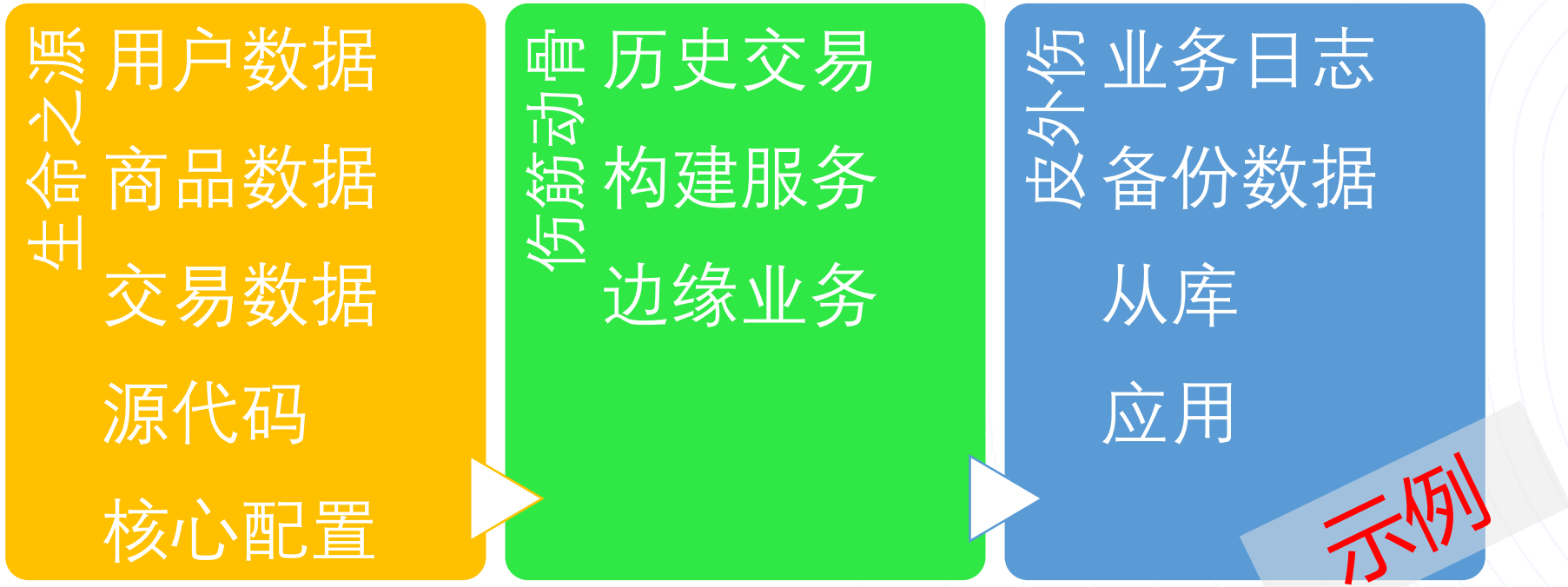
数据安全的七种“武器”

防火防盗防删库


预防
安全锁
恢复
堡垒机
备份
次认证
云内方案
功能
数据库审计
Ufile
UDB
罗马
数据方舟
离线备份
跨云方案
UHub + UK8s


备份
恢复
Ufile
UDB
预防
罗马
离线备份
堡垒机
数据库UDTS
跨云方案
云内方案
数据方舟
UHub + UK8s
数据库审计
次认证
功能
子帐号安全防控

对关键业务、数据严防死守



对数据/业务按重要性分层，优化恢复速度和成本
对人员和流程进行演练
对备份进行审计

UCLOUD优刻得

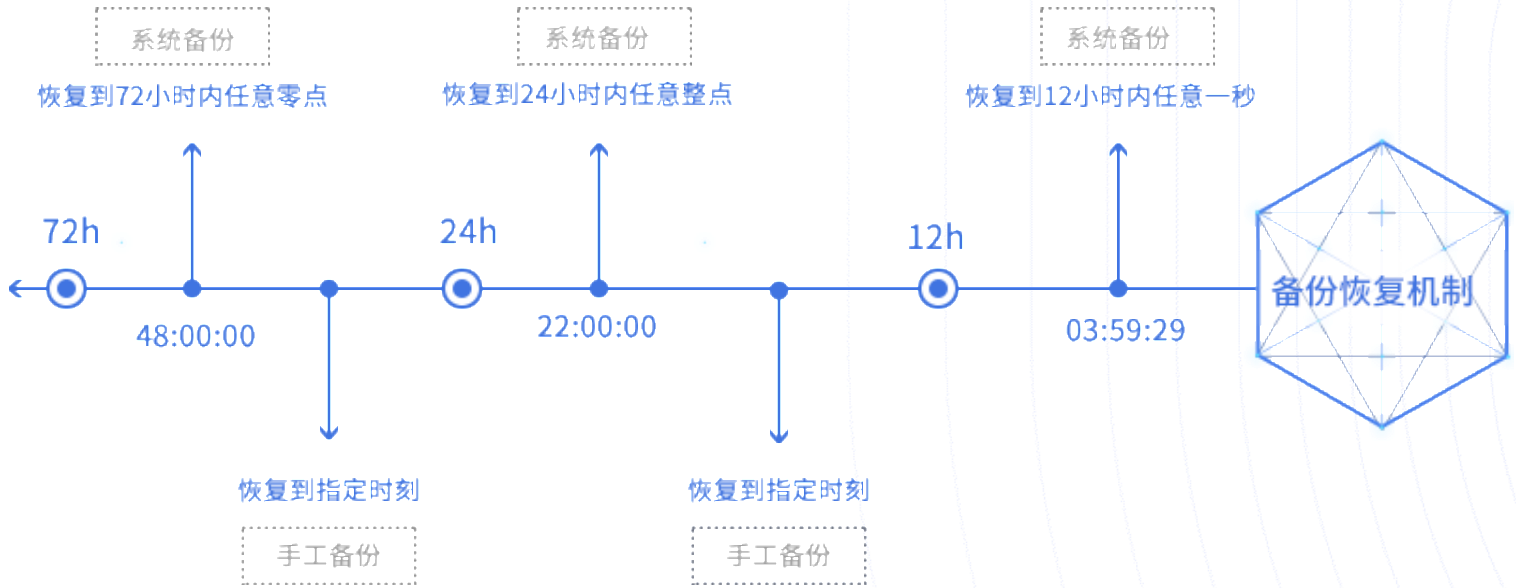
备份、恢复之云内篇
定时演练

主机：数据方舟

数据库：备份与恢复

文件备份：UFile

数据方舟



支持系统盘、数据盘单独恢复。 **支持云主机重装系统** **支持云主机配置升级**

数据方舟，秒级恢复

UCLOUD优刻得

数据方舟(UDataArk)是云计算场景基于块设备实时连续数据备份(CDP)解决方案

数据方舟(UDataArk)产品适用于:

- 基于本地盘主机与云盘主机部署的核心业务。
- 需要跨可用区容灾的核心业务。
- 混合云场景。

数据方舟(UDataArk) SLA:

- 数据持久性:99.999999%
- 服务可用性:99.95%

数据方舟(UDataArk)关键指标:

- RPO
- RTO

磁盘容量	恢复需要时间
100G	5-10分钟
500G	15-25分钟
1000G	20-30分钟

如何使用数据方舟

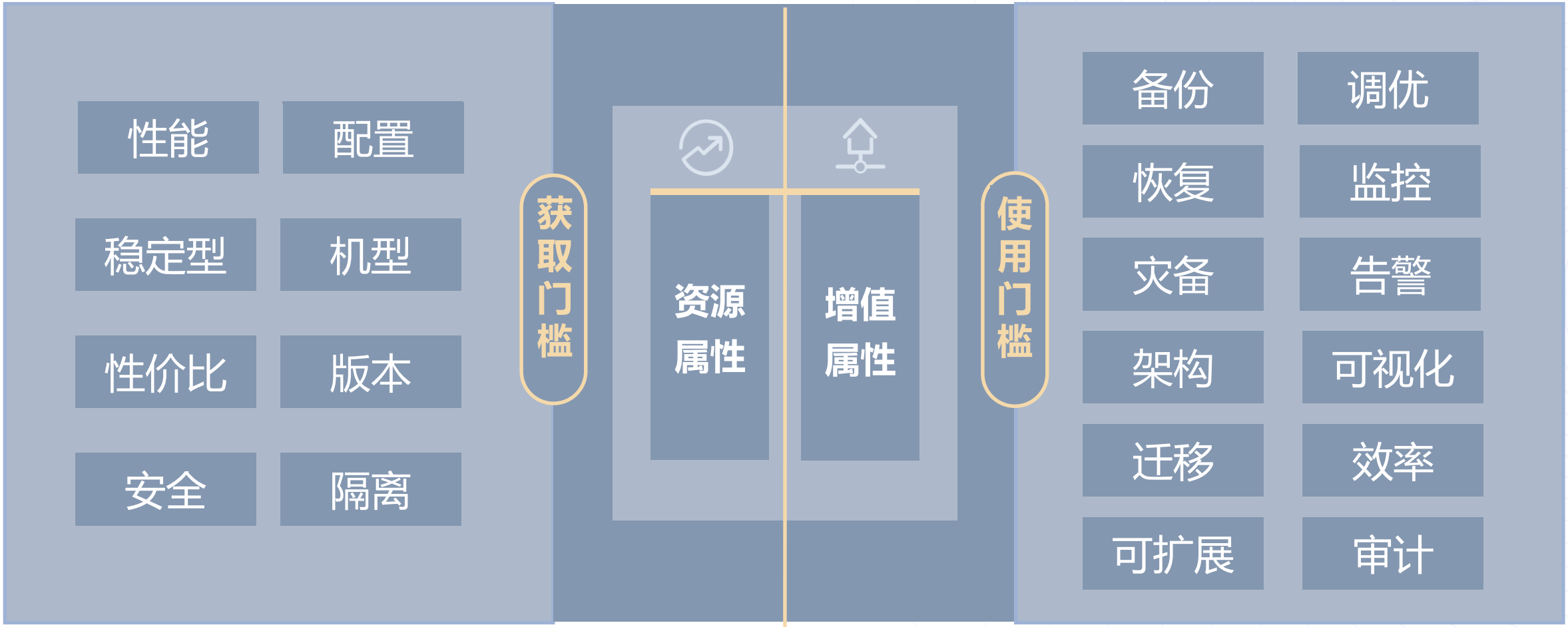
更详细的操作指南： https://docs.ucloud.cn/storage_cdn/uda/common

云数据库UDB简介 - 产品线

UCLOUD优刻得

分布式	UDDB			-	-	Sharding Cluster
高可用	高可用UDB					Replica Set
分支	MySQL 5.1、5.5、5.6、5.7	Percona 5.5、5.6、5.7	MariaDB 10.0	PostgreSQL 9.4、9.6、10.4	企业版 2012R1	MongoDB 2.4、2.6、3.0、3.2、3.4、3.6、4.0
协议	MySQL			PostgreSQL	SQL Server	MongoDB
分类	SQL（RDBMS）					NoSQL

云数据库UDB简介 - 云数据库的优势



UDB-备份与恢复功能

- UDB的备份模式
  - 自动备份每天自动进行一次备份
  - 用户可以对某些关键时间点的重要数据进行手动备份，允许保留个数为3个。
- UDB备份文件存储
  - 备份文件存储在UCloud独立的备份资源池中，安全性有保障。
  - 备份文件的副本始终保持多份异地冗余。
- 备份文件转存
  - Web控制台或API支持下载备份文件
  - Web控制台或API支持下载二进制日志文件
- 备份成功率保障机制
  - UDB的自动备份具备有效的告警机制，如果备份失败，则会自动触发告警。
  - UDB后台会定期进行备份成功率的巡检，通过SPT反馈备份情况给到用户。

产品-简介

对象存储（UFile）是为互联网应用提供分布式存储的服务，非常适合存储**非结构化**数据，比如图片、视频、音频、文本、日志等各种类型的文件。相对于传统硬盘存储，对象存储具有存储无上限、安全可靠、支持高并发访问、成本更低等特点。

- *分布式存储系统，存储容量无限扩展*
- *服务可用性99.998%*
- *数据三副本，数据持久性99.999999999%*
- *基于HTTP访问*
- *支持HTTPS访问*
- *结合CDN分发加速有效降低访问延迟、提升下载速度*
- *可视化控制台*
- *多版本客户端工具*
- *API接口及丰富的SDK包支持，适合多种语言*

存储类型概述

UCLOUD优刻得

UFile

对象存储（UFile） 提供标准、低频、归档三种存储类型，分别用于频繁访问的热点数据，低频访问的备份数据和适用于长期保存的归档数据，全面覆盖从热到冷的各种数据存储场景。用户可以根据业务场景选择不同的存储类型，优化存储成本。

标准存储

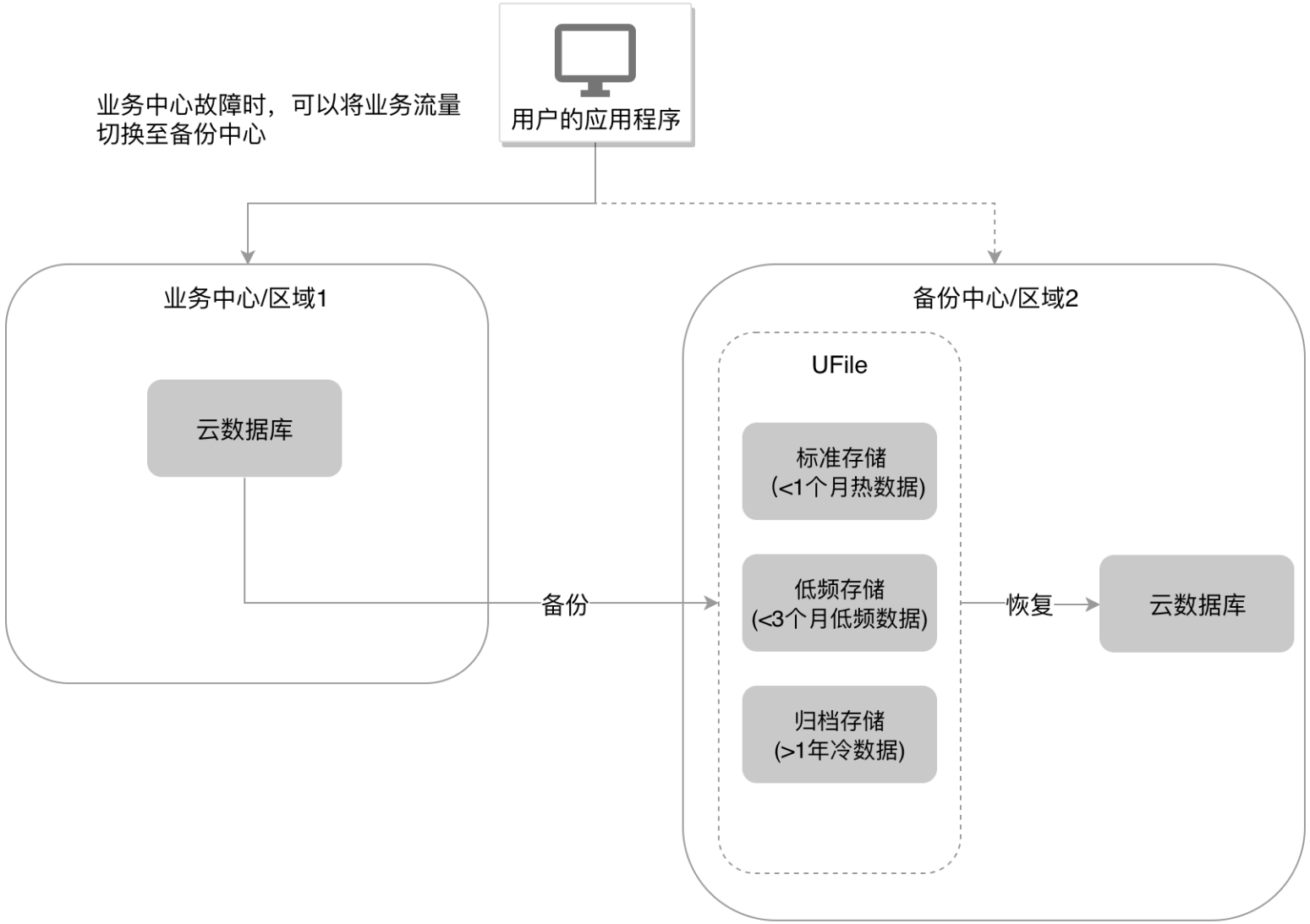
低频存储

归档存储

功能-概览

UFile功能概览	
空间管理	创建空间　获取空间信息　更改空间属性　删除空间
上传	普通上传　表单上传　分片上传　秒传文件　上传回调
下载	普通下载　分段下载
域名管理	自定义域名
文件管理	获取文件信息　前缀列表查询　删除文件　生命周期　跨地域复制
安全管理	鉴权机制　令牌管理　日志管理　跨域访问　防盗链

应用场景-数据库备份



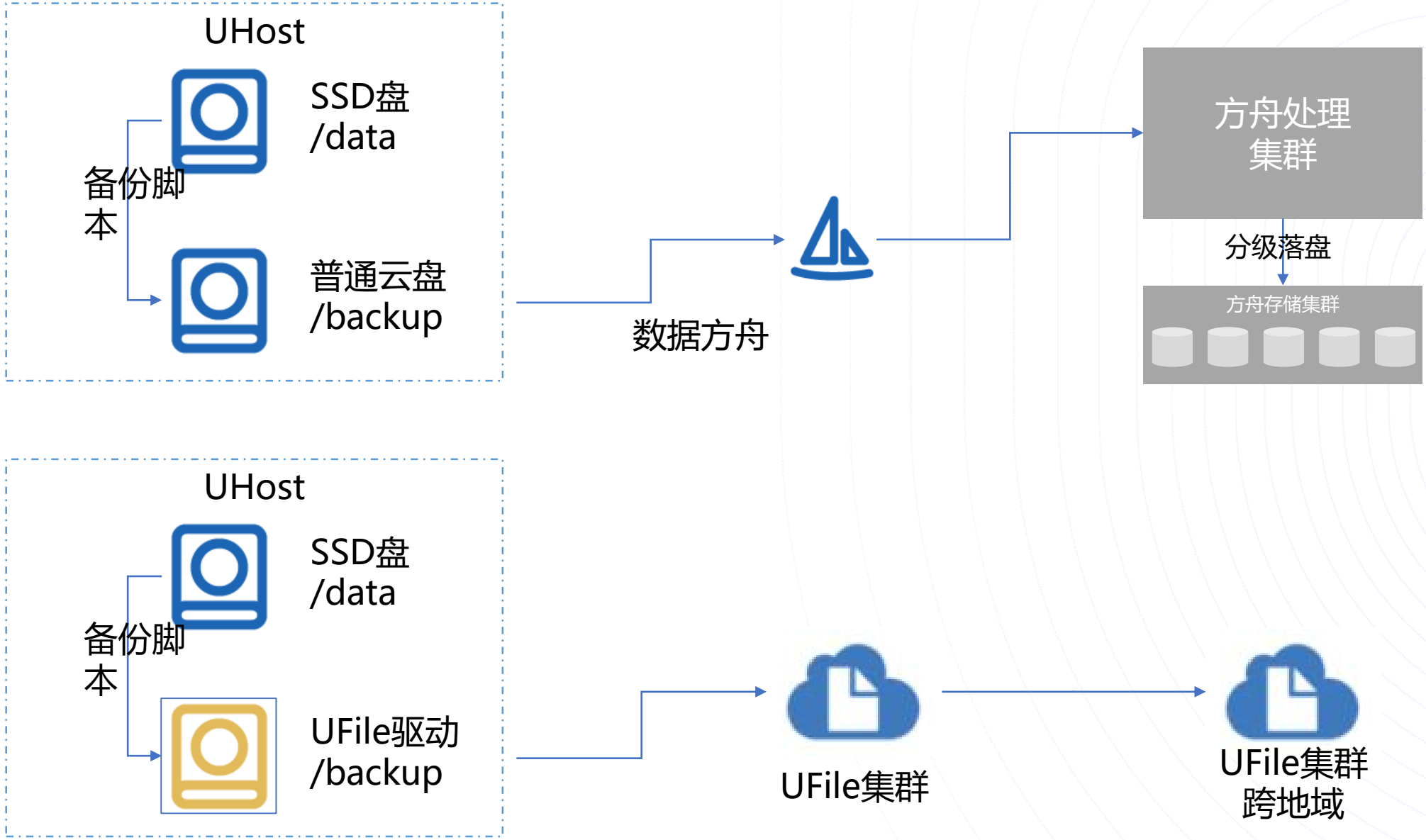
数据库备份

用户自建数据库或云数据库在UFile上备份或长期归档，当业务中心区域发生故障时，可以通过备份中心区域的备份数据进行恢复。

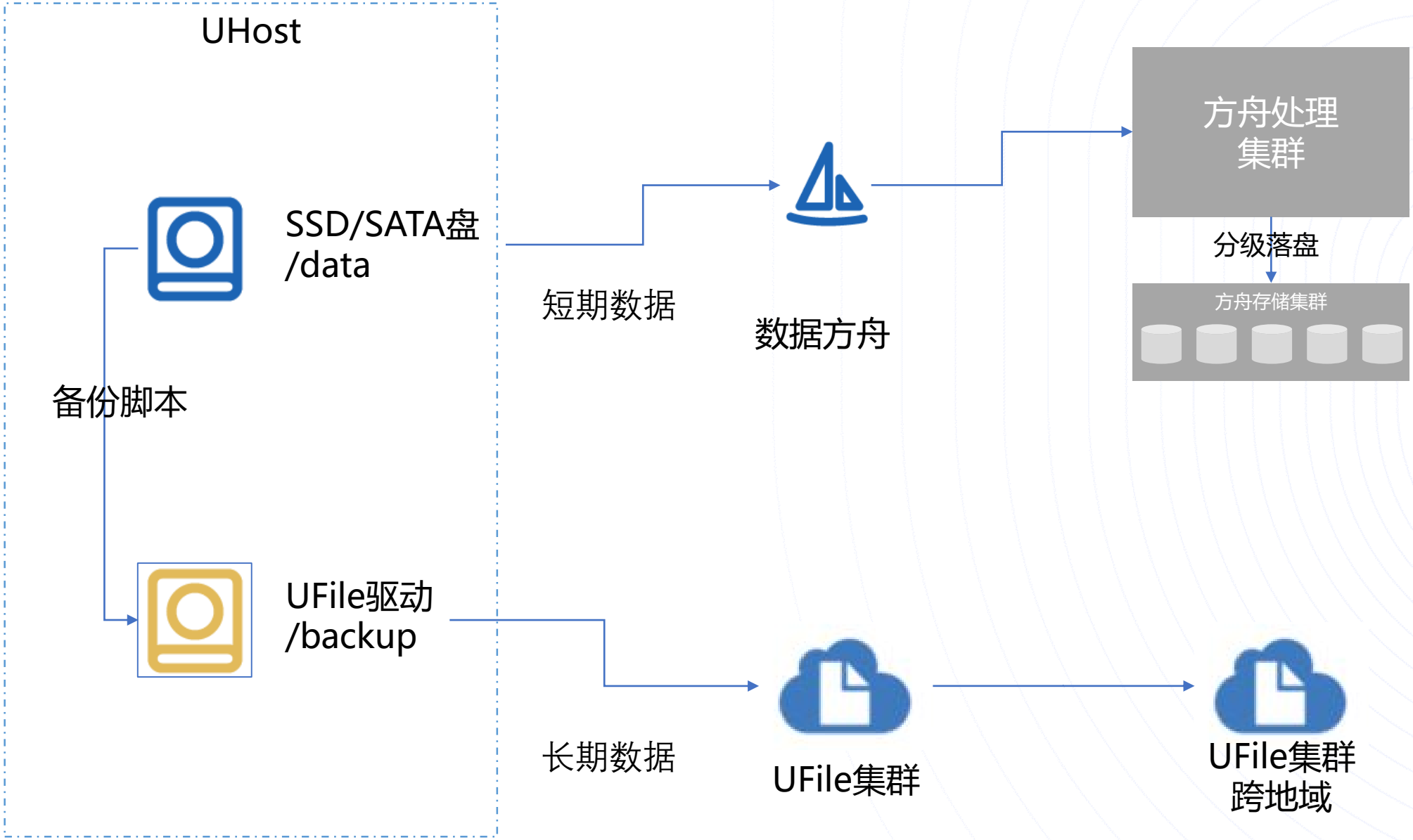
推荐配置

标准存储 + 低频存储 + 归档存储 + 云数据库

综合应用


UHost
SSD盘
/data
备份脚
本
普通云盘
/backup
数据方舟
方舟处理
集群
分级落盘
方舟存储集群
UHost
SSD盘
/data
备份脚
本
UFile驱动
/backup
UFile集群
UFile集群
跨地域

综合应用- 2020 年6 月之后



UCLOUD优刻得

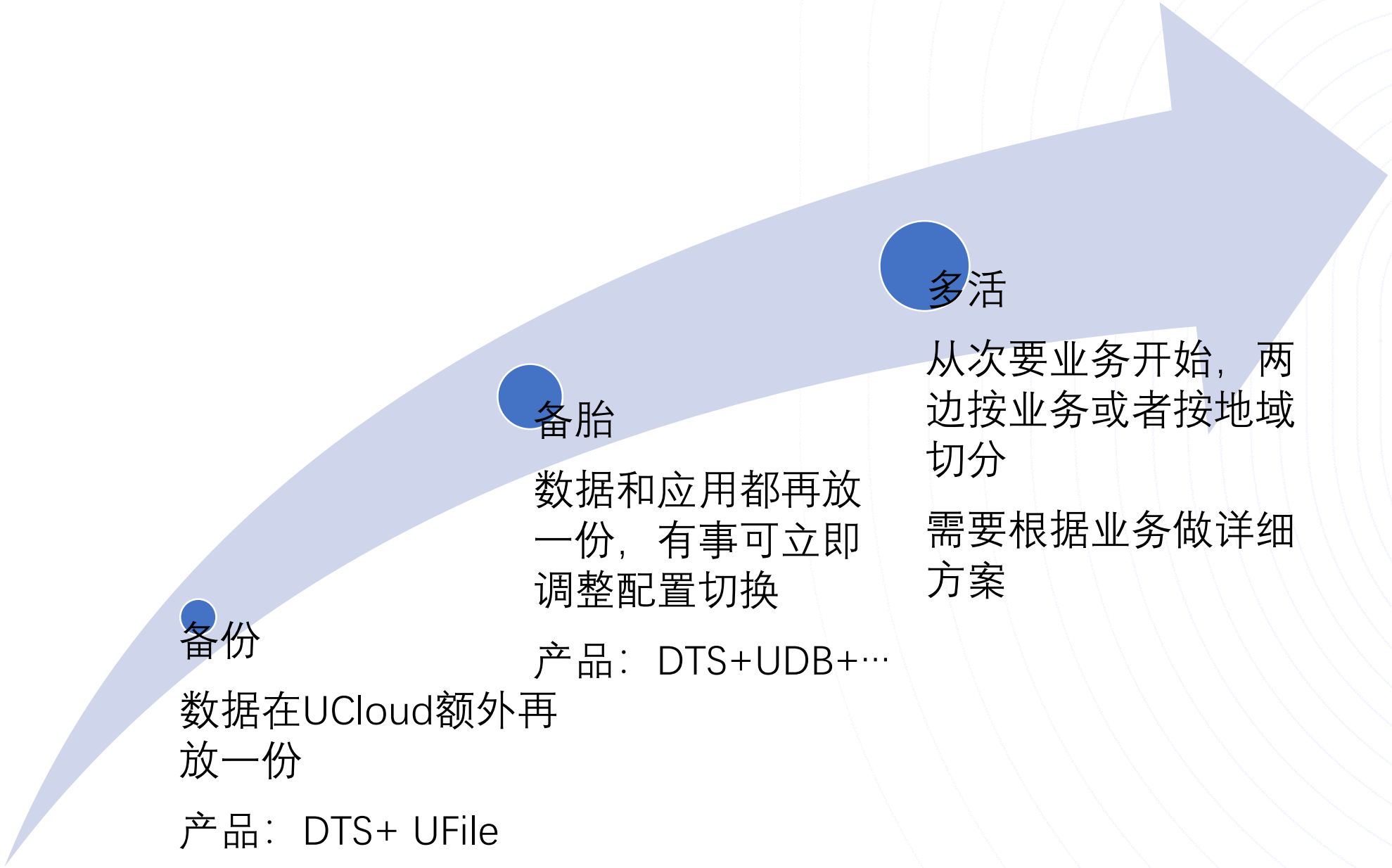
云间篇：备份，备胎及多活

数据传输：UDTS

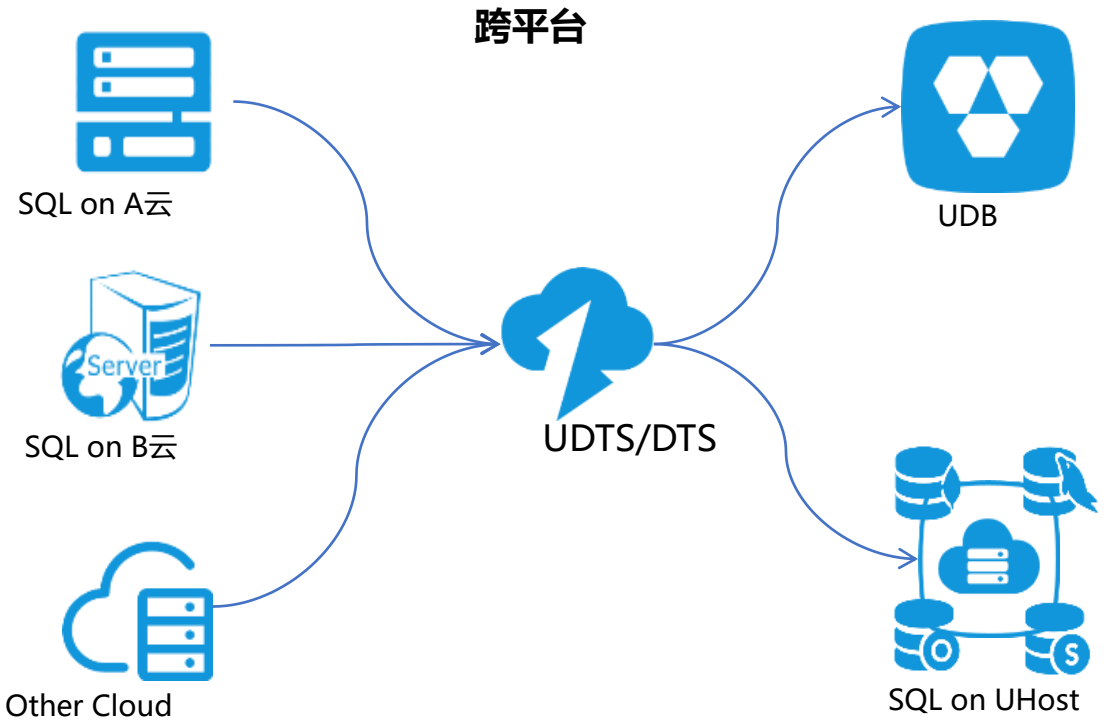
云原生：UK8S

多云互联：Rome

备份，备胎及多活


备份
数据在UCloud额外再放一份
产品：DTS+ UFile
备胎
数据和应用都再放一份，有事可立即调整配置切换
产品：DTS+UDB+…
多活
从次要业务开始，两边按业务或者按地域切分
需要根据业务做详细方案

数据库同步 UDTS



结构化数据同步方案

通过UCloud UDTS 或者其他公有云DTS功能实现两地数据库数据的同步。

用户获益：

① 实现自动化不停服数据迁移，支持断点续传，操作简单。
② 实现多种同异构数据源之间的迁移同步。
③ 实现迁移过程中的增量数据传输，保持数据一致性。
④ 更丰富多样、高性能、高安全可靠的数据传输链路。

UDTS支持的场景

UCLOUD优刻得

数据源	数据目标	全量迁移	增量迁移
UDB	MySQL	支持	支持
UDB	TiDB	支持	支持
MySQL	MySQL	支持	支持
MySQL	TiDB	支持	支持
MySQL	UDB	支持	支持
TiDB	TiDB	支持	暂不支持
MongoDB	MongoDB	支持	暂不支持
CSV	MySQL	支持	暂不支持
CSV	UDB	支持	暂不支持
CSV	UDW	支持	暂不支持
UFile-bucket	UFile-Bucket	支持	方案支持
Redis	Redis	当前仅支持全量+增量任务	

罗马网络 Rome

罗马即罗马全球加速网络的简称，它依托于UCloud全球数据中心及28条专线，为用户提供就近接入、链路动态调度，实现端到端的高稳定连接，规避骨干网络故障等导致的响应慢 、丢包等问题。

多云互联

- ✓ 接入罗马的VPC，任意两者均可互通。目前支持的云商及地域（后续将增加可支持的地域及云商）：
- ✓ UCloud： 北京、上海、广州、香港、洛杉矶、法兰克福、曼谷、新加坡、东京、迪拜；
- ✓ 其他公有云： 北京、杭州、上海、深圳、香港；

接入简单

只需几步，即可完成 VPC 的接入。

链路动态调度

链路实时监控，通过SD-WAN技术自动选择最优路线，避免链路拥塞、中断造成的传输延迟、抖动、丢包的情况，保证网络可靠性。

高质网络

罗马内部使用专线网络及多线BGP网络出口， 保障网络访问的稳定及高速。

高可用性

多接入节点，多线路灾备，接入、转发高可用部署，避免单点故障。

计费灵活

根据实际链路使用情况进行后付费，避免先购买后使用时，预估不准确造成的浪费

预防篇

堡垒机，数据库审计

控制台权限，操作安全锁

控制台子帐号权限管理


编辑角色
角色名称：*
运维
角色描述：
运维专用
产品权限*
增
删
改
查
云主机 uhost
物理主机 uphost
托管云 uhybrid
基础网络 unet
负载均衡 ulb
云数据库 udb
SSD云硬盘 udisk
云内存存储 umem
对象存储 ufile
分布式数据处理 uddp
取消
确定

控制台操作安全锁

产品	操作
主机	开机、关机、删除实例
物理机	关机、删除实例
云数据库 UDB	删除实例、关闭
云内存存储 UMem	释放内存
对象存储 UFile	删除bucket、删除UFile geo bucket
云硬盘 UDisk	删除实例

堡垒机：核心思路

UCLOUD优刻得

事前干预

- 身份管理
- 权限设定
- 密码管理

事中管控

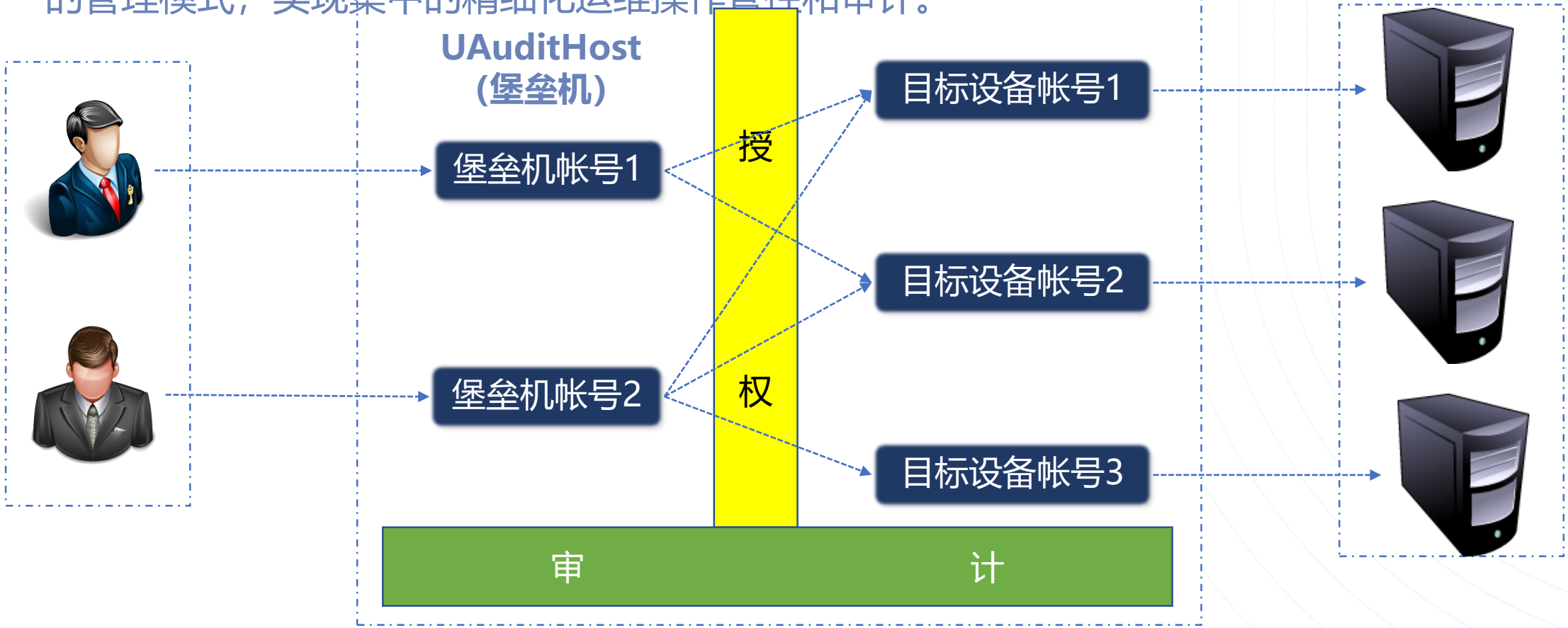
- 单点登录
- 命令管控
- 实时监控

事后审计

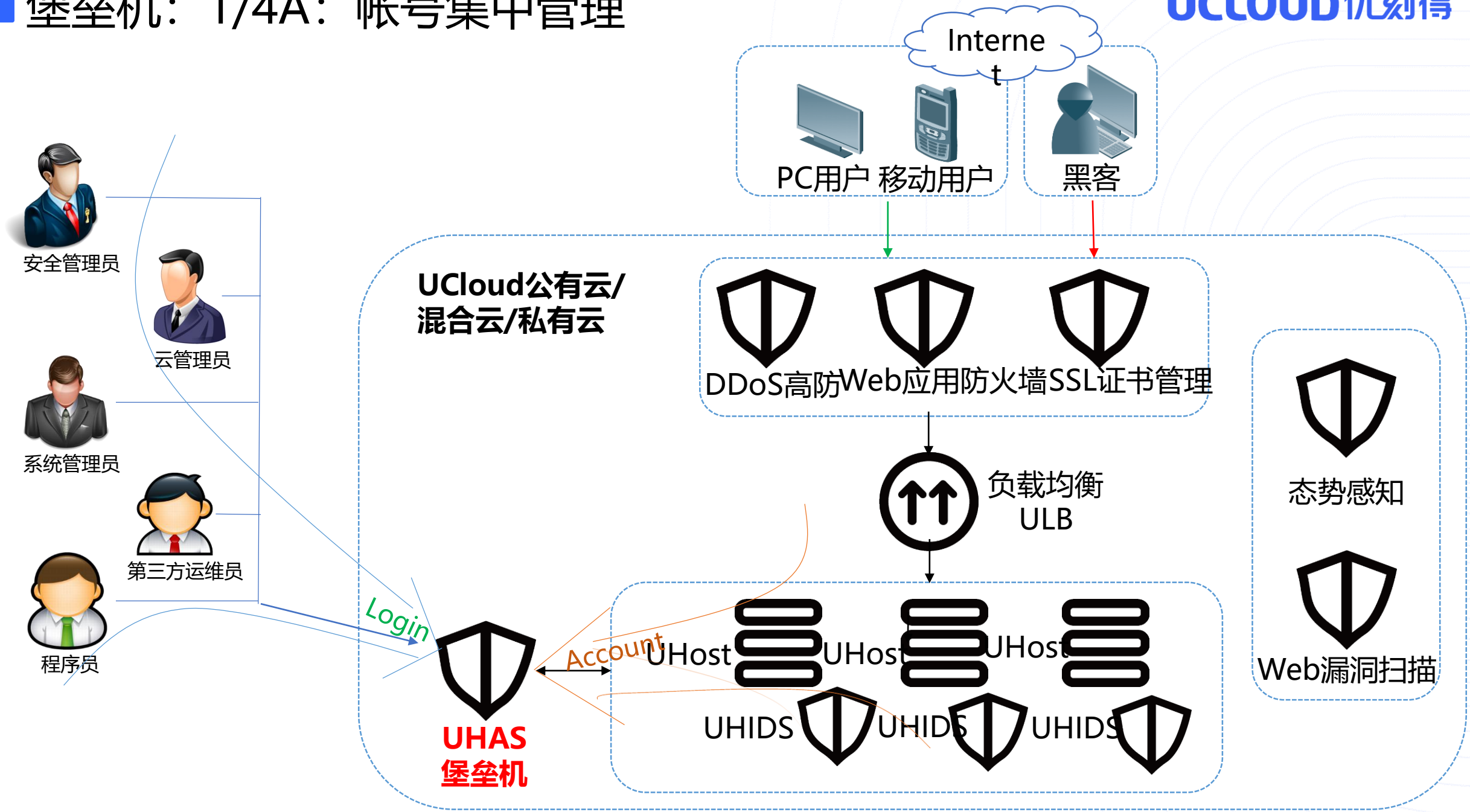
- 日志查询
- 视频回放
- 审计报告

堡垒机：核心思路

UAudtiHost（堡垒机）通过逻辑上将人员与目标设备分离，建立“人->堡垒机帐号->认证&授权&审计->服务器等目标设备帐号->目标设备（例如UHost）”的管理模式，实现集中的精细化运维操作管控和审计。



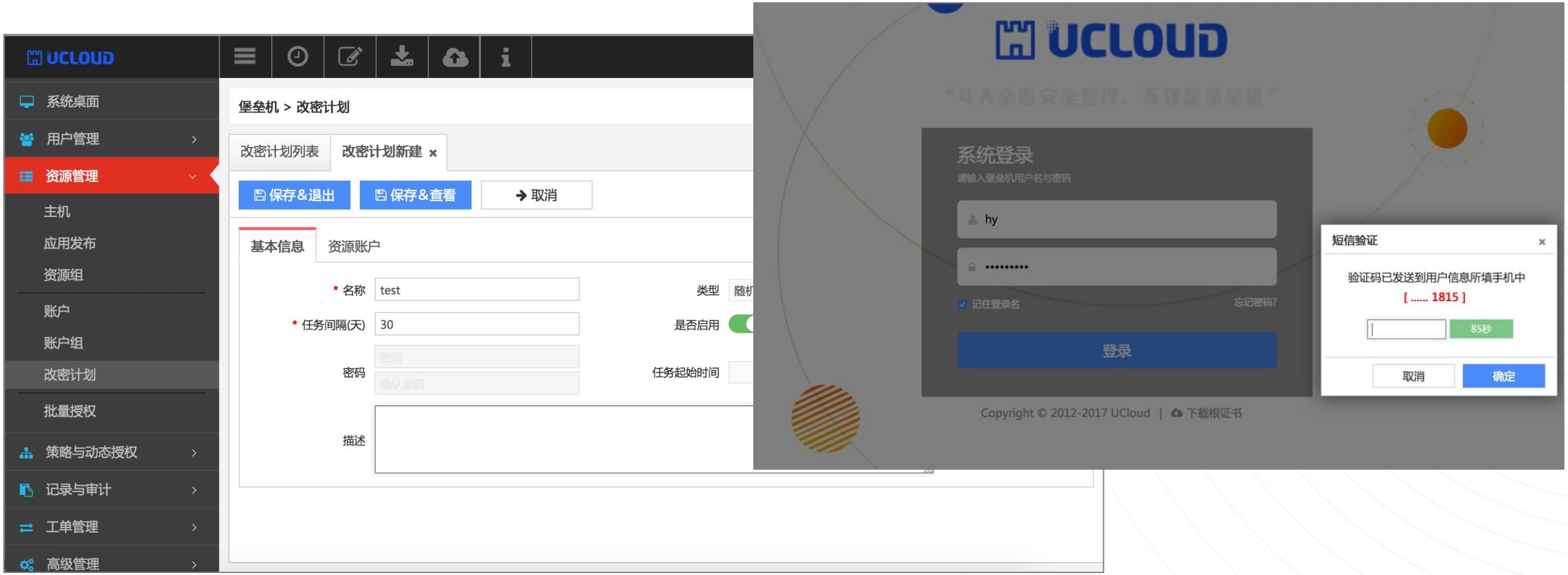
堡垒机：1/4A：帐号集中管理



堡垒机：2/4A：集中强认证

UCLOUD优刻得

- 登录堡垒机双因子认证，支持短信、令牌、radius等。
- 资源改密计划，定期改密。



堡垒机：3/4A：统一授权

UCLOUD优刻得

访问控制：杜绝危险操作

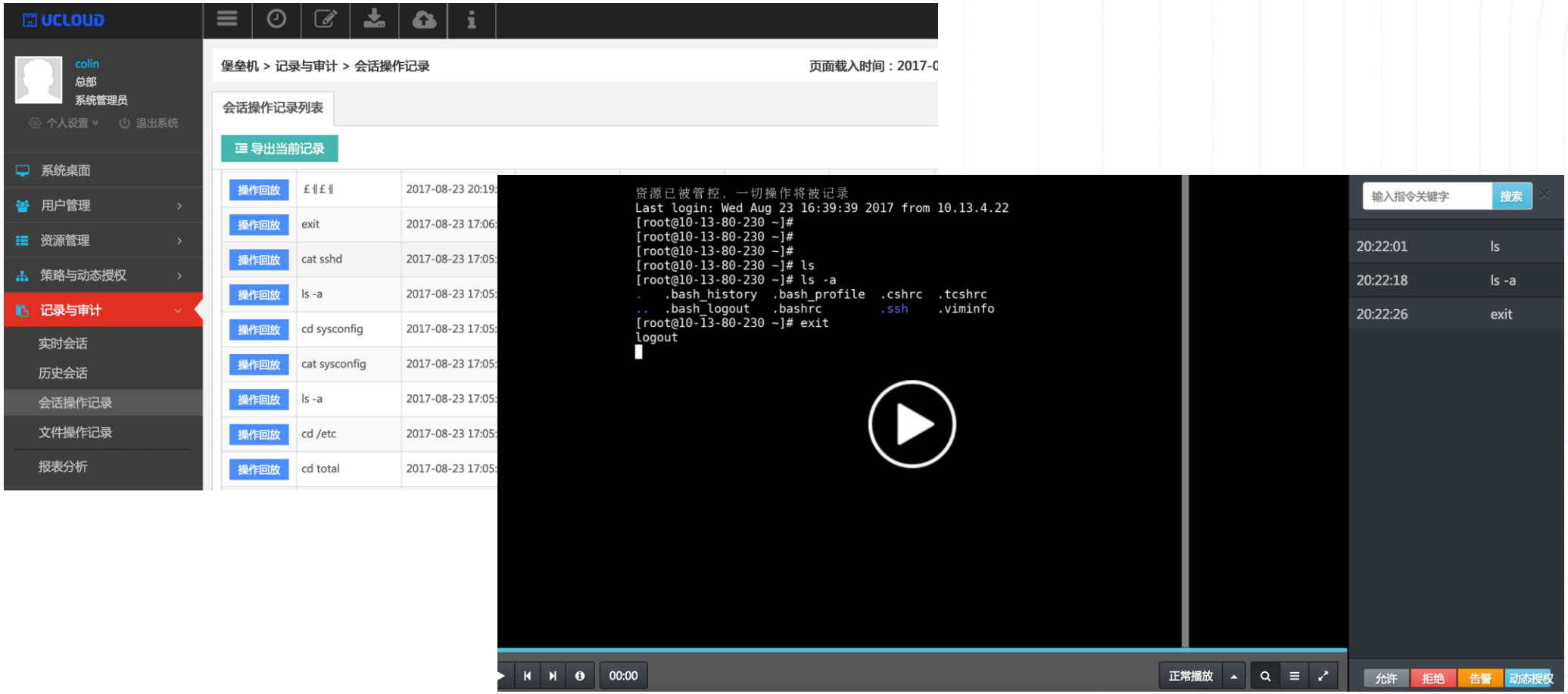
➢三权分立，多角色划分；多种控制方式的策略设定

堡垒机：4/4A：操作审计

UCLOUD优刻得

字符会话审计

- 基于内容的操作审计，输入、输出结果关键字搜索快速定位播放



数据库审计UDB-Audit 支持多种数据库类型

- Oracle、MS-SQL、DB2、Sybase、Cache DB国外主流数据库;
- MySQL、PostgreSQL开源数据库;
- 达梦、人大金仓、南大通用等国内主流数据库;
- HBase等NoSQL数据库;
- IP21实时数据库。

数据库管理三权分立

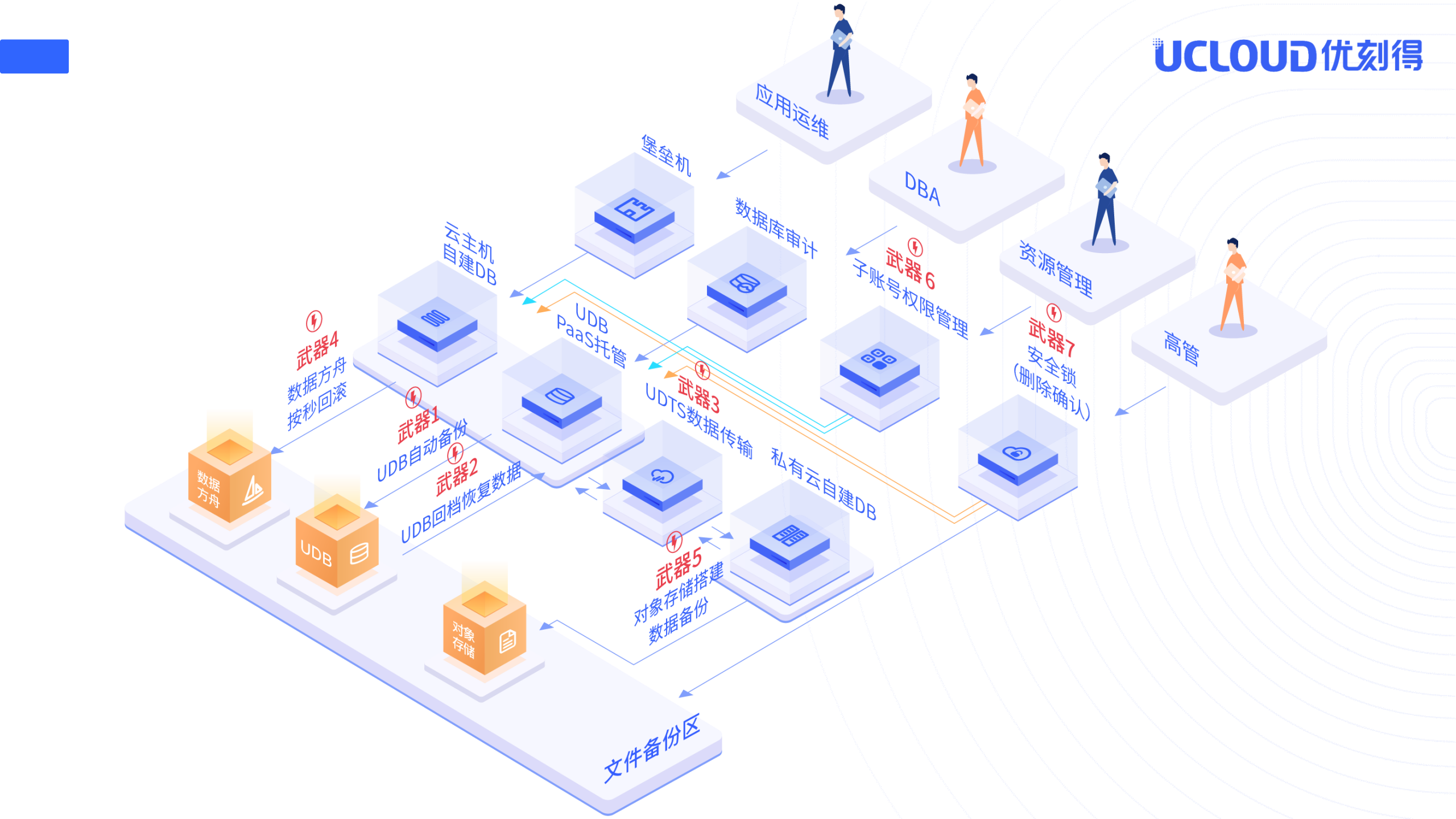
- 审计管理：auditadmin/***
- 规则管理:ruleadmin/***
- 系统管理:admin/***

数据库审计之深度检测

UCLOUD优刻得

操作行为	内容和描述
用户行为	数据库用户的登录、注销
数据定义语言（DDL）操作	create、alter、drop等创建、修改或者删除数据库对象（数据库、表、列、索引等数据库对象）的SQL指令
数据操作语言（DML）操作	insert、delete、update和select等用于添加、删除、更新和查询数据库记录的SQL指令
数据控制语言（DCL）操作	grant、revoke授出、收回等定义数据库、表、字段、用户的访问权限和安全级别的SQL指令
其它操作	包括execute、commit、rollback等事务操作指令

内容回顾


UCLOUD优刻得
应用运维
DBA
资源管理
高管
堡垒机
数据库审计
云主机
自建DB
UDB
PaaS托管
武器6
子账号权限管理
武器7
安全锁
(删除确认)
武器4
数据方舟
按秒回滚
武器1
UDB自动备份
武器2
UDB回档恢复数据
武器3
UDTS数据传输
私有云自建DB
武器5
对象存储搭建
数据备份
数据
方舟
UDB
对象
存储
文件备份区

总结

UCLOUD优刻得

数据的备份在哪里?

从备份恢复要多久?

宕机的损失有多大?

Q&A