From: honda@luckstar.com.tw

Date: 2012.04.16

Subject: 如何建立加密欄位

說明

A 使用pwdencrypt()與pwdcompare機制.

B 使用 hashbytes().

/\* A 使用pwdencrypt()與pwdcompare()機制:

1 pwdencrypt()加密的內容可用pwdcompare()=1方式驗證.

2 pwdencrypt()每次加密的結果不同, 但是都可以用pwdcompare()=1方式驗證.

\*/

select PWDENCRYPT('test1')

go

/\*

每次執行結果會不同,

例如測試結果為x010028E17BB1B292DB106DC0F4E92252D8845CEEE4007E9601C8,

可驗證如下, 若結果=1則正確,否則為.

\*/

select PWDCOMPARE('test1', 0x010028E17BB1B292DB106DC0F4E92252D8845CEEE4007E9601C8)

go

/\* 參考\*/

USE TEMPDB

GO

declare @hash varbinary (255)

CREATE TABLE tempdb..h (id\_num int, hash varbinary (255))

SET @hash = pwdencrypt('123') -- encryption

INSERT INTO tempdb..h (id\_num,hash) VALUES (1,@hash)

SET @hash = pwdencrypt('123')

INSERT INTO tempdb..h (id\_num,hash) VALUES (2,@hash)

SELECT TOP 1 @hash = hash FROM tempdb..h WHERE id\_num = 2

SELECT pwdcompare ('123', @hash) AS [Success of check] -- Comparison

SELECT \* FROM tempdb..h

INSERT INTO tempdb..h (id\_num,hash)

VALUES (3,CONVERT(varbinary (255),

0x01002D60BA07FE612C8DE537DF3BFCFA49CD9968324481C1A8A8FE612C8DE537DF3BFCFA49CD9968324481C1A8A8))

SELECT TOP 1 @hash = hash FROM tempdb..h WHERE id\_num = 3

SELECT pwdcompare ('123', @hash) AS [Success of check] -- Comparison

SELECT \* FROM tempdb..h

DROP TABLE tempdb..h

GO

/\* B 以上的方法如果不放心, 可改用hashbytes()自行處理MD5或SHA1加密(或自行由外部程式加密) \*/

/\* 1 MD5結果為BYTES, SHA1結果為BYTES. 以下適用於存檔為varbinary欄位\*/

select hashbytes('MD5','test1') as MD5,hashbytes('SHA1','test1') as SHA1;

/\* 2 存入varchar 欄位時, 需轉換為字串\*/

select sys.fn\_VarBinToHexStr(hashbytes('MD5','test1')) as MD5,sys.fn\_VarBinToHexStr(hashbytes('SHA1','test1')) as SHA1;

/\* 3 以上方法, 每次都會固定回傳相同的加密後結果.

簡單加入salt 19BYTES處理: yyyy-mm-dd hh:mi:ss(24h). 將salt值放在加密值後面,

解碼時需先取得SALT值, 再結合password才能取得相同的加密值.

註: salt值可分開存放, 不需要與加密結果放在一起,

註: salt值的演算法可再嚴密一些, 本例僅為展示處理方式, 簡化演算過程.

\*/

declare @salt varchar (19)

declare @MD5 varchar(128)

declare @SHA1 varchar(128)

declare @right19 varchar(19)

set @salt = convert(varchar(19), getdate(), 120)

set @MD5 = sys.fn\_VarBinToHexStr(hashbytes('MD5','test1' + @salt ))+@salt

set @SHA1 = sys.fn\_VarBinToHexStr(hashbytes('SHA1','test1' + @salt))+@salt

select @salt as salt, @MD5 as md5, @SHA1 as sha1

set @right19 = right(@MD5, 19)

set @MD5 = sys.fn\_VarBinToHexStr(hashbytes('MD5','test1' + @right19 ))+@right19

set @SHA1 = sys.fn\_VarBinToHexStr(hashbytes('SHA1','test1' + @right19 ))+@right19

select @right19 as right19, @MD5 as md5, @SHA1 as sha1

go