SQL Server Encrypted Backup and Restore Guide with Certificate Handling

# 1. Overview

This document provides a complete guide to:

- Taking encrypted backups using Ola Hallengren's maintenance scripts

- Backing up and restoring certificates used for encryption

- Restoring full and log backups using the certificate

# 2. Backup with Certificate Using Ola Hallengren

Prerequisites:

- SQL Server 2014 or later

- Certificate created in master database

Create a certificate:

USE master;

CREATE CERTIFICATE BackupEncryption

WITH SUBJECT = 'Backup Encryption';

Backup script using encryption:

EXEC dbo.DatabaseBackup

@Databases = 'USER\_DATABASES',

@Directory = 'E:\Backup',

@BackupType = 'FULL',

@Encrypt = 'Y',

@EncryptionAlgorithm = 'AES\_256',

@ServerCertificate = 'BackupEncryption',

@Verify = 'Y',

@Checksum = 'Y';

# 3. Backing Up the Certificate and Private Key

Important: If the certificate is lost, encrypted backups cannot be restored.

Backup the certificate:

USE master;

BACKUP CERTIFICATE BackupEncryption

TO FILE = 'E:\CertBackup\BackupEncryption.cer'

WITH PRIVATE KEY (

FILE = 'E:\CertBackup\BackupEncryptionKey.pvk',

ENCRYPTION BY PASSWORD = 'YourStrongPassword@123'

);

# 4. Restoring the Certificate on Another Server

USE master;

CREATE CERTIFICATE BackupEncryption

FROM FILE = 'E:\CertBackup\BackupEncryption.cer'

WITH PRIVATE KEY (

FILE = 'E:\CertBackup\BackupEncryptionKey.pvk',

DECRYPTION BY PASSWORD = 'YourStrongPassword@123'

);

# 5. Restoring Encrypted Full and Log Backups

Full Restore (WITH NORECOVERY):

RESTORE DATABASE YourDB

FROM DISK = 'E:\Backup\YourDB\_FULL.bak'

WITH NORECOVERY,

ENCRYPTION(ALGORITHM = AES\_256, SERVER CERTIFICATE = BackupEncryption);

Log Backup Restore:

RESTORE LOG YourDB FROM DISK = 'E:\Backup\YourDB\_LOG1.trn' WITH NORECOVERY;

RESTORE LOG YourDB FROM DISK = 'E:\Backup\YourDB\_LOG2.trn' WITH RECOVERY;

# 6. Common Errors and Resolutions

| Error Message | Cause | Solution |

|---------------|-------|----------|

| @ServerCertificate not supported | Invalid or missing certificate | Verify in sys.certificates |

| Certificate has not been backed up | No .cer or .pvk file created | Backup certificate and private key |

| Cannot find server certificate | Certificate not restored on target server | Use CREATE CERTIFICATE ... FROM FILE |

| The step failed | Directory access issue or incorrect parameter | Check job history and folder permissions |

# 7. Recommendations

- Always store certificate and private key in a secure, offsite location

- Schedule log backups every 15 minutes (or as per RPO)

- Regularly test restore operations, including certificate restoration

# 8. Error: Msg 15581 - Master Key Required

Error Message: Msg 15581, Level 16, State 1, Line 4  
'Please create a master key in the database or open the master key in the session before performing this operation.'  
  
### Resolution Steps:  
1. \*\*Check if the Master Key Exists\*\*  
 Run the following query to check if the master key exists in the target database:  
 ```sql  
 USE master;  
 GO  
 SELECT \* FROM sys.symmetric\_keys;  
 ```  
 If no results are returned, the master key needs to be created.  
  
2. \*\*Create a Master Key (If It Doesn't Exist)\*\*  
 If the master key doesn't exist, create it with the following command:  
 ```sql  
 USE master;  
 GO  
 CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'YourStrongMasterKeyPassword';  
 ```  
  
3. \*\*Open the Master Key (If It Already Exists)\*\*  
 If the master key exists, ensure it is unlocked by running the following command:  
 ```sql  
 USE master;  
 GO  
 OPEN MASTER KEY DECRYPTION BY PASSWORD = 'YourStrongMasterKeyPassword';  
 ```  
  
4. \*\*Restore the Certificate Again\*\*  
 After creating or opening the master key, restore the certificate using this command:  
 ```sql  
 USE master;  
 CREATE CERTIFICATE BackupEncryption  
 FROM FILE = 'E:\CertBackup\BackupEncryption.cer'  
 WITH PRIVATE KEY (  
 FILE = 'E:\CertBackup\BackupEncryptionKey.pvk',  
 DECRYPTION BY PASSWORD = 'YourStrongPassword@123'  
 );  
 ```  
  
### Important Notes:  
- \*\*Password\*\*: Use a strong password for both the master key and private key, and ensure consistency when restoring the certificate.  
- \*\*Master Key Protection\*\*: The master key is critical for the encryption of certificates and asymmetric keys. Ensure the password is stored securely.