**一、新OSS路径定义规则：**

|  |
| --- |
| oss://{keyID}:{SecretKey}@{host}{:port}/{bucket}/{object} ?[{param}={param}] |

示例：oss://user1:Sakyxxiarg;waXgalkdg@172.16.131.40:9020/test/2019/01/02/my.avi?version=2&product=emc&type=https&encode=0

定义如下：

|  |  |
| --- | --- |
| keyID | Keyid |
| SecretKey | 伪secretkey，需要通过特殊算法处理后才能使用  （**见“二”**） |
| host | S3存储的地址，IP或者域名，不能表示是https还是http |
| port | 访问端口 |
| BucketName | 桶名 |
| object | 文件名，包含路径 |
| param | 扩展定义 |

Param定义如下：

|  |  |
| --- | --- |
| version | S3存储使用协议版本号 |
| product | 存储厂商。说明：对于部分厂商使用的S3协议是私有的，可以通过厂商进行区分 |
| type | 服务端请求类型：http或者https |
| encode | SecretKey是否需要解密：0不需要；1需要 |

**二、SecretKey的解密规则（包含NAS、FTP等的密码）**

由于基于个人空间强管理的场景下，内容入库端需要从hive获取**可用路径**。该可用路径可能是一个NAS的UNC路径，也可能是一个S3的Bucket路径，这些路径都需要密码访问。由于**安全考虑密码不能直接在网络上传输**，因此，总体的规则如下：

* 对于所有的密码、SecretKey，在获取的时候都是**密文返回**
* 对于所有的密码、SecretKey，在使用的时候都需要**解密使用**

比如：

* **对于nas**

//host/test/ 这个unc的实际访问用户密码为admin, admin

hive返回的是admin，zxcasdgasdga

加密使用是admin，**encode**(zxcasdgasdga) => admin, admin

* **对于S3**

http://host/buckettest这个bucket的实际访问凭据为keyid=admin, secretkey=aasdg34rabehsdhsdfa

hive返回的是admin, zxcasdgasdga

加密使用是admin，**encode**(zxcasdgasdga) => admin, aasdg34rabehsdhsdfa

**统一的解密算法如下：**

|  |
| --- |
| **$key\_to\_use = Aes($public\_, Hex2Byte($key\_from\_hive))**  **其中：**  **$key\_from\_hive是hive返回的存储访问密码、或S3的secretKey**  **$public\_是一个固定密钥，为：sobeystoragekey\_**  **$key\_to\_use是解密后，访问存储的真实密码或secretKey**  **算法验证：**  **1、**  **$key\_from\_hive = 03a7a84c5aa47f5207ea93c8027543c2**  **$key\_to\_use = 123456**  **2、**  **$key\_from\_hive = 0ccad39e2e32b11dadec0f1a19a94d4c**  **$key\_to\_use = abc** |