

mysql>

2.15 제품 운용

2.15.1 함수 설명

DA에서 제공되는 함수와 사용하는 방법에 대해서 설명한다.

2.15.1.1 파라미터 설명

2.15.1.1.1 L_KEY



L_KEY : 암호화/복호화 때 사용하는 암호화 키

- 설정 파일(scpdb_agent.ini)의 [KEYINFO] 중 ALIAS 값
- 아래 [설정 파일 예제]의 경우 ALIAS는 'KEY1'과 'KEY2'이다.
- ALIAS는 SCPS파일로 암호화 할 것인지, SG-KMS의 서비스 ID로 암호화 할 것인지 설정 가능하다.

[설정 파일 예제]

- 설정 파일(scpdb_agent.ini)의 [KEYINFO] 중 ALIAS 값
KEY1=AES256.SCPS
KEY2=ARIA256

[함수 사용 예제]

SELECT ENC_STR('KEY1', 'abc') AS RESULT;

2.15.1.1.2 L_DATA



L_DATA : 평문(암호화 함수일 경우), 암호문(복호화 함수일 경우)



DA에서 제공하는 암호화 함수에서 성능 향상을 위해 라이브러리에서 정책 이름(KEYINFO ALIAS)을 바탕으로 Cash하여 동작한다. 정책 이름은 같은데 실제 키(대칭 키)가 다른 정책을 사용하면 Cash에서 이전 키로 복호화를 시도하여 오류가 발생한다. 이 상황을 해결하기 위해서는 데이터베이스 서버 재시작이 필요하다

다.

표 2-5 DA 함수 (MYSQL)

함수 명	입력		출력	
ENC_STR	I_KEY	IN 문자열	Hex String 암호문	
	I_DATA	IN 문자열 (평문)		
ENC_B64	I_KEY	IN 문자열,	Base64 Encording 암호문	
	I_DATA	IN 문자열 (평문)		
DEC_STR	I_KEY	IN 문자열,	평문	
	I_DATA	IN 문자열 (Hex String 암호문)		
DEC_B64	I_KEY	IN 문자열,	평문	
	I_DATA	IN 문자열 (base64 String 암호문)		
INDEX_STR	I_KEY	IN 문자열,	Hex String 암호문	
	I_DATA	IN 문자열 (평문),		
	I_TYPE	IN 문자열 " or 'IX '(Plug-IN 연동 시 사용)		
DEC_INDEX_STR	I_KEY	IN 문자열,	Hex String 암호문 입력받아 OPE 데이터	
	I_DATA	IN 문자열 (암호문),		
	I_TYPE	IN 문자열 " or 'IX '(Plug-IN 연동 시 사용)		
DEC_INDEX_B64	I_KEY	IN 문자열,	Base64 Encording 암호문 입력받아 OPE 데이터	
	I_DATA	IN 문자열 (암호문),		
	I_TYPE	IN 문자열 " or 'IX '(Plug-IN 연동 시 사용)		
HASH_STR	I ALOG	IN 숫자,	SHA1 =70	Hex String 해쉬 암호문
			SHA256 =71	
			SHA384 =72	
			SHA512 =73	
			HAS160 =74	
	I_DATA	IN 문자열		
HASH_B64	I ALOG	IN 숫자,	SHA1 =70	Base64 String 해쉬 암호문
			SHA256 =71	

			SHA384 =72
			SHA512 =73
			HAS160 =74
	I_DATA	IN 문자열	
HEXTOB64	I_DATA	IN 문자열 (Hex String 암호문)	base64 Encording 암호문
B64TOHEX	I_DATA	IN 문자열 (base64 Encording 암호문)	Hex String 암호문
CONFIG_REINIT			성공시 'SUCCESS', 그외 에러

2.15.2 함수 호출 예제

1. ENC_STR

```
mysql> SELECT ENC_STR('KEY1', 'abc');
```

2. ENC_B64

```
mysql> SELECT ENC_B64('KEY1', 'abc');
```

3. DEC_STR

```
mysql> SELECT DEC_STR('KEY1', ENC_STR('KEY1', 'abc'));
```

4. DEC_B64

```
mysql> SELECT DEC_B64('KEY1', ENC_B64('KEY1', 'abc'));
```

5. INDEX_STR

[DP 제품에 연동 하지 않을 경우]

```
mysql> SELECT INDEX_STR('KEY1', 'abc', '');
```

[DP 제품에 연동 할 경우]

```
mysql> SELECT INDEX_STR('KEY1', 'abc', 'IX');
```

6. DEC_INDEX_STR, DEC_INDEX_B64

DP 제품에 연동 하지 않을 경우

```
mysql> SELECT DEC_INDEX_STR('KEY1', ENC_STR('KEY1', 'abc'), '');
```

```
mysql> SELECT DEC_INDEX_B64('KEY1', ENC_B64('KEY1', 'abc'), '');
```

DP 제품에 연동 할 경우

```
mysql> SELECT DEC_INDEX_STR('KEY1', ENC_STR('KEY1', 'abc'), 'IX');
```

```
mysql> SELECT DEC_INDEX_B64('KEY1', ENC_B64('KEY1', 'abc'), 'IX');
```

7. HASH_STR

```
mysql> SELECT HASH_STR( 71, 'abc' );
```

8. HASH_B64

```
mysql> SELECT HASH_B64( 71, 'abc' );
```

9. HEXTOB64

```
mysql> SELECT HEXTOB64('A305378D8F974F1C1537ED7CB0CB959245D1AC31');
```

10. B64TOHEX

```
mysql>SELECT B64TOHEX('owU3jY+XTxwVN+18sMuVkkXRrDE=');
```

11. CONFIG_REINIT

```
mysql>SELECT CONFIG_REINIT();
```