

vinchin

创新安全基座 为TiDB注入可靠恢复新韧性

主讲人：云祺科技-王斌



目 录

PART 01 云祺 TiDB数据保护方案

PART 02 云祺 TiDB数据保护原理

PART 03 云祺 TiDB数据保护方案亮点

PART 04 应用场景

PART 01

TiDB数据保护方案



TiDB数据保护挑战

在万物互联的时代，数据库作为核心业务系统，面临诸多安全风险

硬件故障

误操作

SQL注入

越权访问



勒索攻击形式严峻

AI技术被滥用后，勒索病毒的变种速度与攻击威力与日俱增，防不胜防是常态



合规要求日趋严格

银行、证券、医疗等行业除备份要求外，还要求定期进行恢复演练确认响应效率

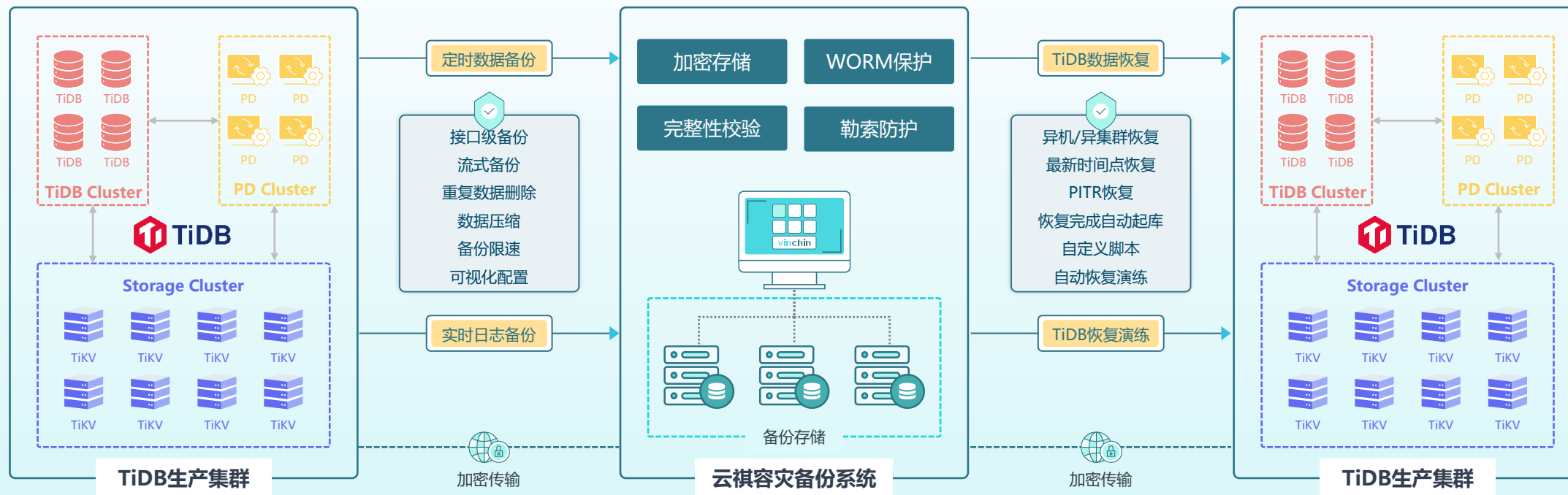


运维管理工作量大

分布式数据库数据一致性要求高，传统备份方案操作复杂，难以有效保护TiDB



云祺 TiDB数据保护解决方案



原生深度对接

流式一致性备份

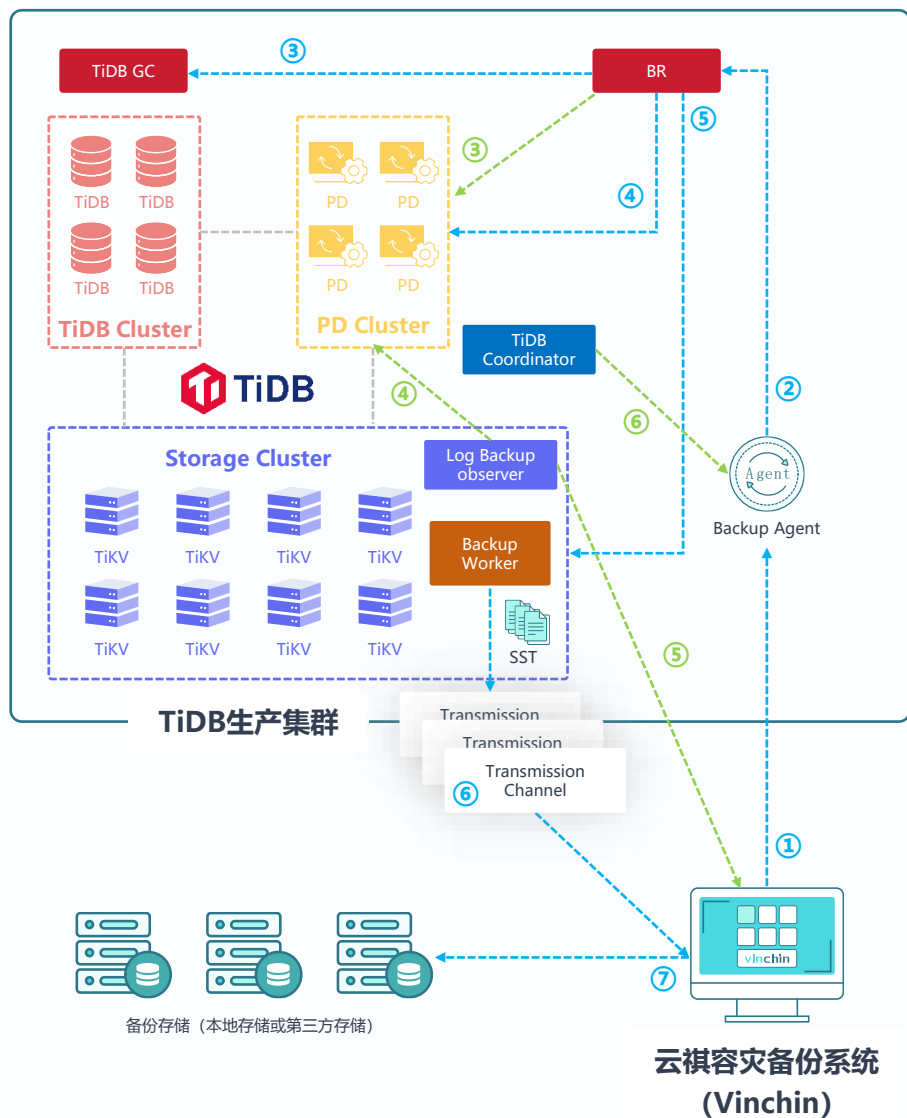
自动恢复演练

勒索后安全恢复

PART 02

TiDB数据保护原理





TiDB数据备份

- 1、备份系统发送TiDB数据备份指令给备份客户端;
- 2、客户端向BR发起备份请求, BR接收备份命令, 并获取数据库快照与备份存储地址;
- 3、BR配置 TiDB GC, 防止要备份的数据被 TiDB GC 机制回收;
- 4、BR访问 PD, 获取所有 TiKV 节点访问地址以及数据的 Region 分布信息;
- 5、BR发送备份请求给TiKV, TiKV 接受备份请求, 初始化 backup worker;
- 6、backup worker 读取对应数据, 通过传输通道将数据传输给vinchin;
- 7、vinchin对数据进行处理后, 写入备份存储;
- 8、BR从TiKV获取数据备份结果, 完成后开始备份sechema、Metadata等元信息, 并传输到备份存储。

TiDB实时日志备份

日志备份将在数据备份任务启动时自动启动, 启动后将持续运行, 日志备份的启动过程如下:

- 1、备份系统发送TiDB日志备份指令给备份客户端;
- 2、客户端向BR发起备份请求, BR接收备份命令, 获取日志起始位置与备份存储地址;
- 3、BR并在PD注册日志备份job;
- 4、每个 TiKV 节点的log backup observer实时监听 PD 中日志备份job的创建与更新, 持续备份指定范围的日志;
- 5、各log backup observer持续将日志备份数据传输到Vinchin;
- 6、备份客户端持续从Coordinator 获取日志备份状态, 并同步到Vinchin。

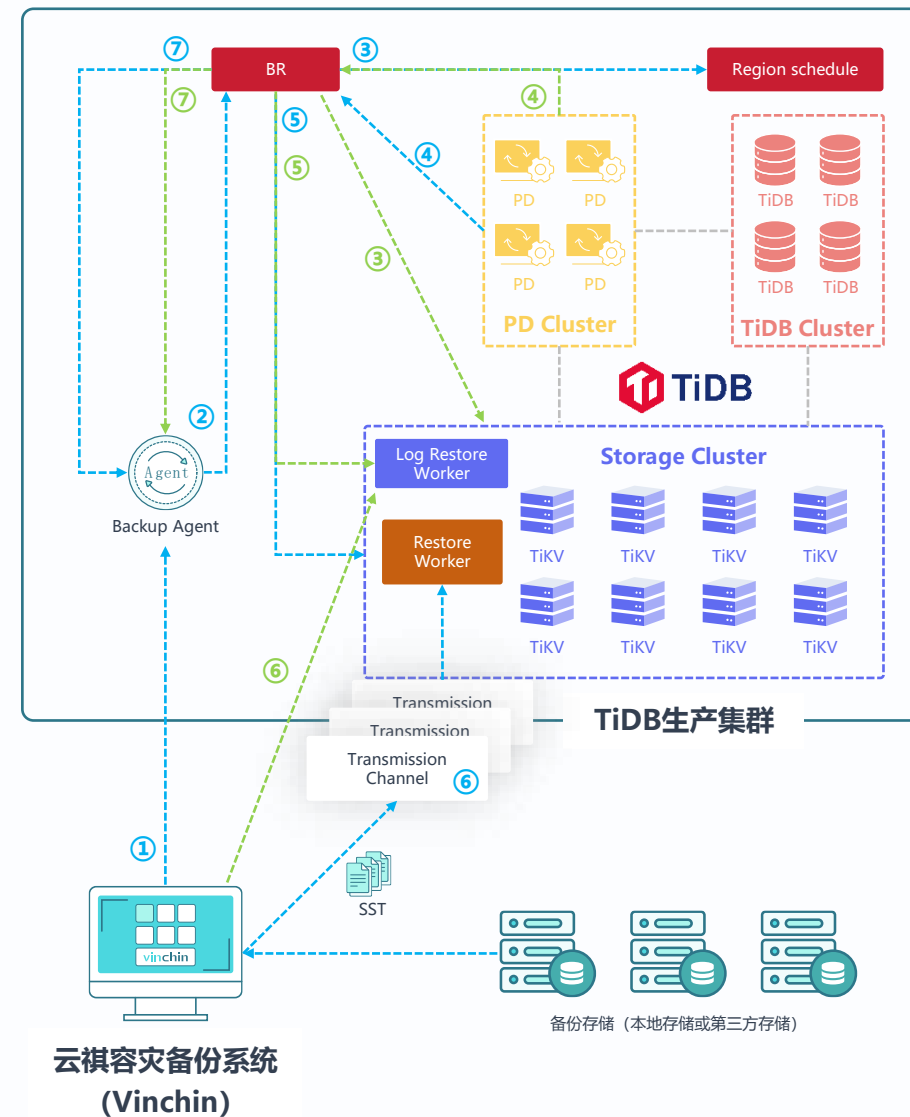
云祺 TiDB数据库恢复原理

TiDB备份点恢复

- 1、备份系统发送TiDB数据恢复指令给备份客户端；
- 2、客户端向BR发起恢复请求，BR接收恢复命令，并获取备份数据的存储地址以及需要恢复的内容；
- 3、BR请求 PD 在恢复期间关闭自动 Region schedule。；
- 4、BR获取需要恢复的schema、database等数据以及恢复目标Region；
- 5、BR发送恢复请求给TiKV，TiKV 接受恢复请求，初始化 restore worker；
- 6、restore worker通过传输通道从Vinchin下载数据，进行数据写入；
- 7、客户端持续查询BR从各个TiKV获取的恢复结果，确认恢复是否完成。

TiDB指定时间点恢复/回退

- 1、备份系统发送TiDB数据恢复指令给备份客户端；
- 2、客户端向BR发起恢复请求，BR接收恢复命令，获取全量备份数据地址、日志备份数据地址以及需要恢复的时间点；
- 3、BR按【TiDB备份点恢复】流程先进行全量备份数据恢复；
- 4、BR读取日志备份数据，并从PD获取所有 Region 和 KV range 的对应关系；
- 5、BR创建恢复请求给TiKV，TiKV 接受恢复请求，初始化 log restore worker；
- 6、log restore worker持续从Vinchin下载需要恢复的数据，并写入到对应位置；
- 7、客户端持续查询BR从各个TiKV获取的恢复结果，确认恢复是否完成。



PART 03

TiDB数据保护方案亮点



TiDB深度对接，从可靠备份到可信恢复

构建与TiDB原生架构相匹配的数据保护层



1

原生适配

与TiDB分布式结构深度集成
对接TiDB原生备份能力
在线备份，无需改造现有架构

2

可靠备份

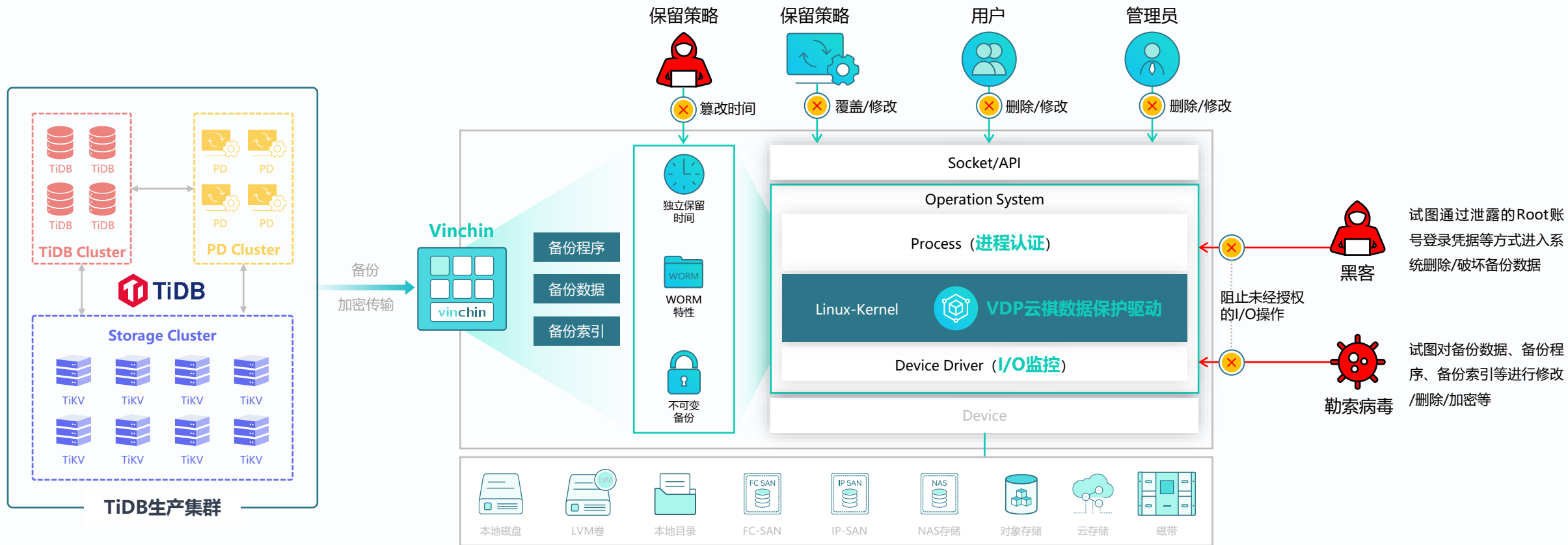
保障TiDB备份数据一致性
简化备份恢复，减少操作失误风险
RPO可达分钟级，更少数据丢失

3

可信恢复

国产行业生态融合，可信灾备平台
支持秒级PITR（任意时间点恢复）
端到端全链路加密，防止数据泄露

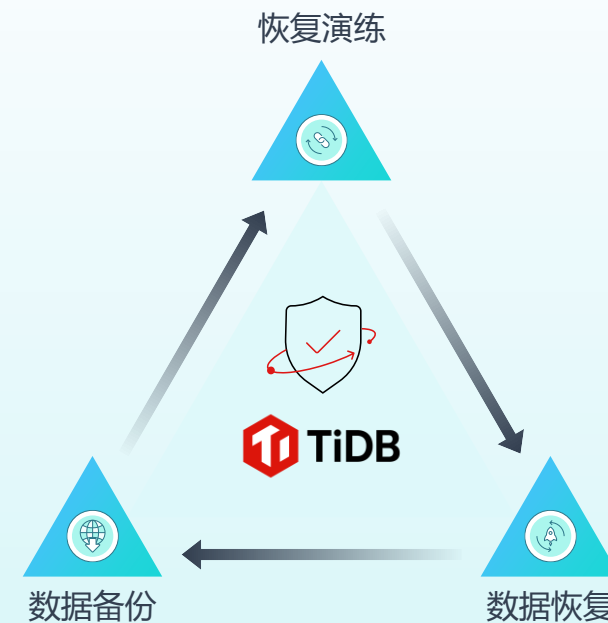
防勒索备份，护航TiDB数据安全



零信任体系，以不变应万变

自动恢复演练，从“有备份”到“可恢复”的安全闭环

超越备份，以持续演练，确保灾备计划持续就绪



持续循环，让安全能力“活”起来

消除不确定性

不要等到恢复时才发现备份数据不可用、操作流程不规范、资源准备不充分、恢复配置不正确等问题。面对不同故障场景，云祺通过自动恢复演练，旨在将“理论上能恢复”的不确定变为“定期验证过”的确定性，帮助用户确保每次恢复都能成功。

驱动持续改进

灾备建设不是“一劳永逸”，数据保护也不是简单的做“是”与“否”的选择，运维人员需要根据实际的业务要求、资源条件及时调整灾备预案。云祺提供可视化的演练报告，帮助客户不断优化灾备策略与流程，确保确保RTO/RPO持续达标，恢复就绪。

可视化引导式操作，减轻运维负担

vinchin



灵活易用·轻松备份

- 常规备份功能可在图形化界面进行启用/关闭，只需简单的点击或输入数值即可方便的进行设置，降低操作复杂度
- 可在界面直接对脚本进行编辑，设置自定义参数，无需登录数据库后台，更支持导入多个现成脚本，一键应用
- 支持将参数设置持久化生成到脚本模板中，新建备份可直接使用已有脚本，无需再次编辑，减少重复的参数配置操作

全部图形化界面操作，无需后台敲命令，写脚本



Vinchin Data Protect Solution for TiDB



更可靠

原生深度对接TiDB，数据一致性有保障；采用流式备份方案，减少对生产环境的资源占用并提高备份性能

更合规

自动化灾难恢复演练，无需人工干预，帮助用户持续优化TiDB数据保护策略，提升数据安全管理水平与故障响应效率

更安全

全链路端到端加密，防止备份数据泄露；WORM防护有效防止勒索病毒或误操作篡改、删除TiDB备份数据

更简单

All in Web，支持对接海量TiDB集群统一灾备；可视化引导式操作，实时查看备份恢复任务进度与状态，大幅降低灾备管理难度

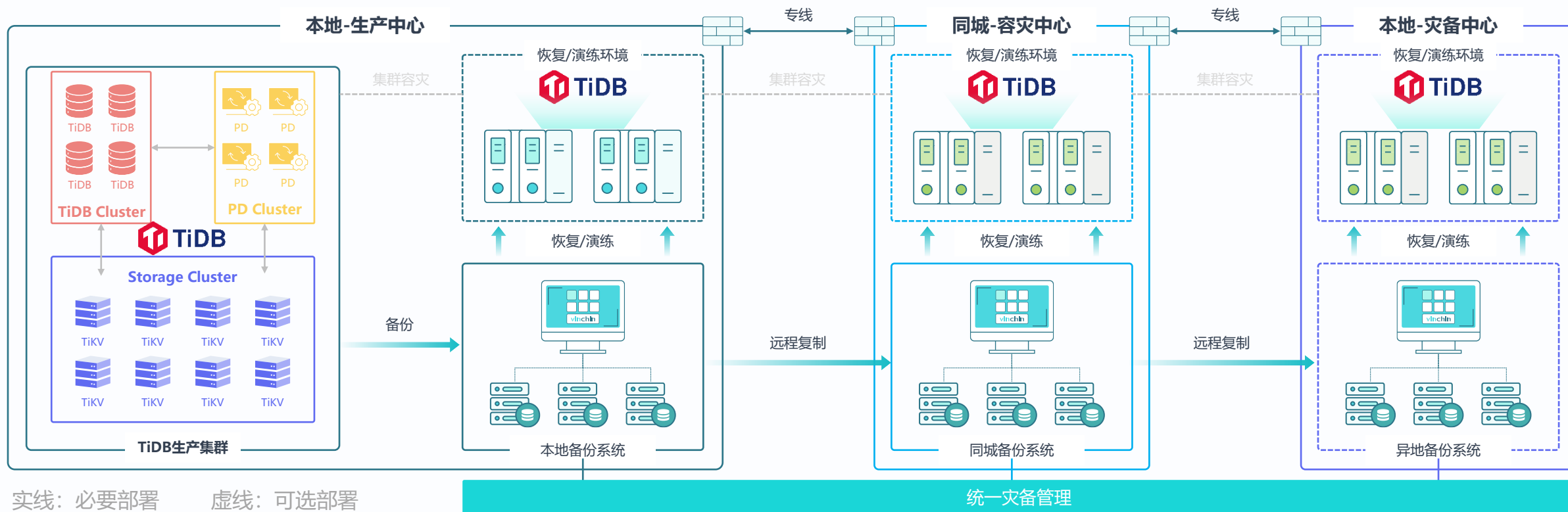
PART 04

应用场景



TiDB本地备份与异地数据容灾

云祺支持无缝接入TiDB现有跨地容灾架构，只需在需要的位置部署云祺容灾备份系统或备份一体机即可。为避免机房级灾难，云祺支持将本地备份数据远程复制到异地灾备中心，故障发生时，可直接从异地恢复TiDB数据。用户也可根据实际资源条件或数据容灾要求扩展为两地三中心灾备方案。



异地数据容灾

异地数据容灾，即使遭遇区域性灾难，异地灾备站点也有数据可供恢复

窄带宽传输

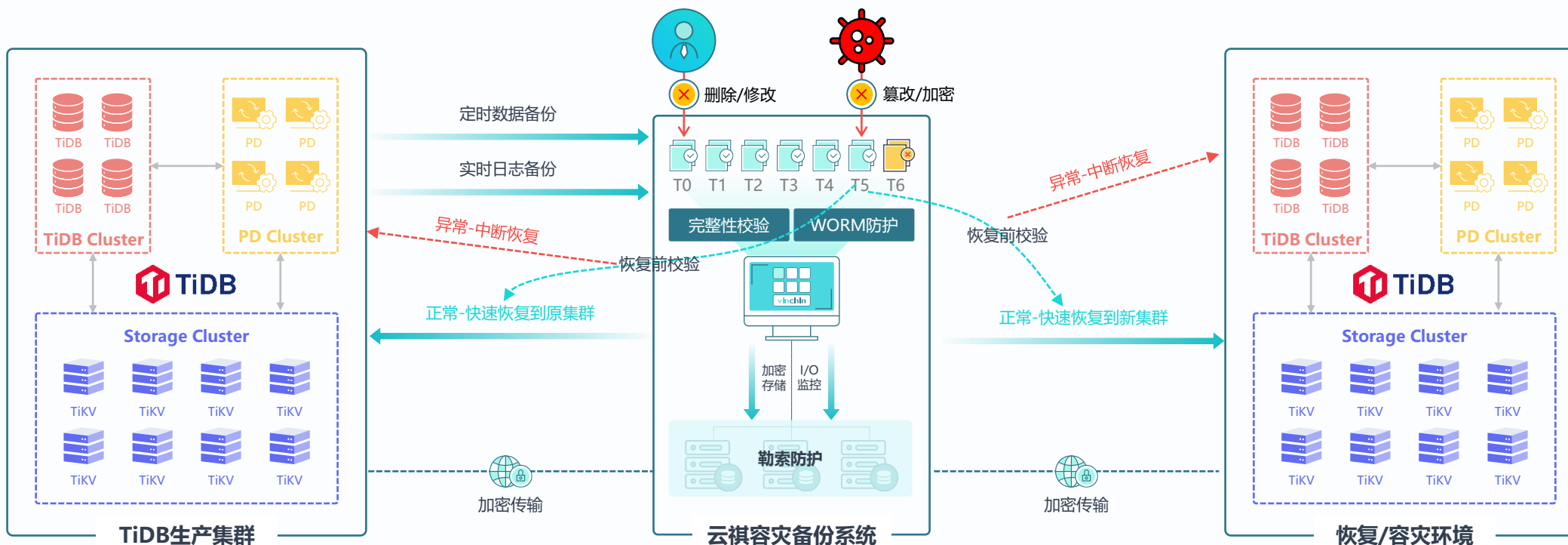
通过源端压缩、断网续传等技术减少窄带宽限制，提升远程数据容灾效率

跨域统一管理

两地三中心接入统一管理平台，提供跨区、跨地的灾备可视化管理能力

勒索后的数据恢复

勒索攻击发生后，我们总是希望通过备份数据恢复TiDB，此时备份数据的安全性受到挑战，必须确保备份数据未受篡改，以此恢复出干净的TiDB数据。用户可通过云祺的不可变备份数据，实现TiDB的安全恢复。



安全恢复

3-2-1-1-0-0体系化防勒索，有效阻止勒索病毒感染备份，确保安全恢复

精准恢复

快速将TiDB集群还原至已备份的任意时刻，并支持恢复后自动验证数据

异常熔断

恢复前将快速校验备份数据安全性，异常时自动中断恢复，避免无效恢复

vinchin

THANKS



云祺公众号



云祺视频号

