

Open Source AceCon

2021 智能云边开源峰会

AI x Cloud Native x Edge Computing

人工智能 × 云原生 × 边缘计算

TiDB Cloud 云原生数据库未来规划

王鹏飞@PingCAP

资深专家

- 云原生的朴素理解
- 成本
- 安全
- 容灾
- 企业级能力

云原生的朴素理解

——以点带面

- “弹”
- 面向云的安全
- “云原生”的容灾
- “云原生”的企业级能力

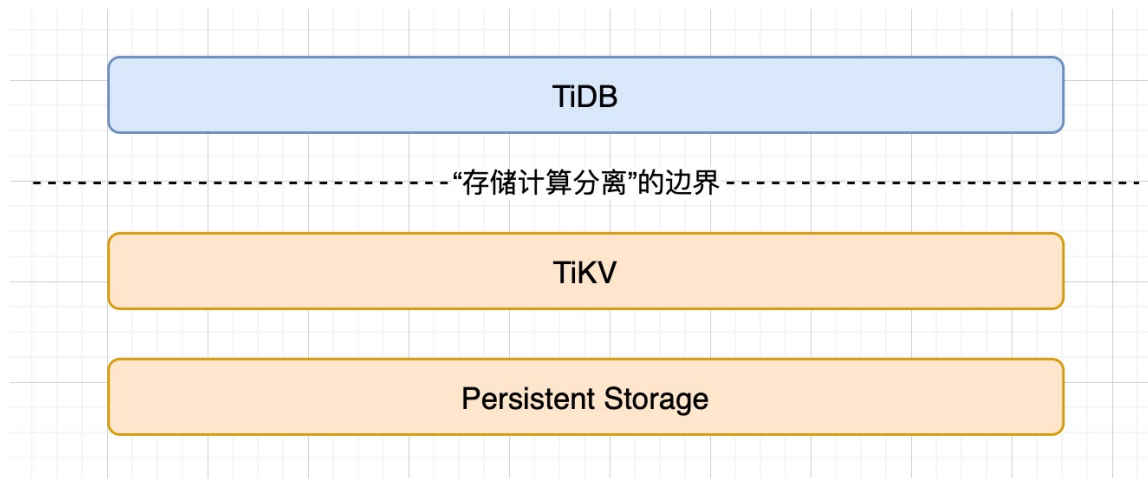
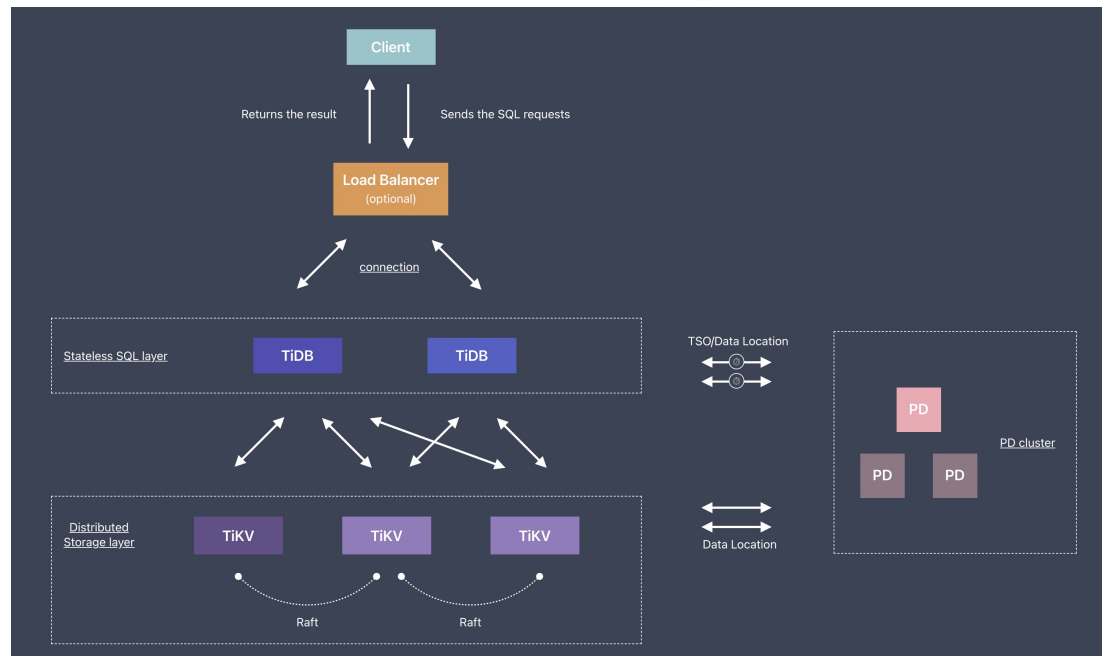


- 云原生的朴素理解
- **成本**
- 安全
- 容灾
- 企业级能力

成本

面向传统的 IDC 设计，而不是云

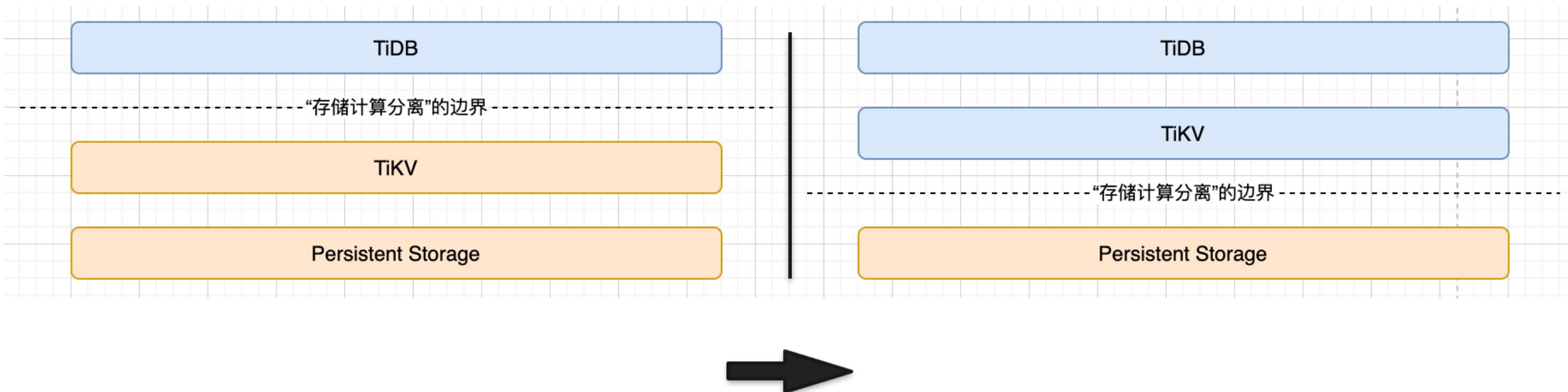
- 存储
 - Persistent Storage = 磁盘
 - 磁盘上 3 份拷贝
 - 不同磁盘，性能、可靠性没有差异
 - 不同磁盘，价格没有差异
 - 3 份拷贝 \approx 6 个 9 的可靠性
- 计算
 - TiDB + Coprocessor@TiKV
- 存储计算分离边界比较模糊，处理不同负载配比的场景比较困难
 - 以扩容为例，增加一个 TiKV 可能浪费计算资源



成本

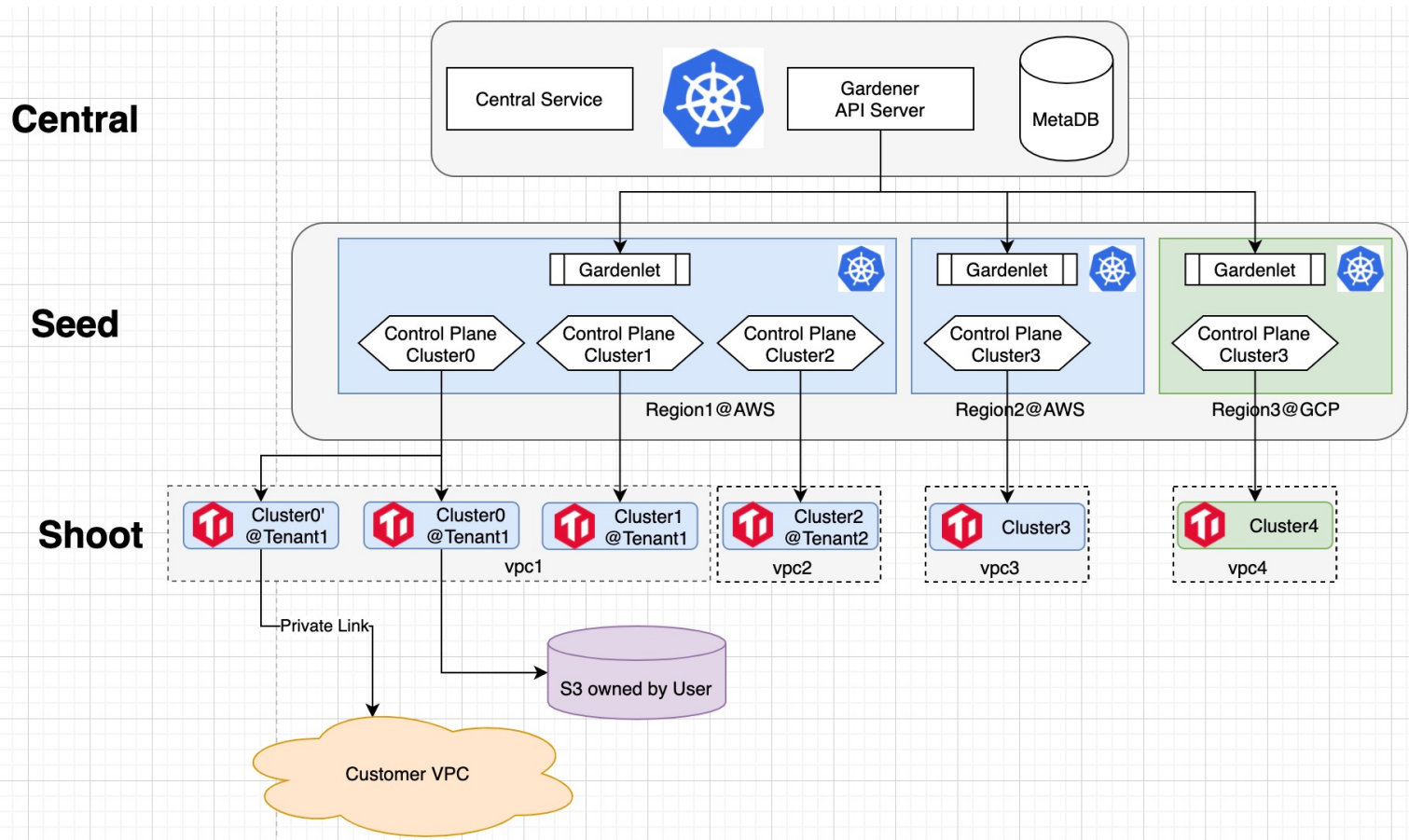
但云有一些 IDC 中不具备的能力

- 以与 IOPS 无关的块存储服务 GP3 为例
 - 从不同的节点访问GP3，性能、代价一致
 - GP3 的表现更接近本地盘
 - 再加上 k8s，我们就有了新机会

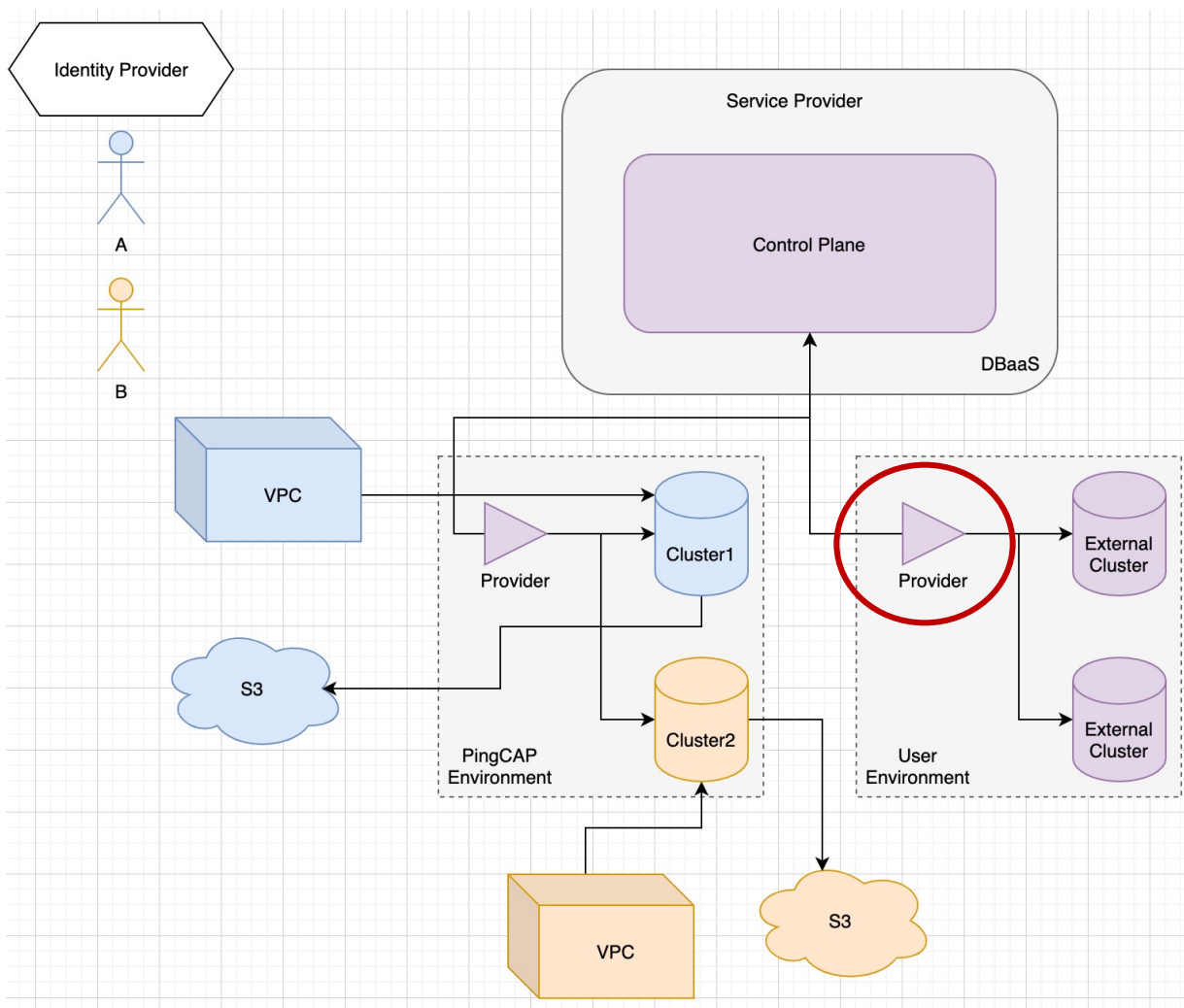


- 其他成本选项
 - 免费集群和基于共享资源池的集群
 - 诸多计算与存储的搭配机型
 - 面向场景定制的集群部件搭配
 - 支付场景 vs 收藏夹场景
 - ...

- 云原生的朴素理解
- 成本
- 安全
- 容灾
- 企业级能力



- 借力云基础设施上强力安全机制
 - 禁用静态密钥
 - TiDB Cloud 内部交互和访问云资源的 Credential 改为通过 Instance Meta 获取的 STS Token
 - 访问用户的 S3 Bucket 走标准 BucketPolicy 授权流程到 IAM Role
 - 各种控制爆炸半径
 - IAM Role 按租户隔离
 - 存放用户数据 S3 桶以租户为单位设置 BucketPolicy
 - ...
 - AWS CloudTrail & System Manager
 - ACM、KMS
 - Private Link
 - ...



- 部署在客户 VPC
- 混合云
 - TiDB Cloud & On-Premise(OP)
- 云上 OP 和 IDC 中的 OP

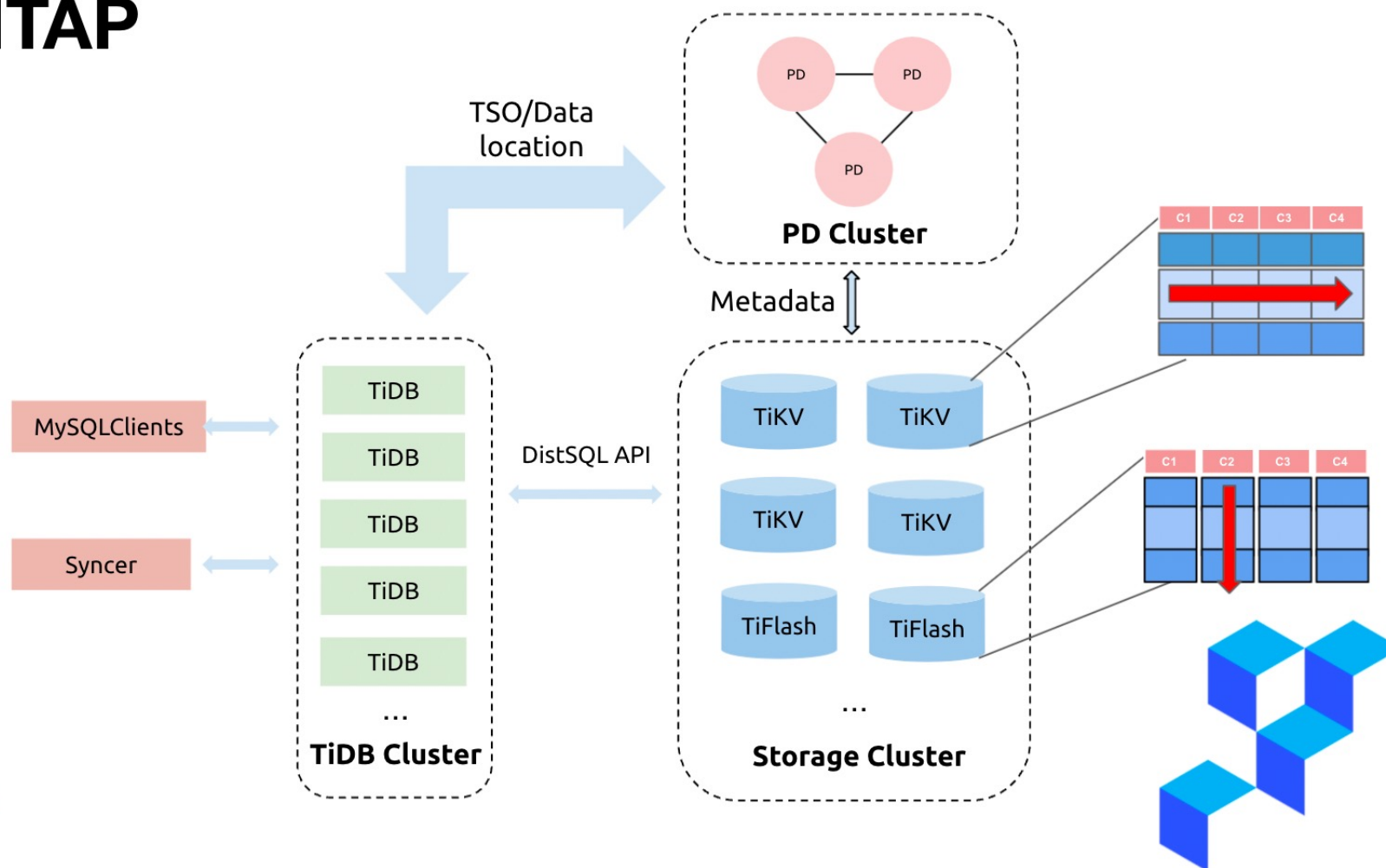
- 云原生的朴素理解
- 成本
- 安全
- 容灾
- 企业级能力

- 默认 3 副本跨 AZ 部署
- Backup/Restore
- PiTR
- TiCDC 外接自定义容灾设备/服务
- Cross Region Replication
- Cross Cloud Replication

- 云原生的朴素理解
- 成本
- 安全
- 容灾
- 企业级能力

TiDB HTAP

TiDB 5.0 GA

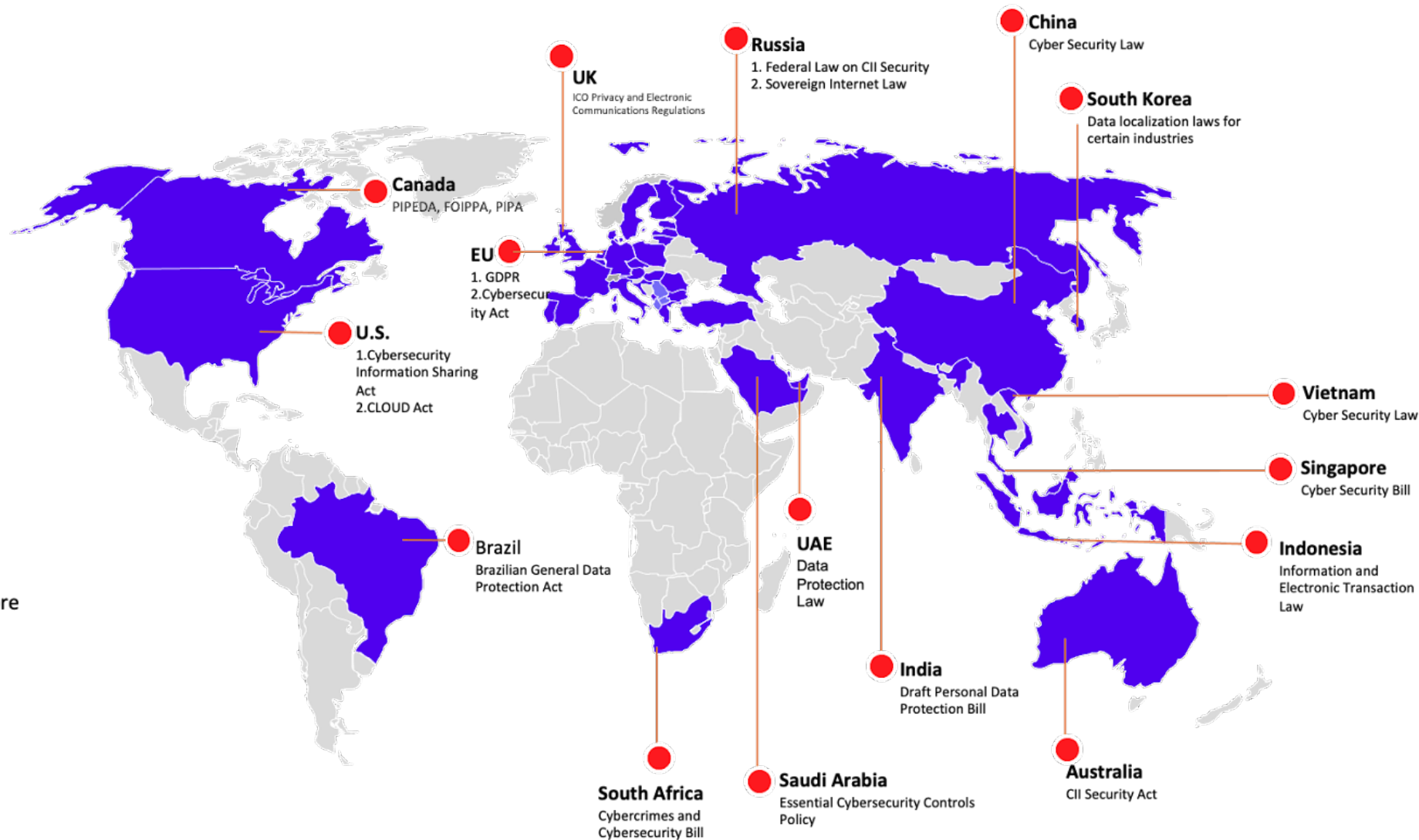


企业级能力

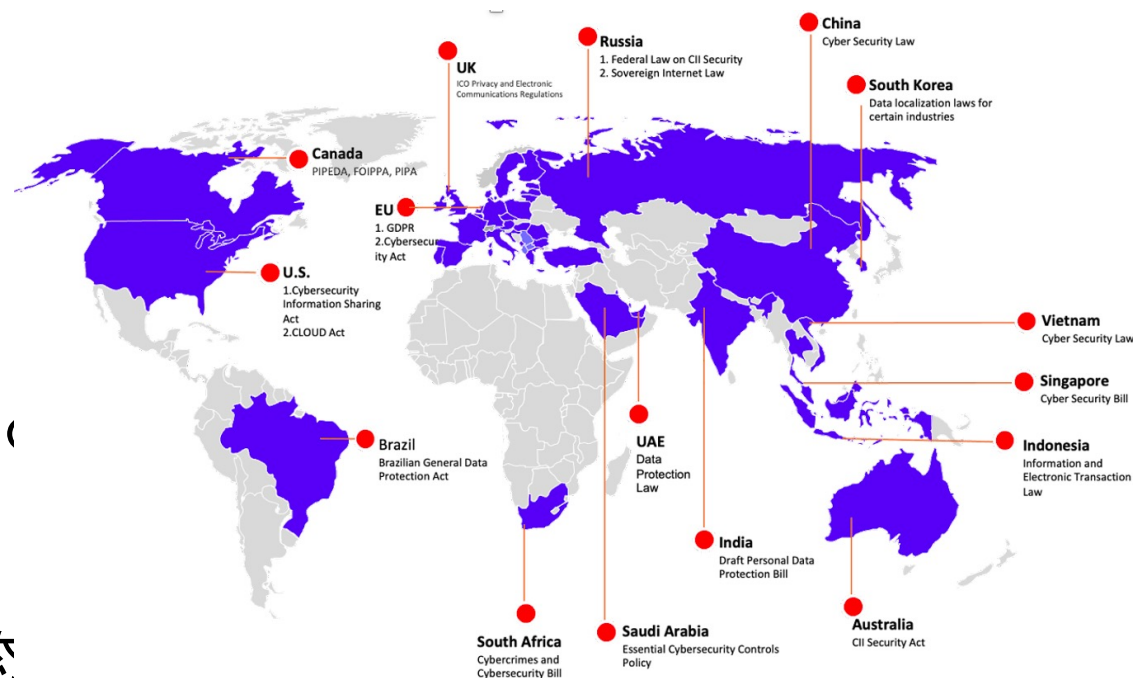
Geo Partitions

Trends

- ✓ More and more countries stipulate data residency laws
- ✓ Data Residency is evolving and often related to national security strategies.
- ✓ Data residency is more and more used as trade weapon and foreign investment review



- 地域敏感数据和全局数据
- 访问控制
 - 只允许特定地域的应用访问
 - 特定的数据必须写到特定的地域
 - ...
- Global Transaction vs Local Transaction
- 脏读
- 当 Geo Partition 遇到容灾、外接生态
 - 离线数据安全性



Open Source AceCon

2021 智能云边开源峰会

AI x Cloud Native x Edge Computing

人工智能 × 云原生 × 边缘计算

Thank You