NO：Green Trend(GT2019-SEB303)

安易备技术说明

文档变更

版本号	修订日期	描述
1.1	2018.03.10	初版
1.2	2018.05.22	修订
1.3	2019.01.18	修订
1.4	2019.02.14	修订

目录

第 1 章 基础知识 5

1.1 当前 IT 数据安全的主要威胁？ 5

1.2 安易备 是什么？ 6

1.3 为什么说是针对数据库、勒索病毒? 6

1.4 如何做到勒索病毒下的更安全？ 6

1.5 具体做了哪些安全措施？ 7

1.6 安易备怎么工作的？ 8

1.7 如何做到自身安全 9

1.8 如何做到数据获取的安全 10

1.9 灾备过程对生产环境有影响吗？ 11

1.10 当系统数据损坏或遭遇病毒，安易备如何发出告警？ 11

第 2 章 部署与还原 12

2.1 安易备的部署模式 12

2.2 对数据库的版本有要求吗？ 13

2.3 安易备需要在生产环境安装插件或 AGENT 吗？ 13

2.4 安易备需要什么样的安装环境 13

2.5 安装过程需要停机吗？需要多少时间？ 13

2.6 安易备对服务器、存储的介质有特殊要求吗？ 13

2.7 我的应用程序很复杂，数据库的表结构也很复杂，是否会对安易备造成影响？ 14

2.8 安易备无法访问如何还原数据？ 14

第1章 基础知识

1.1 当前 IT 数据安全的主要威胁？

- **计算机病毒**

  计算机病毒及变种病毒肆虐，影响计算机软件、硬件的正常运行，破坏数据的正确与完整，甚至导致系统崩溃等重大恶果，特别是一些针对盗取各类数据信息的木马病毒等。

- **黑客攻击**

  电脑入侵、账号泄漏、资料丢失、网页被黑等等也是企业信息安全管理中经常遇到的问题。其特点是往往具有明确的目标。当黑客要攻击一个目标时，通常是首先收集被攻击方的有关信息，分析被攻击方可能存在的漏洞，然后建立模拟环境，进行模拟攻击，测试对方可能的反应，再利用适当的工具进行扫描，最后通过已知的漏洞，实施攻击。然后就可以读取邮件，搜索和盗窃文件，毁坏重要数据，破坏整个系统的信息，造成不堪设想的后果。

- **数据信息存储介质的损坏**

  在物理介质层次上对存储和传输的信息进行安全保护，是信息安全的基本保障。物理安全隐患大致包括三个方面：一是自然灾害(如地震、火灾、洪水、雷电等)、物理损坏(如硬盘损坏、设备使用到期、外力损坏等)和设备故障(如停电断电、电磁干扰等)；二是电磁辐射、信息泄漏、痕迹泄露(如口令密钥等保管不善)；三是操作失误(如删除文件，格式化硬盘、线路拆除)、意外疏漏等。

- **自身数据信息安全管理不完善**

人为因素。人为因素包括人为的无意失误和人为恶意攻击。

安易备是一款集自动化、智能化、高安全为一体的备份产品，它的责任是让数据有一道安全的防线，不被外界的因素所影响。

1.2 安易备 是什么？

安易备是针对数据库的灾备软件，是核心数据的最后一道防线。

1.3 为什么说是针对数据库、勒索病毒？

企业最重要的就是核心数据，所以最容易被定位为攻击目标。

勒索病毒和容灾的场景下，数据库体量大，恢复难、技术要求高。

同时数据库事务高一致性的特性导致极端情况下花大力气恢复出来的数据竟然无法正常访问。

安易备减去了操作系统，文件系统，虚拟机这些内容而专注于数据库，因为专注，所以在数据库层面的灾备可以做到更针对、更专业、更安全、更快速。

1.4 如何做到勒索病毒下的更安全？

安全主要在 2 点:

1. 自身更安全 ：安全配置层、访问机制层、数据保护层做到病毒下的高安全

而传统灾备是针对灾备不是针对病毒，很多病毒情况下自身安全不足。

2. 获取数据的安全 ：主动拉取、SQL 文件格式解析、实时演练、预警告警

针对数据库，日志的解析，数据文件格式的解析、分析就是我们的核心 。

1.5 具体做了哪些安全措施？

自身安全:

安全配置层——最小开放，最大防护

1. 内核裁减版系统，最大化安全设置（端口、防火墙、应用、管理权限等），保证灾备机无法被入侵。
2. 最小化网络接入，避免病毒程序网络分析。
3. 最小化功能开放，专机专用，避免病毒程序通过应用、服务漏洞入侵。

访问机制层——单向访问

1. 任何机器无法通过网络直接访问安易备，无法 ping 通。
2. 任何文件只由安易备以“拉”的方式主动获取。
3. “拉”取的文件必须符合数据库安全可用标准，以排除感染或加密文件。

数据保护层——从演练到预警保证数据可用

1. 实时数据灾备演练，保证灾备必可用。
2. 文件识别、使用恢复，全程监控预警，保证数据安全、有效。
3. 每日灾备演练成功后即离线，只允许物理访问。

灾备同步

日志变化级同步

使用数据库日志，实时捕获日志变化，保证数据库级别事务完整性、一致性。

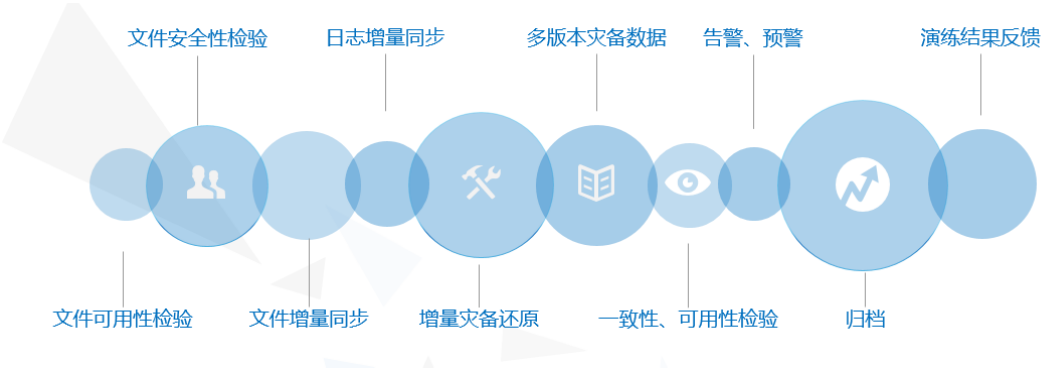
如：文件被病毒加密，磁盘级别或文件级依然会把加密文件拷贝作为灾备，而安易备自动解析日志格式（for SQL Server）不符合则阻止传输，并告警。

灾备演练

传统灾备缺少实时的灾备可用性验证，数据被病毒感染、损坏、不一致、不可用无法被发现，只有在真正发生灾难出现问题时才得知备份不能使用或已经损坏。

安易备在灾备的前、中、后校验灾备数据的可用性，并实时进行灾备演练 100%保证灾备数据的可用性、完整性，同时可以及时发现源数据库的加密、损坏，提出预警和告警。

灾备演练过程



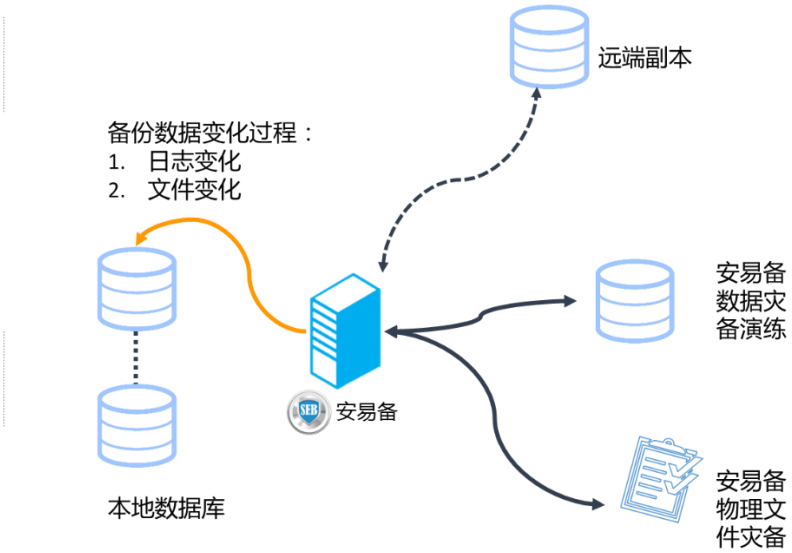
1.6 安易备怎么工作的？

安易备共分 3 部分：灾备文件获取、实时还原演练、文件和实时可用数据双存储

灾备文件获取：通过日志解析、日志同步和文件拷贝的两种方式获取数据变化

实时还原演练：从文件检测、同步、还可用检验、监控、告警，保证数据可以实时还原并 100%可用。

文件和实时可用数据双存储：安易备中会保留三种灾备数据，实时可使用的数据，实时备份文件、拷贝的原始备份文件，同时也支持提供远端灾备



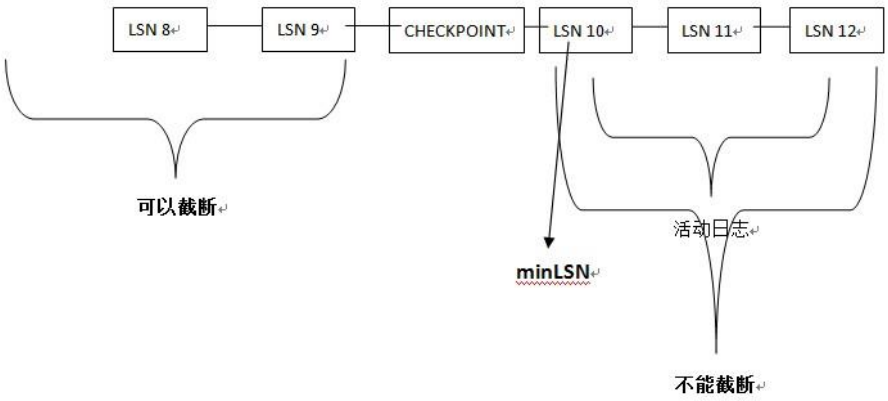
1.7 如何做到自身安全

安易备的自身防护分为三层:

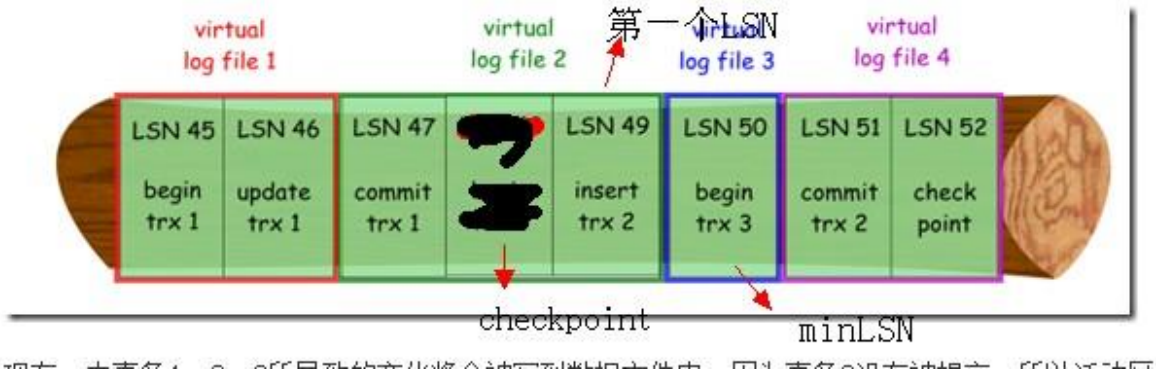
1. 网络层/系统层: 采用单项访问，无法在网络中被访问; 系统环境极简，安装部署，只能通过命令行操作
2. 应用层: 内置多重防火墙,应用无法对外提供访问,功能单一,服务、端口等均不对外开启
3. 硬件层: 在数据文件的防护上做到，硬件灵活调配，数据落盘则物理隔离

1.8 如何做到数据获取的安全

内核程序（SEB Core）以文件分析和驻留实例的内核中的两种方式检测数据变化，监测数据库内数据的变化，同时还要分析引起数据变化的文件格式是否满足 SQL 日志标准格式（文件格式检验）



经智能分析后，还需进行文件安全型可用性校验，防止文件极端情况下被病毒感染带来破坏影响（如编译日志文件内容类极端情况）



1.9 灾备过程对生产环境有影响吗？

灾备过程分为三大过程：

1. 文件的安全、可用检查

2. 灾备数据同步

3. 灾备数据还原演练并告警

其中文件检查阶段、还原演练阶段均对生产环境无任何影响，灾备数据同步阶段可能会占用部分文件传输的网络资源，但影响可以忽略不计。

整个数据校验、传输、演练过程均与生产环境异步进行，不会影响正常事务的进行。

1.10 当系统数据损坏或遭遇病毒，安易备如何发出告警？

安易备在三大过程提供告警：

1. 文件检测、安全检测

2. 恢复演练

3. 可用性检测

安易备告警信息接收三种途径：

1. 日常 SQL 查询，定期手动检测

2. 配套产品告警，如：SQL 专家云

3. 配置邮件、WebService 接口

第2章 部署与还原

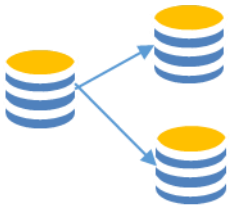
2.1 安易备的部署模式

安易备支持灵活的部署及灾备方式：

1. 1 对 1 适用于核心系统单独灾备，可以应对灾难发生时将安易备直接用于生产，快速恢复业务

1对1

2. 1 对多 适用于核心系统，本异地灾备，安全系数更高，灾难发生时将本/异地安易备直接用于生产，快速恢复业务



1对多

3. 多对 1 适用与数据集中灾备，灾难发生时安易备中依然有数据留存，可以用安易备的数据恢复到生产环境，保证数据不丢失

多对1

4. 多对多 综合前三种模式，重要系统与其他非核心综合考量，满足前三种场景

多对多

2.2 对数据库的版本有要求吗？

安易备可用于 SQL Server2000-2016 所有版本，即支持所有 SQL Server 数据库。

2.3 安易备需要在生产环境安装插件或 Agent 吗？

安易备属于“非入侵“式设计，无须在生产环境安装任何插件或 Agent

2.4 安易备需要什么样的安装环境

安易备提供软件版、硬件一体机两种模式

软件版：用户只需要参照 2.1 章节的部署模式准备相应的硬件机器（不建议使用虚拟机）

2.5 安装过程需要停机吗？需要多少时间？

安易备提供的软件版、硬件一体机两种模式均可在线完成配置，无须停机，初次程序虚拟化需要较长时间，根据灾备数据量大小而定。

2.6 安易备对服务器、存储的介质有特殊要求吗？

安易备作为核心数据的最后一道防线，对服务器、存储介质无任何要求，根据生产环境的数据量，业务复杂度，灾备演练的过程需要消耗一定的自身资源，建议配置 2 路 16G 内存以上配置的服务器。

2.7 我的应用程序很复杂，数据库的表结构也很复杂，是否会对安易备造成影响？

安易备以数据结果、变化过程为导向，应用与表结构的复杂不会对安易备造成影响。

2.8 安易备无法访问如何还原数据？

安易备作为最后一道防线，日常工作确实无法访问，但灾难发生，需要数据还原时可根据《安易备日常操作手册》流程，暂时关闭访问、应用、网络等限制。取出安易备中的数据副本。待到生产环境恢复后再根据流程开启安全设置即可。