

众筹DAPP系统开发-漫云科技-行业app软件成品开发现成案例

产品名称	众筹DAPP系统开发-漫云科技-行业app软件成品开发现成案例
公司名称	河南漫云科技有限公司
价格	.00/个
规格参数	漫云科技:区块源码 区块系统:定制开发 区块app系统开发:快速搭建
公司地址	郑东新区升龙广场3号楼A座3202
联系电话	13103827627 13103827627

产品详情

数据归档主要针对BlockDB和ResultDB将平时不怎么需要访问的数据归档，专注行业APP软件开发，主要经营业务包括APP定制开发、网站定制开发、集“软件、营销、服务和运营”为一体的国家高新技术企业。小程序定制开发、行业软件开发、为企业打造属于自己平台的开发解决服务商，河南漫云科技有限公司成立于2019年，是一家以“践行工匠精神，用心服务客户”为使命，河南漫云科技有限公司成立于2019年，是一家以“践行工匠精神，用心服务客户”为使命，目前也仅支持leveldb和badgerdb这两种数据库归档，暂不支持mysql，节点启动文件存储(>=v2.2.x)之后，暂时不支持归档，归档实现方式：归档前设置不允许归档的高度(unarchive_block_height，默认300000，当设置值小于10时，自动设置成10)，能归档的高度即为当前高度-unarchive_block_height

归档的内容会从上删除，需要事先将数据转存到外数据库 归档会删除BlockDB中的tx详细内容和ResultDB中的RWSets，并记录当前归档的高度(该高度也会被归档)，并触发kvDB的compaction 归档过程中会跳过GenesisBlock和ConfigBlock，如果要归档的目标高度正好为这两种区块，归档会失败，可以将目标高度修改到普通区块的高度 归档后的区块依然可以从上获取区块的原数据(MetaBlock)，众筹系统开发：I35原理7O98开发O7I8,只是无法获取到交易内容和RWSets(读写集)。所以无法获取完整的区块信息。但GenesisBlock和ConfigBlock任然可以获取完整区块信息 归档后的节点在对其他节点提供区块同步信息时，无法提供已归档的区块信息，所以在需要同步的节点选择连接的peer节点时，会只选择已归档高度比自己高度低的节点。如果是高度为1的全新节点，则只能从未归档的节点(peer)同步区块

用户可以多次归档，每次归档接着上次归档的高度继续 归档后的区块查询时会返回错误：
区块错误信息：“archivedblock” 交易错误信息：“archivedtransaction”
读写集错误信息：“archivedRWSet”

2. 归档数据恢复

数据恢复时会将数据写回上，慢慢恢复未归档前的样子
数据恢复时会将交易内容和读写集(RWSets)写回节点，节点恢复到未归档前样子 恢复过程中区块内容按照高度从高到低写回BlockDB和ResultDB，GenesisBlock和ConfigBlock跳过(不需要恢复)更新的已归档的高度，同时触发kvdb的compaction

用户可以多次恢复归档数据，每次恢复接着之前恢复的高度继续

3. 数据恢复(rebuild_dbs)

操作步骤 `./chainmakerrebuild-dbs-c./config/wx-org1-solo/chainmaker.ymlci-solo`
查看日志，确认恢复成功 停止区块服务 执行数据恢复(执行过程如上图)，示例如下

使用限制 当前仅支持leveldb存储方式的恢复 其他

storage: rebuild_block_height:10,众筹开发逻辑及源码唯：MrsFu123

可以在命令行末尾添加chainid来恢复的chainid ./chainmakerrebuild-dbs-c../config/wx-

org1-solo/chainmaker.ymlci-solo--chain-id=chain1 可以在命令行末尾添加need-

verify, 对于可靠的数据恢复原始数据跳过区块验证过程, 提高恢复速度, 默认true

./chainmakerrebuild-dbs-c../config/wx-org1-solo/chainmaker.ymlci-solo--chain-id=chain1--need-verify=false

执行数据恢复, 会自动备份原数据 可以配置恢复区块高度, 不配置则恢复全部 用法

数据库恢复:在数据库数据损坏时, 需要完整的多个数据库文件夹, 使用该工具重新生成数据到的数据

未损坏时的高度 回滚到高度:在数据写入紊乱, 数据库不可用时, 也可以使用该工具恢复到数据

未紊乱时的高度, 达到数据回滚的效果 数据库恢复:在数据库数据损坏时, 使用block和ledgerData1

文件夹的数据, 可以重新生成其他文件夹的数据 数据同步:在同步过程中, 可以拷贝目标节点的bl

ock和ledgerData1数据, 然后使用该工具在本地重新生成其他文件夹的数据, 之后即可以快速启动, 达到

快速同步的效果 回滚到高度:在数据写入紊乱, 数据库不可用时, 也可以使用该工具恢复到数据

未紊乱时的高度, 达到数据回滚的效果 启用了文件存储功能(推荐启动):

未启用文件存储功能: 4. 透明数据加密 (TDE) 透明数据加密 (TransparentDataEncrypti

on(简称TDE)) 是指可以在文件层对数据和文件进行实时加密和解密, 落盘的文件是加密后的内容, 而

对于上层应用系统和开发人员而言, 加解密过程是无感知的, 写入和读取的内容是明文内容, 所以叫做

透明数据加密。长安模块同时提供了软件实现和硬件集成, 使用以下步骤即可完成TDE的配置。

5. 基于软件实现的TDE配置 6. 创建对称密钥 长安的透明数据加密默认支持AES和国密S

M4两种对称加密算法。AES算法支持128位、192位、256位这3种密钥长度, SM4算法支持128位密钥长度

。密钥长度必须与对应的算法匹配, 如果长度不匹配则无法正常启动长安。我们以国密SM4算法为例,

密钥推荐使用随码生成器生成的, 比如"这样的形式, 将有效提高数据的安全性, 防止被字典破解。除

了字符串形式的密钥, 长安还支持任意二进制形式的密钥, 只要长度满足要求(国密SM4: 128位)即可

。新生成的密钥请做好安全备份, 防止密钥丢失后数据无法解读。 7. 配置透明数据加密

在长安节点的配置文件, 即chainmaker.yml文件中, storage配置项下提供了对该节点TDE的配置选项, 形

如: storage: encryptor:sm4 #sm4/aes encrypt_key:"1234567890123456"#16byteskey

encryptor是采用的对称加密算法, 目前支持sm4和aes两个选项。

encrypt_key是对称加密的密钥, 支持字符串、十六进制和文件路径三种形式。

字符串, 支持字母大小写、数字、符号、空格等, 长度必须满足加密算法要求

十六进制, 必须以0x开头, 后面跟对应密钥的十六进制内容 文件路径, 将密钥保存到一个文件中

, 然后将文件路径配置到这里, 并确保长安进程用户具有读写该文件的权限。以下配置示例: sto

rage: encryptor:aes #sm4/aes encrypt_key:"0x48656c6c6f20436861696e4d616b6572"#16byteskeystorage: en

cryptor:sm4 #sm4/aes encrypt_key:"/usr/key/my.key"#thisfilecontentisa16byteskey 8. 启用节点

完成TED的配置后, 请确保当前节点没有任何数据, 如果之前已经有数据, 需要完全删除。节点启

动后将会从创世区块开始基于TDE的密钥对每个区块每个交易每个世界状态Value进行统一的加密存储。

在encrypt_key上使用文件路径配置密钥的情况下, 长安在启动时将读取文件内容作为密钥, 同时将文件

内容清空, 防止硬盘数据被盗时密钥也同时被盗。所以如果下次要重新启动长安进程, 必须重新在对应

的密钥文件中写入密钥才能正常启动。 9. 基于硬件机的TDE配置 基于软件的对称加密存

在占用主机计算资源, 密钥容易暴露的风险, 基于硬件机的方案可以有效提升加解密的性能和密钥的安全

性。长安支持PKCS11标准的硬件机接入, 以下为在TDE中启用硬件机集成的步骤。

10. 在加密中生成对称密钥 基于硬件机的情况下, 密钥都托管在机内部, 外部程序无法获得密钥

内容, 只能通过标准接口进行密钥生成、加解密、签名、哈希等学操作。进入机自带的管理后台可以为

TDE生成对应的密钥, 对称加密算法可选择AES或者国密SM4。密钥生成后会有一对应的KeyID作为该

密钥在机中的标识, 在接下来配置中会用到。 11. 配置PKCS11 长安基于PKCS11标准与机

进行通讯, 其对应的配置在chainmaker.yml配置文件的node配置节点下, 配置示例如下: node: p

kcs11: enabled:true library:/usr/local/lib64/pkcs11/libupkcs11.so #pathtothefileofpkcs11interface

label:HSM #labelfortheslottobeused password:111111

11 #passwordtologontheHSM session_cache_size:10

#sizeofHSMsessioncache,defaultto10 hash:"SHA256"

#hashalgorithmusedtocomputeSKI

具体配置因为对应的机不同而不同, 具体参见硬件加密章节。 12. 配置透明数据加密 在

完成了node配置节点下的pkcs11配置后，接下来需要进行storage配置节点下关于TDE加密算法和密钥的配置，对于机，我们并不知道对应的密钥内容，只有密钥的ID，所以我们只需要配置成对应的KeyID即可，比如：`storage: encryptor:sm4 #sm4/aes encrypt_key:"MasterKey1"#机上对应KeyID`

13.. 启用节点 在完成配置后，同样是需要保证本节点的数据库是空的，如果之前已经同步过区块或者已经写入了创世区块，都需要删除。启动节点后，长安将会把所有写入数据库的键值作者：Cd_MrsFu123<https://www.bilibili.com/read/cv20808995>出处：bilibili