状态和数据一致性进行持续监测。
- **快速恢复：**故障发生后，通过内置的恢复机制快速重建受损数据。
- **扩展性强：**能够随着存储需求的增加灵活扩展系统规模。

3. 应用场景

数据容错技术已经被广泛应用到各种数据存储场景中。

- **企业数据中心：**用于保护关键业务数据，例如客户信息和财务记录。
- **分布式存储系统：**确保大规模数据在多节点环境中的高可用性。
- **云存储平台：**提供用户数据的高可靠性和高可用性保障。

8.2.2 磁盘阵列技术

磁盘阵列技术是数据容错技术的一种重要实现方式。通过多个物理磁盘组成一个逻辑存储单元，磁盘阵列不仅提高了存储性能，还为数据提供了强有力的容错能力。磁盘阵列技术的核心是RAID（Redundant Array of Inexpensive Disks，独立磁盘冗余阵列），它通过不同的配置级别实现数据的高效存储和容错保护。

1. 认识磁盘阵列技术

RAID译为“廉价磁盘冗余阵列”，也称为“磁盘阵列”。后来RAID中字母“I”的含义被改为Independent，RAID就成了“独立磁盘冗余阵列”，但这只是名称的变化，实质性的内容并没有改变。RAID技术是利用若干台小型磁盘驱动器加上控制器按一定的组合条件而组成的一个大容量、快速响应、高可靠的存储子系统。

由于有多台驱动器并行工作，大大提高了存储容量和数据传输率，还采用了纠错技术，提高了可靠性。RAID按工作模式可以分为RAID 0、RAID 1、RAID 2、RAID 3、RAID 4、RAID 5、RAID 6、RAID 7、RAID 10、RAID 53等多种级别。

2. RAID 技术原理

RAID是一种通过虚拟化技术将多个物理磁盘驱动器组合为一个或多个逻辑单元的存储虚拟化技术。在RAID中，数据被分布到多个磁盘中，因此各磁盘可以并行工作，从而提高数据处理的速度。同时，RAID可以复制数据到多个磁盘，以提供数据冗余保护，从而提高数据的可靠性。RAID技术有多种不同的级别，每种级别的RAID技术都提供了不同的冗余机制和性能水平。

3. RAID 的功能

RAID是一种数据存储技术，通过将多个磁盘组合成一个逻辑单元，以提高数据的可靠性、性能和/或容量。RAID技术主要有以下几种基本功能。

- 通过对磁盘上的数据进行条带化，实现对数据成块存取，减少磁盘的机械寻道时间，提高数据存取速度。
- 通过对一个阵列中的几块磁盘同时读取，减少磁盘的机械寻道时间，提高数据存取速度。
- 通过镜像或者存储奇偶校验信息的方式，实现对数据的冗余保护。

知识拓展

RAID技术的优缺点

RAID技术提高了磁盘的可靠性和可用性，降低了存储成本。但RAID技术增加了复杂性，降低了存储空间利用率以及磁盘的性能。

4. RAID 的实现方式

RAID可以通过硬件和软件两种方式实现。

（1）硬件RAID

使用专用的RAID控制器，控制器上有自己的处理器和内存，独立于主机CPU。硬件RAID具有更好的性能和稳定性，适用于高端服务器和数据中心环境。

（2）软件RAID

通过操作系统内置的RAID驱动程序或第三方软件实现。软件RAID依赖主机CPU来执行RAID计算和管理，性能可能受到影响，但成本较低，适用于普通服务器和个人计算机。

5. RAID 的级别

实际使用中，常见的RAID级别有RAID 0、RAID 1、RAID 0+1、RAID 3、RAID 5等。不同的级别对应不同的功能、原理及应用。

（1）RAID 0

RAID 0在*N*块磁盘上选择合理的带区来创建带区集。其原理类似于显示器隔行扫描，将数据分割成不同条带，分散写入所有磁盘中并可实现，如图8-3所示。多块硬盘的并行操作使同一时间内磁盘读写的速度提升*N*倍。

如果把所有的磁盘都连接到一个控制器上，可能会带来潜在的危害。因为频繁进行读写操作时，很容易使控制器或总线的负荷超载。建议用户可以使用多个磁盘控制器。最好的解决方法还是为每一块磁盘配备一个专门的磁盘控制器。

虽然RAID 0可以提供更多的空间和更好的性能，但是整个系统非常不可靠，如果出现故障，无法进行任何补救。所以，RAID 0一般只在对数据安全性要求不高且需要高速读写的情况下才被使用。

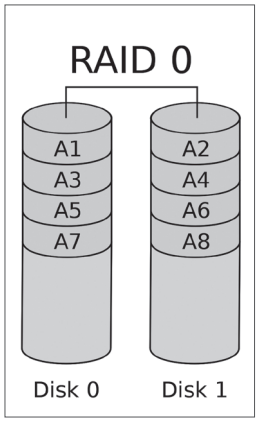

图 8-3

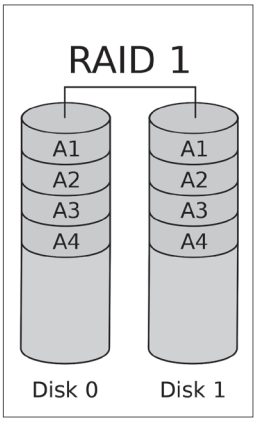

图 8-4

（2）RAID 1

RAID 1称为磁盘镜像，原理是把一个磁盘的数据镜像到另一个磁盘上，如图8-4所示。数据在写入一块磁盘的同时，会在另一块磁盘上生成镜像文件，在不影响性能的情况下最大限度地保证系统的可靠性和可修复性，当一块磁盘失效时，系统会忽略该磁盘，转而使用备份的镜像盘读写数据，具备很好的磁盘冗余能力。虽然这样对数据绝对安全，但是成本也会明显增加，且不会提高读写的速度，此时磁盘的利用率为50%。另外，出现磁盘故障的RAID系统不再可靠，应当及时更换损坏的磁盘，否则剩余的镜像盘如果出现问题，那么整个系统就会崩溃。更换新磁盘后，原有数据会需要很长时间同步镜像，但外界对数据的访问不会受到影响，只是恢复时整个系统的性能有所下降。因此，RAID 1多用在保存关键性数据的重要数据的场合。

（3）RAID 5

RAID 5为无独立校验盘的奇偶校验磁盘阵列。RAID 5把校验块分散到所有的数据盘中，它

使用了一种特殊的算法，可以计算出任何一个带区校验块的存放位置，这样就可以确保任何对校验块进行的读写操作都会在所有的RAID磁盘中进行均衡，从而消除了产生瓶颈的可能。任何一块磁盘的损坏，都可以通过其他几块磁盘恢复数据，RAID 5能提供较为完美的整体性能，因而是被广泛应用的一种磁盘阵列方案。适合于I/O密集、高读写比率的应用程序，如事务处理等。为了具有RAID 5级的冗余度，至少需要3个磁盘组成的磁盘阵列。常见的RAID 5模式如图8-5所示。RAID 5既可以通过磁盘阵列控制器硬件实现，也可以通过某些网络操作系统软件实现。

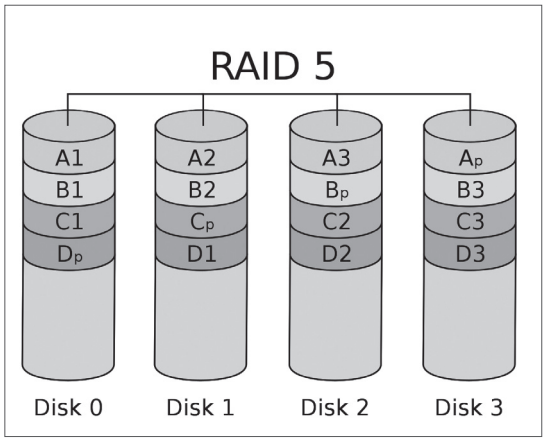

图 8-5

注意事项 RAID 5的恢复要求

如果一块磁盘损坏，RAID 5可以恢复，如果同时有多块磁盘损坏，则会因为文件的缺失而无法恢复。

（4）RAID 0+1与RAID1+0

从RAID 0+1的名称上便可以看出其是RAID 0与RAID 1的结合体。在单独使用RAID 1时也会出现类似单独使用RAID 0那样的问题，即在同一时间内只能向一块磁盘写入数据，不能充分利用所有的资源。为了解决这一问题，可以在磁盘镜像中建立带区集。这种配置方式综合了带区集和镜像的优势，所以被称为RAID 0+1。把RAID 0和RAID 1技术结合起来，数据除分布在多个盘上，每个盘都有其物理镜像盘，提供全冗余能力，允许至多一个磁盘发生故障，且不影响数据可用性，同时具有快速读写能力。RAID 0+1要在磁盘镜像中建立带区集至少需要4块磁盘，如图8-6所示。

除了RAID 0+1外，还有RAID1+0，有时也称为RAID 10，如图8-7所示，只是先后顺序变化了而已。

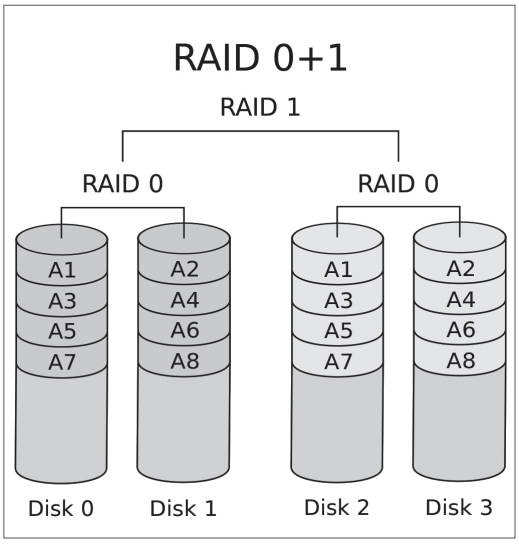

图 8-6

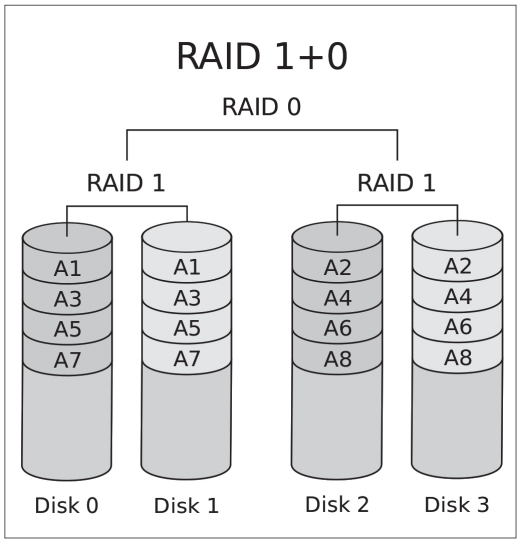

图 8-7

8.3 数据容灾技术

随着信息技术的普及，数据的重要性日益凸显。企业和机构在面对硬件故障、自然灾害、网络攻击等威胁时，如何保护关键数据并快速恢复业务，成为数据管理的核心挑战。数据容灾技术通过有效的备份、冗余和恢复手段，保障了数据的完整性、可用性和安全性，是现代企业IT系统中不可或缺的部分。本节将深入讲解数据容灾技术的基本概念、实现等级以及检测与迁移的关键实践。

8.3.1 认识数据容灾技术

数据容灾技术是一系列用于在灾难发生后快速恢复数据和系统运行的技术和方法。这些技术以数据备份为基础，结合实时数据同步、镜像复制以及多地部署等先进手段，帮助企业在数据丢失或系统崩溃时迅速恢复。

1. 数据容灾的意义

现代数据容灾技术已经成为企业竞争力的重要指标，其发展趋势包括向云计算和人工智能的方向延伸。数据容灾技术的主要意义如下。

- **保障业务连续性：**即使在极端条件下，也能保证业务服务不中断或快速恢复。
- **降低经济损失：**通过快速恢复减少停机时间和数据丢失导致的经济损失。
- **满足法规要求：**遵守如《通用数据保护条例》（GDPR）等数据保护法规的要求。

知识拓展

数据容灾的应用

数据容灾适用于广泛的场景，如金融系统中的交易数据保护、电商平台的订单记录恢复、政府机构的档案存储等。

2. 数据容灾技术的原理

数据容灾技术基于以下原理实现。

（1）备份和复原

定期备份关键数据、应用程序和系统，以便在灾难发生时能够快速恢复。

（2）数据复制

通过数据复制技术，在不同的地理位置或存储介质上保存数据的副本，以提供备份和灾难恢复的多样性和可靠性。

（3）灾难恢复计划

制订详细的灾难恢复计划（DRP），包括数据备份策略、灾难恢复流程和应急响应计划等，确保在灾难发生时能够迅速、有效地恢复业务。

3. 数据容灾技术常见方法

数据容灾技术的常见方法如下。

（1）站点复制

站点复制是指将本地数据中心的数据和应用系统实时复制到异地数据中心。站点复制的优

点是数据丢失量小、恢复速度快，缺点是成本高。

（2）异地备份

异地备份是指定期将本地数据中心的数据备份到异地数据中心。异地备份的优点是成本低，缺点是数据丢失量可能较大，恢复速度较慢。

（3）日志备份

日志备份是指备份数据库的日志文件。日志备份的优点是恢复速度快，缺点是需要完整的备份作为基础。

（4）虚拟机复制

虚拟机复制是指将虚拟机及其数据复制到异地数据中心。虚拟机复制的优点是灵活性和可扩展性好，缺点是对网络带宽要求较高。

8.3.2 数据容灾系统等级

企业应根据自身业务规模和关键性选择适合的容灾等级，同时不断优化容灾策略，以适应变化的业务需求和技术进步。根据国际标准SHARE78将数据容灾系统定义并简化成如下4个级别。

1. 第 0 级：没有备援中心

第0级容灾备份实际上没有灾难恢复能力，它只在本地进行数据备份，并且被备份的数据只在本地保存，没有送往异地。

2. 第 1 级：本地磁盘备份，异地保存

在本地将关键数据备份，然后送到异地保存。灾难发生后，按预定数据恢复程序恢复系统和数据。这种方案成本低、易于配置。但当数据量较大时，存在存储介质难以管理的问题，并且当灾难发生时存在大量数据难以及时恢复的问题。为了解决这些问题，灾难发生时，先恢复关键数据，再恢复非关键数据。

3. 第 2 级：热备份站点备份

在异地建立一个热备份点，通过网络进行数据备份，也就是通过网络以同步或异步方式，把主站点的数据备份到备份站点。备份站点一般只备份数据，不承担业务。当出现灾难时，备份站点接替主站点的业务，从而维护业务运行连续性。

4. 第 3 级：活动备援中心

在相隔较远的地方分别建立两个数据中心，它们都处于工作状态，并相互进行数据备份。当某个数据中心发生灾难时，另一个数据中心接替其工作任务。这种级别的备份根据实际要求和投入资金的多少，又可分为两种。

- 两个数据中心只限于关键数据的相互备份。
- 两个数据中心互为镜像，即零数据丢失。

零数据丢失是目前要求最高的一种容灾备份方式，它要求不管什么灾难发生，系统都能保证数据的安全。它需要配置复杂的管理软件和专用的硬件设备，需要的投资相对而言是最大的，但恢复速度也是最快的。

8.3.3 数据容灾检测及数据迁移

对于一个容灾系统，在灾难发生时，尽早地发现生产系统端的灾难，尽快地恢复生产系统的正常运行，或者尽快地将业务迁移到备用系统上，都可以将灾难造成的损失降低到最低。

1. 容灾检测

容灾检测旨在验证现有容灾方案的有效性。其核心在于确保数据备份的完整性和恢复过程的可行性，具体如下。

- **数据完整性验证：**定期检查备份数据是否完好无损，并确保其能够恢复到系统中。
- **模拟演练：**在受控环境中模拟灾难场景，测试系统的恢复时间和数据丢失范围。
- **自动化监测：**利用监控工具实时分析数据传输和存储状态，及时发现异常。

除了依靠人力对灾难进行确定之外，对于系统意外停机等灾难还需要容灾系统能够自动地检测灾难的发生。目前容灾系统的检测技术一般采用心跳技术。

心跳技术的实现方式是，生产系统在空闲时每隔一段时间向外广播一次自身的状态，检测系统在收到这些“心跳信号”之后，便认为生产系统是正常的，若在给定的一段时间内没有收到“心跳信号”，检测系统便认为生产系统出现了非正常的灾难。心跳技术的另外一个实现方式是，每隔一段时间，检测系统就对生产系统进行一次检测，如果在给定的时间内被检测系统没有响应，则认为被检测系统出现了非正常的灾难。心跳技术中的关键点是心跳检测的时间和时间间隔周期。如果间隔周期短，会给系统带来很大的开销。如果间隔周期长，则无法及时发现故障。

2. 数据迁移

灾难发生后，为了保持生产系统的业务连续性，需要实现系统的透明迁移，利用备用系统透明地代替生产系统进行运作。一般对实时性要求不高的容灾系统，例如Web服务、邮件服务器等，可以通过修改DNS或者IP来实现。对实时性要求高的容灾系统，则需要将生产系统的应用透明地迁移到备用系统上。目前基于本地机群的进程迁移算法可以应用在远程容灾系统中，但是需要对迁移算法进行改进，使其适应复杂的网络环境。迁移可能发生在灾难恢复后，也可能是技术更新或业务调整的结果。数据迁移主要包括以下两类。

- **在线迁移：**通过实时同步技术在不中断业务的情况下完成数据迁移。
- **离线迁移：**适用于数据量较大或网络条件有限的场景，迁移过程中可能需要暂停业务运行。

8.4 数据灾难恢复技术

数据灾难恢复技术是一种用于在重大数据损失或业务中断后快速恢复数据和系统运行的技术与策略。随着现代企业对数据依赖程度的不断提高，数据灾难恢复技术已成为确保业务连续性的重要组成部分。

8.4.1 数据灾难恢复技术原理

数据灾难恢复技术原理是指在灾难发生后，通过预设的恢复机制和手段，将业务系统和关键数据恢复到可用状态的过程。其核心目标是降低因灾难引发的业务中断和数据丢失所造成的损失。

1. 核心概念

在数据灾难恢复技术领域中，有一些核心概念需要了解。

（1）恢复点目标（RPO）

恢复点目标是衡量灾难发生后能够容忍的数据丢失范围。RPO时间越短，容灾系统的实时性要求越高。例如，金融交易系统的RPO可能仅为几秒，而普通业务系统的RPO可能是数小时。

（2）恢复时间目标（RTO）

恢复时间目标是指灾难发生后恢复系统和业务所需的时间长度。RTO的长短直接关系到业务中断的持续时间。

（3）冗余与备份

灾难恢复的基本原则是通过数据冗余与备份确保关键数据的可用性，包括异地备份、镜像存储等技术手段。

2. 工作流程

数据灾难恢复技术的主要流程如下。

① 灾难发生：可能的灾难包括硬件故障、软件漏洞、恶意攻击、自然灾害等。

② 触发恢复计划：当灾难发生时，企业会根据预定的恢复计划启动灾难恢复流程。

③ 切换运行环境：根据灾难的严重程度，可能需要切换到备用数据中心或云服务。

④ 恢复数据与系统：通过备份数据、镜像或其他容灾技术恢复受损的数据与系统。

⑤ 验证与优化：确保恢复后的数据完整性和系统稳定性，并对灾难恢复计划进行优化。

3. 灾难恢复的意义

现代数据灾难恢复技术已成为企业IT战略的重要组成部分，其不断创新为数据保护与业务连续性提供了坚实的基础。其主要意义如下。

- **保障业务连续性：**在最短时间内恢复业务运行，减少经济损失。
- **增强数据安全性：**通过异地备份和冗余机制有效防止数据丢失。
- **提升风险管理能力：**为企业提供应对突发事件的技术手段和管理经验。

8.4.2 常见的数据灾难恢复技术

为应对不同类型的灾难，数据灾难恢复技术提供了多种手段，以满足企业的不同需求。这些技术各有特点，通常需要结合使用以实现最佳效果。

1. 数据备份

数据备份是灾难恢复的基础。将重要数据复制到安全的存储介质中，企业可以在灾难发生后恢复丢失的数据。数据备份主要包括三种类型。

- **全量备份：**对所有数据进行完整备份，适用于关键数据保护。
- **增量备份：**仅备份自上次备份以来发生变化的数据，节省存储空间和时间。
- **差异备份：**备份自上次全量备份以来发生的所有变化，因此恢复过程更快。

2. 异地灾备

异地灾备是指将备份数据存储在远离主数据中心的地点，以避免因同一灾难同时损毁主数

据和备份数据。异地灾备主要分为以下两类。

- **异步复制：**数据变化定期同步到异地备份站点，适合对实时性要求较低的业务。
- **同步复制：**数据实时同步到异地站点，保证数据一致性，但需要较高的网络带宽。

3. 快照技术

快照是一种记录存储系统某一时间点状态的技术。通过快照，企业可以快速回滚到某一正常状态，避免灾难影响扩大。快照技术分为以下两类。

- **存储快照：**基于存储设备的硬件快照技术，恢复速度快。
- **应用快照：**针对数据库等应用系统的快照，确保数据完整性。

4. 镜像备份

镜像备份是一种高级备份技术，通过实时复制将数据同步到备份系统。镜像备份分为以下两类。

- **本地镜像：**在同一数据中心内建立数据镜像，适合短时间恢复需求。
- **异地镜像：**数据同步到异地数据中心，增强灾备能力。

5. 云灾难恢复

云灾难恢复利用云计算的灵活性和高可用性，通过云服务平台实现数据备份和系统恢复。其中云存储备份是将数据备份到云存储平台，降低维护成本。云迁移是在灾难发生时，将业务切换到云端运行。

6. 冗余架构

通过构建多层次的冗余架构，企业可以在灾难发生时快速切换到备用系统。例如采用高可用集群，也就是使用多个服务器节点共同运行，确保业务不中断。并且实现负载均衡，将流量分散到不同节点，提高系统容灾能力。

7. 灾难恢复即服务（DRaaS）

DRaaS是一种基于云的灾难恢复服务，提供全面的数据备份、监控和恢复功能。企业只需支付订阅费用，无须自行维护复杂的容灾系统。

8.5 数据库安全技术

数据库安全技术是网络空间安全技术的重要组成部分，旨在保护数据库中的数据免受未经授权的访问、篡改、泄露和破坏。随着现代信息系统的发展，数据库安全技术不断进步，为保障数据的完整性、可用性和保密性提供了有力支持。本节将从数据库的基础知识、安全问题及其应对技术等方面进行全面阐述。

8.5.1 认识数据库

数据库是信息系统中用于存储和管理数据的核心组件，是现代社会数据驱动发展的基础设施。它通过数据库管理系统（DBMS）实现对数据的高效组织、存储、查询和更新操作。数据

库不仅为各行各业提供了可靠的数据存储工具，也成为了攻击者关注的重点目标。

数据库（Database）简单来说就是一个电子化的仓库，是一个有组织的数据集合，专门用于系统化地存储和管理数据，例如文字、数字、图片、视频等。数据库不仅存储数据，还对数据进行组织，使之便于访问、修改、查询和分析。数据可以来自各方面，包括企业的业务数据、用户的行为数据、社交媒体内容、物联网设备的数据等。数据库本质上是一个文件系统，但它比传统文件系统更为复杂，能够支持结构化数据存储以及高效的数据操作。

1. 数据库的功能

数据库系统的功能非常丰富，主要包括数据存储与管理、数据查询、数据一致性与完整性、数据分析与优化以及数据备份与恢复等。

（1）数据存储与管理

数据库的首要功能是存储和管理数据。数据库能够以结构化方式存储数据，通过表、视图、索引等结构组织数据，以便于高效存取和更新。数据库还会通过优化数据存储布局（如行存储和列存储）来提高存取速度，并支持存储和检索大量结构化、半结构化和非结构化数据。

（2）数据查询

数据库系统通常提供强大的查询功能，允许用户使用查询语言（如SQL）访问和操作数据。SQL（结构化查询语言）是关系数据库的标准查询语言，通过它可以进行数据的筛选、排序、分组、聚合等操作。数据库的查询优化器会根据查询条件自动优化查询路径，提高查询效率。

（3）数据一致性与完整性

数据库系统通过多种机制确保数据的一致性和完整性，避免数据冗余和不一致。数据库中的完整性约束（如主键、外键和唯一性约束）能够维护数据间的正确关系。例如，外键约束保证关联表之间的数据一致性。此外，数据库还通过事务机制保证在并发操作和异常情况下，数据状态的完整性。

（4）数据分析和优化

数据库不仅提供基础的存储和管理功能，还逐步支持数据分析和查询优化。现代数据库系统集成了许多分析工具，用户可以执行复杂的数据挖掘、分析和报表生成等操作。此外，数据库优化器会自动分析查询模式、生成最优执行计划，进而减少查询时间，提高数据库性能。

（5）数据备份与恢复

数据库系统提供数据备份和恢复功能，以确保数据在系统故障、硬件损坏或其他灾难性事件中依然能够被恢复。备份通常有完整备份、增量备份和差异备份等不同策略，数据库管理员可以根据需求设定备份频率。数据库的恢复功能可以将数据恢复到最近的稳定状态，从而避免数据丢失。

2. 数据库系统的结构

一个完整的数据库系统通常由以下几个关键部分组成，各部分在数据库的高效、安全和可靠运行中起着不同的作用。

（1）数据库

数据库是系统的核心部分，用于存储实际数据。数据库是一个数据的集合，通常包含多张

表，每张表由若干行（记录）和列（字段）组成。数据库的存储结构根据数据模型而不同，在关系数据库中，数据以表格形式存储；在NoSQL数据库中，数据可能以文档、键值对或图的结构存储。

（2）数据库管理系统（DBMS）

数据库管理系统（DBMS）是数据库的软件平台，负责数据库的创建、维护和管理。它提供了用户与数据库之间的接口，通常包括查询语言（如SQL）和管理工具，使用户可以创建表、插入和查询数据、更新记录、删除记录等。DBMS还包括事务管理、并发控制、数据备份、恢复等功能，以确保数据的一致性、安全性和高效访问。

知识拓展

常见的数据库管理系统

常见的DBMS有关系数据库，例如MySQL、Oracle、SQL Server、PostgreSQL等；NoSQL数据库，例如MongoDB、Cassandra、Redis等。

（3）数据库用户

数据库用户是被授权访问和操作数据库的人员。用户权限可以通过DBMS进行管理，不同用户可能拥有不同的权限，例如普通用户可以读取和写入数据，而管理员用户可以修改表结构和数据库设置。这种权限控制确保数据的安全性和访问的合理性。

（4）数据库应用程序

数据库应用程序是基于数据库构建的各种软件或系统，例如网站、客户关系管理（CRM）系统、企业资源计划（ERP）系统等。应用程序通常通过DBMS访问数据库，在应用程序中进行数据的增、删、改、查操作。数据库应用程序可以帮助用户完成具体的业务需求，并且实现数据的集中管理和存储。

（5）数据库管理员

数据库管理员（DBA）负责数据库的整体维护和管理。其职责包括数据库的规划、设计、实施、监控和性能优化，确保数据库的安全性和完整性。DBA还负责备份和恢复机制的设置，防止数据丢失。DBA通过权限管理、用户管理和日志审计等措施保证数据库的安全。

8.5.2 数据库安全概述

数据库是现代信息技术系统的重要组成部分，它存储和管理着大量的敏感数据和关键信息，如客户记录、交易历史、财务报表等。确保数据库的安全是保护整个信息系统安全的关键环节。数据库安全的目标是防止未经授权的访问、篡改、泄露或破坏，同时保证合法用户能够高效、安全地访问所需数据。

1. 数据库面临的主要威胁

数据库的安全威胁主要来源于外部攻击者和内部用户。外部威胁通常包括SQL注入攻击、暴力破解、恶意软件以及分布式拒绝服务（DDoS）攻击等；内部威胁则可能源于操作失误、权限滥用或恶意行为、技术漏洞导致敏感信息被暴露。数据库的复杂性和多样性也使得其安全问题更加突出，尤其是在分布式数据库、云数据库和物联网环境中，数据库的安全性面临更多挑

战。此外，自然灾害、硬件故障，如磁盘损坏、电力中断等都有可能导致数据丢失。

2. 数据库安全的主要应对方式

为了应对这些威胁，数据库安全必须从技术和管理两方面着手。技术上需要采用严格的访问控制、加密措施、实时监控和审计等手段；管理上则需制定完善的安全策略和规范，包括用户权限划分、数据备份策略以及应急响应计划。通过这些措施，可以有效保障数据库的保密性、完整性和可用性。

知识拓展

数据库安全的目标

数据库安全的目标主要包括保密性、完整性和可用性。具体如保护数据不被非授权用户访问；防止数据被恶意篡改，确保数据的正确性和一致性；保证数据库在预期条件下能够持续提供服务。

8.5.3 数据库安全体系与控制技术

构建完善的数据库安全体系需要从技术、管理和策略三方面入手，通过多种手段相结合，实现对数据库的全面保护。

1. 数据库安全体系

构建完善的数据库安全体系是确保数据库安全运行的重要基础。这一体系需要整合身份认证、访问控制、加密技术、日志审计、漏洞管理等多种安全技术等。

（1）身份认证与访问控制

数据库安全的第一道防线是身份认证与访问控制。身份认证通过验证用户的身份（如用户名、密码、多因素认证等）来防止未授权的访问。访问控制则通过权限管理来确保不同用户只能访问特定的数据库资源。例如，基于角色的访问控制（RBAC）可以根据用户角色分配权限，细粒度访问控制（FGAC）则允许更精确的权限设置，限制用户对特定数据记录或字段的操作权限。

（2）数据加密

加密技术在保护数据保密性方面起到了重要作用。透明数据加密（TDE）可对整个数据库或文件系统进行加密，列级加密则专注于保护特定的敏感字段。加密不仅限于静态数据，还包括传输中的数据。采用TLS/SSL协议加密传输，可以有效防止中间人攻击。此外，密钥管理系统（KMS）在加密技术中也扮演了关键角色，它负责安全的生成、分发和存储加密密钥。

（3）日志审计与实时监控

日志审计是数据库安全的重要工具，记录所有访问和操作行为，便于事后分析和追踪。例如，管理员可以通过审计日志发现异常操作，如权限提升、批量数据导出等。实时监控则能在威胁发生时立即触发警报或采取防护措施。结合入侵检测系统和异常行为分析技术，能够更高效地识别潜在威胁。

（4）数据备份与灾难恢复

数据备份与灾难恢复是应对数据丢失或损坏的核心手段。一套完整的备份策略应包括全量备份、增量备份和差异备份，并确保备份数据的存储地点安全可靠。此外，灾难恢复计划

（DRP）需要详细定义系统恢复的步骤和优先级，并通过定期演练来验证恢复的有效性。

（5）安全更新与漏洞管理

数据库系统的漏洞是攻击者入侵的主要入口。定期进行漏洞扫描、及时更新安全补丁以及关闭不必要的服务和端口，可以有效减少攻击面。同时，安全团队还需关注数据库供应商发布的漏洞公告，并评估其对系统的影响。

2. 数据库安全控制技术

除了上述体系的构建，数据库安全控制技术在保障数据的安全性和系统的稳定性方面起到了至关重要的作用。

（1）数据脱敏技术

数据脱敏技术通过将敏感数据替换为虚拟数据，在不影响数据使用的情况下保护隐私信息。例如，在系统测试或数据共享中，开发者和测试人员可以访问脱敏后的数据，而无须接触真实数据。静态脱敏适用于测试环境，动态脱敏则可以在生产环境中实时保护数据。

（2）数据库防火墙

数据库防火墙能够通过分析SQL语句和访问模式来识别和阻止异常请求。例如，它可以阻止SQL注入攻击或不符合安全策略的访问行为。结合行为分析技术，数据库防火墙还能动态调整策略以应对新型威胁。

（3）分布式数据库的安全保护

在分布式环境中，数据被分散存储于多个节点，安全管理的复杂性显著增加。分布式数据库需要在节点之间建立安全的通信通道，同时采用分布式身份认证和访问控制机制。此外，通过数据分片和冗余备份，可以进一步提高系统的抗攻击能力。

3. 数据库安全发展

随着信息化和数字化的深入发展，数据库安全技术面临着前所未有的挑战，也迎来了更多机遇。人工智能和机器学习技术正在快速改变数据库安全技术的格局。通过这两项技术可以进行异常检测与预测、自适应安全策略、自动化响应。随着企业逐渐迁移到云端，云数据库的安全需求愈发重要，如采用容器化防护、无服务器计算环境的数据库安全措施，以及云环境下的密钥管理。为不同用户提供严格的逻辑隔离机制。进一步集成智能化灾备技术，通过全球化分布的容灾网络，实现更加可靠的数据恢复和业务连续性。另外数据库安全技术的标准化也将迎来新的发展，如为不同数据库系统（如MySQL、PostgreSQL、Oracle）设计统一的认证、加密和访问控制标准。通过开放的API和标准化协议，企业可以更轻松地整合多个数据库的安全审计和监控数据，构建全局的安全视图。

4. 零信任架构下的数据库安全

在数据库安全中引入零信任架构，可有效降低数据泄露和内部威胁风险。零信任要求所有数据库访问都经过严格验证，包括动态访问控制、多因素认证和细粒度权限管理，以确保仅授权用户能访问特定数据。结合行为分析与持续监控技术，能够实时检测异常查询和恶意访问，同时通过数据微分段策略，限制未经授权的横向移动，确保数据库在复杂网络环境下的安全性和可控性。

知识延伸：误删除文件的恢复

对于个人使用计算机来说，可能会发生文件误删除操作。正常情况，删除的文件会存放到“回收站”中，如果清空了回收站，或者在删除文件时按Shift+Delete组合键，就会将文件彻底删除，无法通过回收站找回。这种情况下就需要使用数据恢复工具进行恢复。恢复的原理如下。

硬盘相当于一个仓库，被划分为很多小的存储单元，像储物柜一样，写入数据相当于在储物柜中放置物品，读取则相当于在存储柜中取物品。存储柜编号，在取物品时则会读取这张登记表。删除的原理相当于在存储柜的物品上贴上“已删除”的标签，并在登记表上登记。清空回收站或者彻底删除的情况，则是除贴上删除标签外，还在登记表上抹除了物品的属性信息。此时则无法通过登记表找到该物品。再放置物品时，只要存储柜有“已删除”标签，就会直接覆盖原物品。

其实在彻底删除后，其物品还存在储物柜中，只是没登记，存储柜也贴了删除标签。但并不是立刻删除，而是等下一批物品使用该储物柜时才会覆盖。只要没再存储数据，物品就还在。

恢复软件相当于到每个储物柜去查找，重新登记所有的物品信息。如果用户删除的这批物品没被覆盖，那么就可以取出来，这就是修复的原理。数据修复从原理上是可以的，但无法保证百分之百成功。利用一些高级软件和高级设备，可以提升修复率，但代价非常大。所以做好数据备份工作很有必要。

在PE中会自带一些数据恢复软件，可以进行数据恢复，而且常见的数据恢复软件的操作基本类似，包括扫描、筛选和恢复。下面以PE中经常使用的磁盘管理软件DiskGenius为例进行介绍。该软件不仅是磁盘的分区管理软件，还可以进行数据的扫描及恢复。用户可以在其他设备上制作PE启动U盘，然后将U盘插入误删除文件所在的计算机，重新启动计算机到PE环境中，使用恢复软件进行数据的扫描及恢复。下面介绍具体的操作步骤。

Step 01 打开DiskGenius后，选择误删除文件所在分区，本例选择“H盘”，单击界面中的“恢复文件”按钮，如图8-8所示。

Step 02 参数保持默认值，单击“开始”按钮，如图8-9所示。

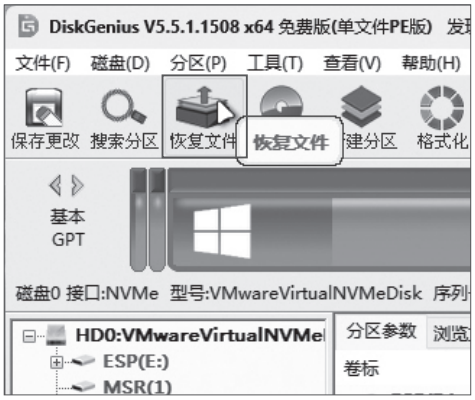

图 8-8

图 8-9

Step 03 DiskGenius扫描后，会找到所有删除的文件，如果文件较多，可以在软件上方的筛

选区中输入筛选的条件，如本例筛选图片，输入“*.jpg”，取消勾选“正常文件”“系统文件”“重复文件”复选框，然后单击“过滤”按钮，筛选出符合条件的误删除文件，如图8-10所示。

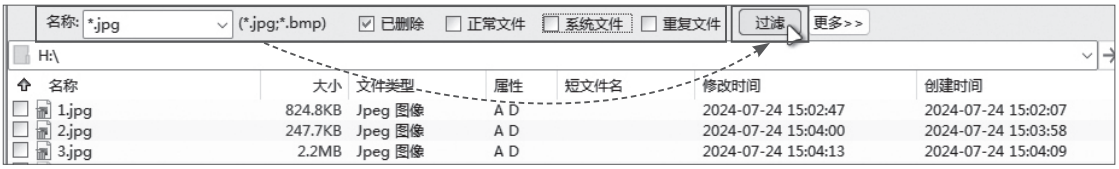

图 8-10

Step 04 勾选需要恢复的文件，在文件上右击，在弹出的快捷菜单中选择“复制到‘桌面’”选项，如图8-11所示。

Step 05 接下来就可以到桌面上查看恢复的文件，如图8-12所示。

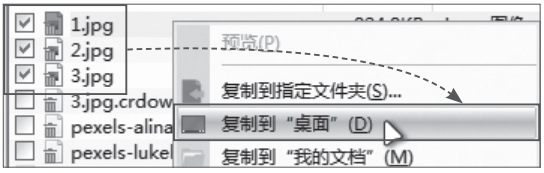

图 8-11

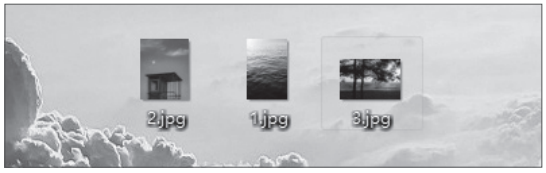

图 8-12

注意事项 误删除发生后的操作

当发生重要数据误删除的情况，应立即关闭计算机的电源（特殊情况还可以直接给计算机断电），不能再次进入系统。可以进入PE中（它相当于另一个系统，并且不会向系统分区进行写入）进行数据恢复，或者将硬盘拆出来，放在其他计算机上，或者交给专业人士恢复。科学地采取各种手段，可以极大地提高恢复的可能性。但读者需要明确，任何人都不可能保证一定能够恢复误删除的数据。在恢复的过程中，不要将恢复文件恢复到删除所在的分区，以免覆盖原始删除文件。

知识拓展

其他恢复工具

常用的其他恢复工具还有专业的7-Data，如图8-13和图8-14所示、万兴恢复专家、EasyRecovery、R-Studio等。但为了提高恢复的效果，不建议用户直接在正常的系统中使用，以免新数据覆盖了被误删除的软件数据，而应该进入PE中启动这些软件尝试恢复。而且在PE中，这些软件都经过了优化，可以突破一些限制，进行恢复操作。

图 8-13

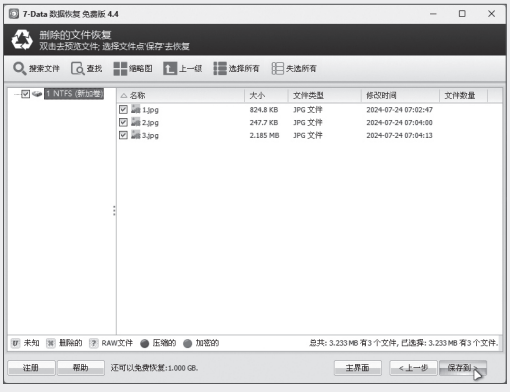

图 8-14

实战训练

实战1：Windows系统的备份与还原

1. 实战目的

了解系统备份的原理和实现方式，掌握通过DISM++备份与还原分区的操作步骤。

2. 实战要求

在PE系统中，使用DISM++工具对Windows系统的系统分区进行备份及还原，并了解增量备份的操作。

3. 实战步骤

Step 01 将制作好的启动U盘插入计算机，启动计算机到PE环境，打开备份工具DISM++。

Step 02 选择系统分区后，选择“工具箱”选项，找到并打开“系统备份”功能。

Step 03 设置好保存的说明、映像保存的位置后，就可以执行备份了，如图8-15所示。

Step 04 再次执行该操作并保存到同一映像，可以执行增量备份，如图8-16所示。

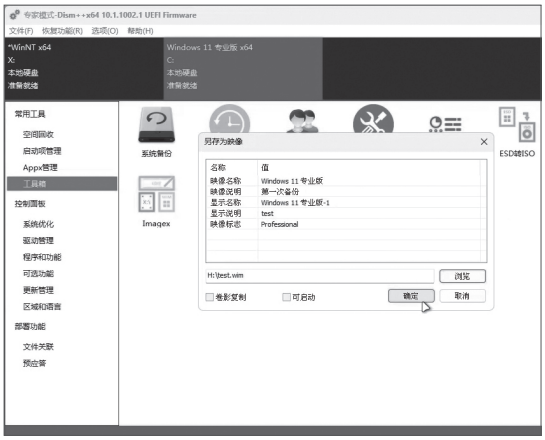

图 8-15

图 8-16

Step 05 还原时，可以使用该软件，也可以使用其他支持“.wim”格式的安装软件，执行系统还原，选择映像后，选择还原的增量备份，勾选“添加引导”和“格式化”复选框，即可还原，如图8-17所示。

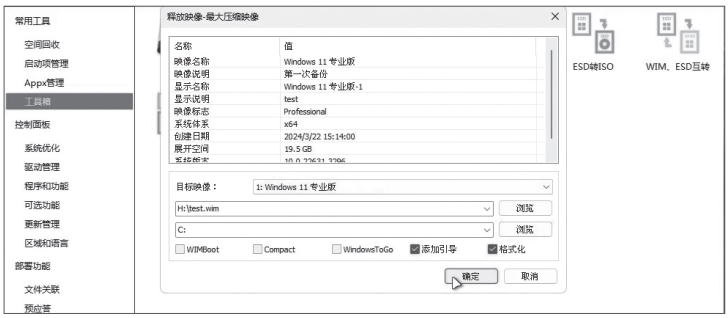

图 8-17

4. 实验点拨

① 使用系统自带的各种备份还原功能都不是特别稳定和合适，例如时间长、备份的文件大、还原时不能解决问题、还原条件苛刻等。

② DISM++通过使用系统的DISM功能进行备份还原，速度快、占用磁盘空间少，还可以进

行增量备份，多种工具都可以还原，非常灵活。用户可以使用各种工具制作PE系统，基本上都会含有该工具。

③ 增量备份时，主要填写各种信息，以区别不同版本。

实战2：使用火绒查杀病毒

1. 实战目的

了解火绒安全软件的使用方法，学习使用火绒安全软件查杀病毒。

2. 实战要求

在Windows系统中，下载并安装火绒安全软件，升级后，进行病毒的查杀。

3. 实战步骤

Step 01 在官网中下载安装程序，并部署在系统中。

Step 02 打开火绒安全软件，执行升级操作，如图8-18所示。

Step 03 升级完毕后，单击“快速查杀”按钮，启动快速查杀功能，如图8-19所示。

图 8-18

图 8-19

Step 04 此时火绒会对包括引导区、系统进程、启动项、服务与驱动、系统组件以及系统关键位置进行查杀，如图8-20所示。查杀完毕会弹出查杀报告。

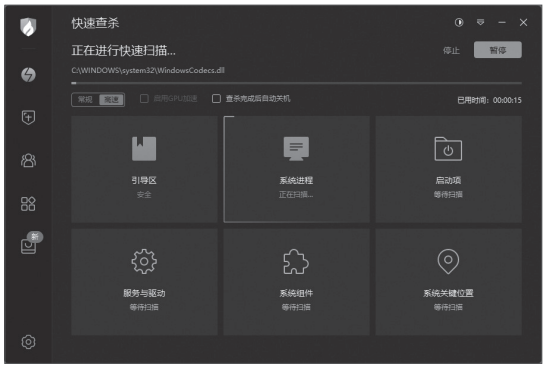

图 8-20

4. 实验点拨

① 一般杀毒软件有三种扫描方式：快速查杀，主要扫描系统关键位置，速度较快，但不全面，随时可以进行；全盘查杀，包括系统中所有的位置、硬盘中的所有文件等，全面但速度较慢，建议一周扫描一次即可；自定义扫描，手动设置扫描的内容，比较灵活，可以设置一些下载目录进行扫描。通常的安全软件都有这三种扫描模式，用户可根据实际情况选择扫描方式。

② 火绒软件本身除了防毒杀毒外，还包含防火墙的功能，可以对网络中的流量进行监控和管理；可以限制联网程序的联网速度；禁止程序启动及开机启动、修复系统、诊断网络故障等。