

Rotate the Transparent Data Encryption Protector Using PowerShell

Last updated by | Soma Jagadeesh | Jan 10, 2021 at 9:46 PM PST


Contents

- [Issue](#)
- [Investigation/Analysis](#)
- [Mitigation](#)
- [RCA \(optional\)](#)
- [More Information \(optional\)](#)
- [Public Doc Reference \(optional\)](#)
- [Internal Reference \(optional\)](#)
- [Classification](#)

Issue

Rotate the Transparent Data Encryption Protector Using PowerShell

Prerequisites a) This tutorial assumes that you are already using a key from Azure Key Vault as the TDE Protector for an Azure SQL Database or Azure SQL Data Warehouse

1. You must have Azure PowerShell version 4.2.0 or newer installed and running. b) [Recommended but Optional] Have a Hardware Security Module (HSM) or local key store
2. For creating a local copy of the encryption key
3. Instructions for using a hardware security module (HSM) and Key Vault <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview> 

Overview This tutorial describes key rotation for an Azure SQL server using a TDE protector from Azure Key Vault. Rotating an Azure SQL server's TDE protector means switching to a new asymmetric key that protects the databases on the server. Key rotation is an online operation and should only take a few seconds to complete, because this only decrypts and re-encrypts the database's data encryption key, not the entire database.

Note: A paused SQL Data Warehouse must be resumed before key rotations.

Warning: Do Not Delete previous versions of the key after a rollover. When keys are rolled over, there will be data encrypted with the previous keys, such as older database backups. There are three options to rotate the TDE protector on the server:

Option 1: Autorotation: Generate a new version of the existing TDE Protector key in Key Vault, under the same key name and key vault. The Azure SQL service will start using this new version within 24 hours.

- To create a new version:

```
Add-AzureKeyVaultKey -VaultName <KeyVaultName> -Name <KeyVaultKeyName> -Destination  
<HardwareOrSoftware>
```

Option 2: Manual rotation: Use this option to add a completely new key, which could be under a new key name or even another key vault.

Note: The combined length for the key vault name and key name cannot exceed 94 characters.

- Add a new key to Key Vault

```
Add-AzureKeyVaultKey -VaultName <KeyVaultName> -Name <KeyVaultKeyName> -Destination  
<HardwareOrSoftware>
```

- Add the new key from Key Vault to the server

```
Add-AzureRmSqlServerKeyVaultKey -KeyId <KeyVaultKeyId> -ServerName <LogicalServerName> -  
ResourceGroup <SQLDatabaseResourceGroupName>
```

--Set the key as the TDE protector for all resources under the server

```
Set-AzureRmSqlServerTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId <KeyVaultKeyId> -  
ServerName <LogicalServerName> -ResourceGroup <SQLDatabaseResourceGroupName>
```

Option 3: Switch the server's TDE Protector Type

- To switch the TDE protector from Microsoft-managed to BYOK mode: Set-
AzureRmSqlServerTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId <KeyVaultKeyId> -
ServerName <LogicalServerName> -ResourceGroup <SQLDatabaseResourceGroupName>
- To switch the TDE protector from BYOK mode to Microsoft-managed: Set-
AzureRmSqlServerTransparentDataEncryptionProtector -Type ServiceManaged -ServerName
<LogicalServerName> -ResourceGroup <SQLDatabaseResourceGroupName>

Investigation/Analysis

Mitigation

RCA (optional)

More Information (optional)

Public Doc Reference (optional)

Internal Reference (optional)

Classification

Root cause tree: Security/User Request/How-to/advisory

How good have you found this content?

