Windows PowerShell Get-Help on Cmdlet 'Invoke-SqlColumnMasterKeyRotation'

PS:\>Get-HELP Invoke-SqlColumnMasterKeyRotation -Full

NAME

Invoke-SqlColumnMasterKeyRotation

SYNOPSIS

Initiates the rotation of a column master key.

SYNTAX

Invoke-SqlColumnMasterKeyRotation [-InputObject] <Database> [-AccessToken <PSObject>] [-Encrypt {Mandatory | Optional | Strict}] [-HostNameInCertificate <String>]

[-KeyVaultAccessToken <String>] [-ManagedHsmAccessToken <String>] [-ProgressAction <ActionPreference>] [-Script] -SourceColumnMasterKeyName <String>

-TargetColumnMasterKeyName <String> [-TrustServerCertificate] [<CommonParameters>]

Invoke-SqlColumnMasterKeyRotation [[-Path] <String>] [-AccessToken <PSObject>] [-Encrypt {Mandatory | Optional | Strict}] [-HostNameInCertificate <String>]

[-KeyVaultAccessToken <String>] [-ManagedHsmAccessToken <String>] [-ProgressAction <ActionPreference>] [-Script] -SourceColumnMasterKeyName <String>

-TargetColumnMasterKeyName <String> [-TrustServerCertificate] [<CommonParameters>]

DESCRIPTION

The Invoke-SqlColumnMasterKeyRotation cmdlet initiates replacing an existing source column master key with a new target column master key for the Always Encrypted

feature.

The cmdlet retrieves all column encryption key objects that contain encrypted key values that are encrypted with the specified source column master key.

Then, the cmdlet decrypts the current encrypted values, re-encrypts the resulting plaintext values with the target column master key, and then updates the impacted

column encryption key objects to add the new encrypted values.

As a result, each impacted column encryption key contains two encrypted values: one produced using the current source column master key and another, produced using

the target column master key.

If a source or a target column master key is stored in Azure, you need to specify a valid authentication token (or tokens) for a key vault or a managed HSM holding

the key. Alternatively, you can authenticate to Azure with Add-SqlAzureAuthenticationContext before calling this cmdlet.

> `Module requirements: version 21+ on PowerShell 5.1; version 22+ on PowerShell 7.x.`

PARAMETERS

-AccessToken <PSObject>

The access token used to authenticate to SQL Server, as an alternative to user/password or Windows Authentication.

This can be used, for example, to connect to `SQL Azure DB` and `SQL Azure Managed Instance` using a `Service Principal` or a `Managed Identity`.

The parameter to use can be either a string representing the token or a `PSAccessToken` object as returned by running `Get-AzAccessToken -ResourceUrl

https://database.windows.net`.

> This parameter is new in v22 of the module.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Encrypt <String>

The encryption type to use when connecting to SQL Server.

This value maps to the `Encrypt` property `SqlConnectionEncryptOption` on the SqlConnection object of the Microsoft.Data.SqlClient driver.

In v22 of the module, the default is `Optional` (for compatibility with v21). In v23+ of the module, the default value will be 'Mandatory', which may create a

breaking change for existing scripts.

> This parameter is new in v22 of the module.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HostNameInCertificate <String>

The host name to be used in validating the SQL Server TLS/SSL certificate. You must pass this parameter if your SQL Server instance is enabled for Force

Encryption and you want to connect to an instance using hostname/shortname. If this parameter is omitted then passing the Fully Qualified Domain Name (FQDN) to

-ServerInstance is necessary to connect to a SQL Server instance enabled for Force Encryption.

> This parameter is new in v22 of the module.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Database>

Specifies the SQL database object, for which this cmdlet runs the operation.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-KeyVaultAccessToken <String>

Specifies an access token for key vaults in Azure Key Vault. Use this parameter if the current and/or the target column master key is stored in a key vault in

Azure Key Vault.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ManagedHsmAccessToken <String>

Specifies an access token for managed HSMs in Azure Key Vault. Use this parameter if the current and/or the target column master key is stored in a managed HSM

in Azure Key Vault.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Path <String>

Specifies the path of the SQL database, for which this cmdlet runs the operation.

If you do not specify a value for this parameter, the cmdlet uses the current working location.

Required? false

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ProgressAction <ActionPreference>

Determines how PowerShell responds to progress updates generated by a script, cmdlet, or provider, such as the progress bars generated by the Write-Progress

cmdlet. The Write-Progress cmdlet creates progress bars that show a command's status.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Script [<SwitchParameter>]

Indicates that this cmdlet runs a Transact-SQL script that performs the task.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-SourceColumnMasterKeyName <String>

Specifies the name of the source column master key.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TargetColumnMasterKeyName <String>

Specifies the name of the target column master key.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TrustServerCertificate [<SwitchParameter>]

Indicates whether the channel will be encrypted while bypassing walking the certificate chain to validate trust.

In v22 of the module, the default is `$true` (for compatibility with v21). In v23+ of the module, the default value will be '$false', which may create a breaking

change for existing scripts.

> This parameter is new in v22 of the module.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

Microsoft.SqlServer.Management.Smo.Database

OUTPUTS

NOTES

Example 1: Initiate the process of rotating the column master key.

Invoke-SqlColumnMasterKeyRotation -SourceColumnMasterKeyName "CMK1" -TargetColumnMasterKeyName "CMK2"

This command initiates the process of rotating the column master key named CMK1, and replacing it with the column master key named CMK2.

Example 2: Initiate the process of rotating the column master key with authentication tokens specified

#?Connect?to?Azure?account.

```
Import-Module?Az.Accounts?-MinimumVersion?2.2.0
Connect-AzAccount

#?Obtain access?tokens.
$keyVaultAccessToken = (Get-AzAccessToken -ResourceUrl https://vault.azure.net).Token
$managedHSMAccessToken = (Get-AzAccessToken -ResourceUrl https://managedhsm.azure.net).Token

# Pass the tokens to the cmdlet.
Invoke-SqlColumnMasterKey -SourceColumnMasterKeyName CMK1 -TargetColumnMasterKeyName CMK2 -KeyVaultAccessToken $keyVaultAccessToken -ManagedHSMAccessToken $managedHSMAccessToken
```

The example initiates the process of rotating the column master key named CMK1 and replacing it with the column master key named CMK2. We assume one of the keys is stored in a key vault and the other key is stored in a managed HSM in Azure Key Vault. The `Invoke-SqlColumnMasterKey` will use the obtained authentication tokens to communicate with key vault and managed HSM endpoints.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/sqlserver/invoke-sqlcolumnmasterkeyrotation

Complete-SqlColumnMasterKeyRotation