MongoDB 适配SM云规范

- 需求单：https://cdp.cestc.cn/productGroup/#/require/detail?productGroupId=1574936024094527490&itemId=10256523

编号	需求	描述	分析（参考后文）	开发	进度	PRD /UED
10256555	云数据库支持备份与恢复	应向客户提供下列信息，支持客户制定其自身的备份策略和规程： 1)备份的范围， 2)备份方式和数据格式， 3)验证备份数据完整性的规程， 4)恢复备份数据的规程，	1. 备份集加密存储，并包含密级信息 2. 只有密级匹配的实例，并提供解密密钥，才能恢复实例 3. 其余实现参考现有备份恢复设计 4. DM还不支持恢复 5. 补充单独做增量备份的能力（UED需要刷新）：一个大备份周期内，首次全量备份，多次增量备份	朱含	1)备份的范围，开发完成，自测中 2)备份方式和数据格式，开发完成，自测中 3)验证备份数据完整性的规程，开发完成，自测中 4)恢复备份数据的规程，开发完成，自测中	
10256556	云数据库实例支持加密传输	数据库实例应支持TLS 加密传输，防止传输过程中篡改：	1. 开启TLS 2. 证书管理机制 3. UED交互参考Redis已有实现	李林	1、开启、关闭的接口自测中。 2、下载和更新证书还在开发中	
10256557	云数据库支持透明加密	应提供透明数据加密能力，数据库在数据写入存储介质时对数据进行加密，从存储介质中读取数据时自动解密，防止物理层篡改。	1. 密钥管理(实例内自签密文保存) 2. 内核持久化数据时能够加密写，读解密 3. UED交互：开通页指定是否打开透明加密，且不可更改；详情页显示是否启用透明加密。	搁置，实例不支持		
10256558	云数据库支持残余信息清除	a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除； b)应保证存有数据的存储空间被释放或重新分配前得到完全清除； c)应可以对指定数据及其所有副本进行全面的清除。通过删除用户与数据之间的素引关系，并将内存、存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原；	1. 有条件的话，对本地盘数据进行覆写清零，确保不可还原。 2. 判例是：信息或数据释放后，仍可非授权访问系统资源或进行操作，可判定为高风险。 3. UED不需体现，默认符合，黑屏确认。	王率帅	1.支持mysql实例相关信息清除（白屏迁移合入主干后还需要清楚相关mysql数据） 2.支持pvc和pv清除 3.支持secret清除 开发完成	
10256559	云数据库用户行为日志上报	b) 云数据库实例管理日志应至少包括日志产生时间、日志ID、 事件主体、事件客体、事件动作、日志级别、事件结果等信息； c) 云数据库用户行为日志应至少包括操作时间、客户端标识、客户端 地址、用户名、数据库标识、数据库类型、数据库端口、操作命令、操作结果(操作成功或失败、影响行数)、操作返回内容(查询结果)等信息。	1. 依要求完善日志体系和日志字段内容。 2. 参考现有日志交互设计	王率帅，在梳理字段 审计日志缺少： 客户端地址 用户名 操作命令 客户端标识 数据库端口 操作状态	待沟通： 审计日志对接：陈实 （朱含跟进一下字段） 行为日志：郑翼斐	

10256560	云数据库实例增强身份认证	a) 云数据库实例应提供并启用登录失败处理功能，应配置结束会话、限制连续登录失败的次数和当登录连接超时自动退出等相关措施； b) 当运维终端访问云数据库实例时，访问终端和云数据库实例之间宜建立双向身份验证机制。	1. 连续登陆失败超过5次，锁定账户；提供运维管理员解锁功能。详情页账号列表中显示账户是否被锁定的状态，及解锁操作。 2. 会话超时断开（一般会有） 3. 双向身份验证：开启TLS/SSL双向认证 4. 运维终端(DBPaaS/DMS) 访问数据库要有配置证书的环节。	搁置，实例不支持		
10256561	云数据库实例提供身份防冒用	a) 云数据库实例应具备默认空闲操作时限的功能，当空闲操作时间超过客户规定时限后，应断开会话或重新鉴别； b) 云数据库实例应具备设置访问白名单的功能，如通过配置网络掩码等； c) 云数据库实例登录的用户应使用全局唯一且不可重用的身份标识。	a) 会话超时断开（已具备） b) 白名单（已具备） c）指云账号（已具备）（数据库账号符合数据库自身要求即可）。	李林	1、用户的唯一且不可重用 开发完成	
10256562	云数据库实例账号密码规范改造	a) 云数据库实例对于基于口令的鉴别： 1) 应设立相关机制，能够强制执行最小口令复杂度，包括：至少包含大写字母、小写字母、数字、特殊符号三种字符的组合、至少10个字符、口令不得与账户一致等； 2) 应对存储的口令使用密码算法加密，宜满足国家密码管理的有关规定； b) 云数据库实例应对口令的传输执行安全保护，如使用HTTPS 保护口令机密性；	a) 1）基于云管创建的口令，密码强度有规范，确认一下是否符合。 2）数据库存储的口令采用国密算法加密 b）管控面API走HTTPS协议（Open API和 inner API）	国密算法加密不支持		
10256529	云数据库产品支持密级管理	云平台内产品实例支持设置和查看密级，密级设置后不允许修改，不同密级实例间禁止互访，数据迁移必须在相同密级的资源内迁移	1. 开通实例时指定密级 2. 实例详情页中提供密级查看 3. 密级不允许修改 4. DTS的云上实例的迁移、同步要识别密级，相同密集的资源内可迁移同步 5. 密级分类, 密级由低到高：内部、秘密、机密 6. 补充需求：按照硬件密级来调度，亲和密级标签	朱含	1) 尚未开发，待实现	

- # 需求：云数据库支持备份与恢复

基础能力：数据库产品备份恢复方案 - 信创云BU-PaaS平台开发部 - WIKI (cestc.cn)

当前设计已支持：用户指定备份策略，指定备份范围（选择实例，设置备份时间），备份方式（自动备份/手动备份, 支持全量和增量备份）

补充开发功能点：

1. 数据格式：
    a. 功能设计：
        i. 支持压缩和非压缩格式存储备份集数据
        ii. 压缩算法用户不可选，软件内置（推荐压缩率和性能兼顾的算法，如lz4，zlib等）
        iii. 同样的数据量，启用压缩格式存储的备份集应当较非压缩格式的备份集小。
    b. 交互设计：
        i. 在”备份策略“页面，增加”启用压缩“复选框，并提示”压缩格式可以节约存储空间，但更耗费时间和计算资源“。
        ii. 在”备份集“页面，在原有列项设计上，补充”压缩“或”非压缩“展示列；可查看压缩格式的备份集，”备份大小“值明显小于非压缩格式备份集
2. 验证备份数据完整性的规程：
    a. 功能设计：
        i. 备份集应当加密存储。备份集数据脱离当前实例的备份管理，无法解读。
        ii. 加密使用的密钥由密钥管理服务产生和管理，不支持用户设置密钥。
        iii. 备份集应当携带数据库实例的”**密级**“信息。将一个备份集恢复到目标实例（可能是原实例，也可以是新实例），目标实例必须与备份集的”密级“保持一致，才允许恢复。
        iv. 管控元数据库中应当存储每个备份集的MD5信息摘要用于校验，当执行恢复操作时，读取备份集文件时，需要通过MD5信息摘要校验备份集是否被篡改。

v. 备份集加密提供开关选择
1. 如果实例设定了密级，加密必选，不可更改
2. 如果实例未设定密级，加密可选，默认不加密
3. 密级是在实例开通时指定，切不可求改；备份集加密选项在实例开通后的备份策略配置页中选择。

b. 交互设计：
i. ”恢复任务“页面中，针对数据完整性的规程验证结果如失败，则在 ”任务状态“ 失败的提示信息中显示具体原因：
1. 当密钥不正确导致的解密失败，提示”未授权的备份集“
2. 当密级不匹配导致的失败，提示”目标实例（$密级）与备份集($密级) 密级不匹配“
3. 当由于MD5信息摘要校验失败，提示”备份集不完整或被篡改“

3. 恢复备份数据的规程：（请参考2，已经覆盖本功能点）
4. 备份策略优化（减少全量备份次数）：

a. 功能设计：
i. 增量备份：可按周/按天指定，可指定备份开始时段，可以指定是否开启压缩和加密
1. 增量备份下的全量备份设定：
a. 必须启用，需指定每N次增量，执行一次全量，首次执行增量，必执行全量。N的取值范围[1，10]
b. RDS在备份管理时，从数据备份恢复安全和一致角度出发，发现有必要发起额外的全量备份时，也可即时执行全量备份（即便这次备份是计划外的）。
2. 自动备份的增量是基于自动备份的最近次增量或上次全量
3. 假定自动备份策略是每天增量，每3次增量做一次全量，那产生的备份集是：
全量（D1），增量（D1-D2），增量（D2-D3），增量（D3-D4）+全量（D4），增量（D4-D5），增量（D5-D6），... ...

ii. 提供备份规则的汇总描述
iii. 支持仅全量备份：可按周/按天指定，可指定备份开始时段, 可以指定是否开启压缩和加密
1. 可能一：用户有需求，下发仅作全量备份的配置
2. 可能二：部分数据库产品，由于内核限制，仅支持全量备份，不支持增量备份

iv. 支持手动备份：手动备份时，弹出提示对话框，说明即将发起一次全量备份，并提示是否启用压缩和加密（复用自动备份策略中加密和压缩的设定）。
v. 选定备份集执行实例恢复时：
1. 恢复的时间点是当前备份集时间，且当前备份集含有全量备份数据，即执行全量恢复即可。
2. 恢复的时间点早于当前备份集时间，或者当前备份集仅有增量备份数据，这种情况为任意时间点恢复。从当前备份集开始，按时间顺序沿着标识“自动备份”的备份集形成的链条，向前找起，确保恢复时间点至最近次全量备份之间的增量备份没有缺失，执行基于全量+增量的恢复。如果这段时间范围内缺失全量或增量备份集，则恢复任务报错，提示“备份集缺失”。注：备份集的缺失可能由于用户手动删除，备份策略中定期清理备份集，或者由于存储库不可访问。

b. 交互设计：
i. RDS MySQL详情-备份恢复-备份策略 (axshare.com)

ii.

- 需求：云数据库实例支持加密传输
  1. 需求描述：数据库实例应支持TLS 加密传输，防止传输过程中篡改。
  2. 功能设计：
     a. 数据库实例提供的连接要支持TLS/SSL, 支持启用和不启用
     b. 在启用TLS/SSL连接时，提供证书管理能力：下载证书、更新证书、证书有效期管理（默认一年）
     c. 数据库内核或代理中间件提供TLS/SSL加密传输能力，可基于此实现
     d. 证书的签发需采用安全部门提供的证书签发服务
  3. 交互设计
     a. 实例详情页提供：启用开关，展示证书有效期，下载证书、更新证书 按钮
     b. 参考Redis既有的UED稿：Redis详情-基本信息（20231230）（axshare.com）

c.

- 需求：云数据库支持透明加密

1. 需求描述：应提供透明数据加密能力，数据库在数据写入存储介质时对数据进行加密，从存储介质中读取数据时自动解密，防止物理层篡改。
2. 功能设计：
    a. 功能的标准叫法：透明数据加密TDE（Transparent Data Encryption）
    b. TDE通过在数据库层执行静止数据加密，阻止可能的攻击者绕过数据库直接从存储中读取敏感信息。经过数据库身份验证的应用和用户可以继续透明地访问应用数据（不需要更改应用代码或配置），而尝试读取表空间文件中的敏感数据的OS用户以及尝试读取磁盘或备份信息的未知用户将不允许访问明文数据。
    c. 开启透明数据加密TDE功能后，会对数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密。
    d. TDE加密使用的密钥由密钥管理服务产生和管理，不支持用户设置密钥。
    e. 加密机制：
        i. MySQL 8.0.16，InnoDB Data-at-Rest Encryption https://dev.mysql.com/doc/refman/8.0/en/innodb-data-encryption.html#innodb-data-encryption-about。
        ii. MySQL 5.7，InnoDB Data-at-Rest Encryption https://dev.mysql.com/doc/refman/5.7/en/innodb-data-encryption.html
        iii. 其余数据库产品，参考内核能力实现
    f. 限制1：TDE只能在创建实例时开通，开通后不可关闭，密钥不可修改。
    g. 限制2：开启透明加密的实例，应当允许备份，对应恢复操作只能恢复到本实例。 注：透明加密和备份集加密是两个独立的加密功能。
        i. 透明加密实例产生的备份集，恢复到新实例（无论是否开启TDE）时将会提示”未授权的备份集“。
        ii. 未开启TDE的实例产生的备份集，恢复到开启TDE的新实例时将会提示”未授权的备份集“。
3. 交互设计：
    a. 实例开通页：透明数据加密：启用（复选框，默认不启用）
    b. 实例详情页：透明数据加密： 已启用/未启用

• 需求：云数据库支持残余信息清除

1. 需求描述：
    a. 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
    b. 应保证存有数据的存储空间被释放或重新分配前得到完全清除；
    c. 应可以对指定数据及其所有副本进行全面的清除。通过删除用户与数据之间的素引关系，并将内存、存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原；
2. 功能设计：
    a. 数据库实例在释放后，应当删除
        i. 管控元数据库中对应该实例的鉴权和描述信息
        ii. 实例的业务数据删除（local pv上的数据）
        iii. 实例的CR资源
    b. 补充： 跟OS或CCOS协商机制，对文件做硬清除
        i. 底座张铭在支持调查清除机制
        ii. 参考：技术|3 个在 Linux 中永久并安全删除文件和目录的方法
    c. 数据回收站
        i. 运营侧已经做了回收站能力。
        ii. 涉密云需求的四个产品后端对sc的删除策略对齐为delete
        iii. 其余产品：如果已实现延期清理策略，可保留。如果未实现延期清理，删除策略应为delete
3. 交互设计：（无）

• 需求：云数据库用户行为日志上报

1. 需求描述：
    a. 云数据库实例管理日志应至少包括日志产生时间、日志 ID、 事件主体、事件客体、事件动作、日志级别、事件结果等信息；
    b. 云数据库用户行为日志应至少包括操作时间、客户端标识、客户端 地址、用户名、数据库标识、数据库类型、数据库端口、操作命令、操作结果(操作成功或失败、影响行数)、操作返回内容(查询结果)等信息。
2. 功能设计：
    a. 参考既有日志设计：数据库产品日志管理PRD - 信创云BU-PaaS平台开发部 - WIKI (cestc.cn)
    b. “操作日志” 对应 “云数据库实例管理日志”

列项解释

时间：操作发生的时间戳，年月日时分秒，精度至少到s

序号：日志行顺序号 （日志ID）

用户：用户名 （事件主体）

客户端：客户端IP

实例ID：数据库实例 （事件客体）

操作类型：GET/SET （事件动作）

级别：日志的级别，如：FATAL,ERROR,WARN,INFO,TRACE,DEBUG

操作内容：本操作内容描述 （事件结果）

操作日志用于记录用户通过控制台入口、OpenAPI等向管控程序发起的操作，主要为实例管理类操作，如实例的创建、启停、变配等

c. “审计日志”对应“云数据库用户行为日志”

时间： 操作发生的时间戳，年月日时分秒，精度至少到ms

客户端地址：客户端的IP地址

用户名：当前登陆账号

数据库：当前登录的database名称

操作命令：查询语句或命令

操作状态：操作成功或失败

操作内容：影响行数或者返回结果集行数

客户端标识：推荐客户端MAC地址，受限于获取难度，以下替代可选，SessionId，ThreadId，ConnectionId

服务端标识：用于区分错误日志的来源，尤其是分布式部署架构中，有SHARD\主从副本的情况，各产品酌情设定取值，例如，

MySQL主从架构： $(server_id)

带SHARD+主从：$(shard_id)-M， $(shard_id)-S

通过POD-ID区分： $(pod-id)

通过POD-IP区分：$(pod-ip)

数据库类型：如MySQL/CeaSQL等

数据库端口：对外开放服务端口

3. 交互设计：参考既有交互设计
   a. RDS MySQL详情-操作日志（231130）（axshare.com） 需修改
   b. RDS MySQL详情-SQL日志（231130）（axshare.com） 需修改

• 需求：云数据库实例增强身份认证

1. 需求描述：
   a. 云数据库实例应提供并启用登录失败处理功能，应配置结束会话、限制连续登录失败的次数和当登录连接超时自动退出等相关措施；
   b. 当运维终端访问云数据库实例时，访问终端和云数据库实例之间宜建立双向身份验证机制。
2. 功能设计：
   a. 登录失败处理：
      i. “账号”管理页面中，增加每账号属性列项：失败次数、锁定时间，默认值为0。 参数可以修改
      ii. 内核版本支持说明：该功能需要内核能力配合支持，以MySQL为例，8.0.19之后版本支持。因此界面上可统一配置，但需增加说明“ 该参数仅对内核版本8.x有效”提示。
      iii. MySQL为例，可据此实现：

```
CREATE USER 'u1'@'localhost' IDENTIFIED BY 'password'
FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME 3;


ALTER USER 'u2'@'localhost'
FAILED_LOGIN_ATTEMPTS 4 PASSWORD_LOCK_TIME UNBOUNDED;



ERROR 3957 (HY000): Access denied for user user.
Account is blocked for D day(s) (R day(s) remaining)
due to N consecutive failed logins.


 -  (lanmper.cn)
```

   b. 连接超时处理：基于“参数“配置能力，已经支持
   c. 双向身份验证：启用TLS/SSL，即可认为客户端和服务端是双向认证的。运维客户端指DMS，在连接时需要基于TLS/SSL连接数据库。
3. 交互设计：
   a. 账号：需修改，RDS MySQL详情-账号 (axshare.com)
   b. 参数更新：已经具备
   c. 双向认证：TLS/SSL需设计

- 需求：云数据库实例提供身份防冒用

1. 需求描述：
   a. 云数据库实例应具备默认空闲操作时限的功能，当空闲操作时间超过客户规定时限后，应断开会话或重新鉴别；
   b. 云数据库实例应具备设置访问白名单的功能，如通过配置网络掩码等；
   c. 云数据库实例登录的用户应使用全局唯一且不可重用的身份标识。
2. 功能设计
   a. 空闲操作超时：基于“参数“配置能力，已经支持
   b. 白名单：已经支持；数据库产品绑定EIP及设置IP白名单 - 信创云BU-PaaS平台开发部 - WIKI (cestc.cn)
   c. 身份唯一标识：用户名，不可重用。（可不真正删除用户，而是隐藏被删除用户，这样新建重名用户即不允许）
   d. 限制：sm场景，不开放高权限账号
3. 交互设计（无）

- 需求：云数据库实例账号密码规范改造

1. 需求描述：
   a. 云数据库实例对于基于口令的鉴别：
      i. 应设立相关机制，能够强制执行最小口令复杂度，包括：至少包含大写字母、小写字母、数字、特殊符号三种字符的组合、至少10个字符、口令不得与账户一致等；
      ii. 应对存储的口令使用密码算法加密，宜满足国家密码管理的有关规定；
   b. 云数据库实例应对口令的传输执行安全保护，如使用HTTPS 保护口令机密性；
2. 功能设计：
   a. 密码复杂度：
      i. 控制台”账号“设置密码应当做复杂度校验
      ii. 考虑到用户可以通过高权限账号自行设定修改密码，内核应该提供密码复杂度校验能力：mysql：validate_password
      iii. 密码复杂度：至少包含大写字母、小写字母、数字、特殊符号三种字符的组合、至少10个字符、口令不得与账户一致
   b. 密码存储：
      i. 加密存储，MySQL支持：`mysql_native_password caching_sha2_password sha256_password`
      ii.
   c. `OpenAPIInner APIhttps V5`
3. 交互设计：无

- 需求：云数据库产品支持密级管理

1. 需求描述：
   a. 云平台内产品实例支持设置和查看密级，密级设置后不允许修改，不同密级实例间禁止互访，数据迁移必须在相同密级的资源内迁移
2. 功能设计
   a. 密级分类,：密级由低到高：内部、秘密、机密
   b. 线上系统的旧实例，兼容处理，认为是：密级未设定

c. 实例开通时指定密级
d. 实例详情页中可查看实例的密级
e. 实例的密级不允许修改
f. DTS在做迁移和同步时，需要查询识别源目实例的密级，
    i. 只有相同密级的实例之间允许迁移和同步。
    ii. 对于云下实例，视为未设定密级
    iii. 由于密级不匹配导致的迁移任务创建失败，需提示”密级不匹配“信息
g. 服务器密级匹配：
    i. 数据库节点需绑定密级标签
    ii. 产品实例依据自身密级，亲和密级标签。
    iii. DBPaaS提供在数据库资源池节点上增打密级标签的能力
    iv. 密级标签定义：
        1. 内部：node-pool.ccos.io/restricted: "true"
        2. 秘密：node-pool.ccos.io/secret: "true"
        3. 机密：node-pool.ccos.io/confidential: "true"

3. 交互设计：
    a. 参考云主机密级管理：CECSTACK-V5密级管理 - 信创云BU-IaaS平台开发部 - WIKI (cestc.cn)

• 安全支撑服务：

1. 证书配置：00.CCOS新架构集群证书配置管理方案 - 信创云BU-云安全资料共享 - WIKI (cestc.cn)
2. 密钥管理：
    a. https://wiki.cestc.cn/pages/viewpage.action?pageId=232278565
    b. DES的sdk的说明：

    https://wiki.cestc.cn/pages/viewpage.action?pageId=228446588
    KES的接口说明：

    https://wiki.cestc.cn/pages/viewpage.action?pageId=151683951

    对于不方便使用SDK的场景，也可以使用DES的restful API：

    https://wiki.cestc.cn/pages/viewpage.action?pageId=121594331

等保知识|测评高风险项详解：安全计算环境-CSDN博客

等保2.0安全计算环境之云计算扩展标准测评（云平台） - FreeBuf网络安全行业门户

数据安全怎么做：数据分类分级 - FreeBuf网络安全行业门户