Full credit is given to all the above companies including the Operating System that this PDF file was generated!

Windows PowerShell Get-Help on Cmdlet 'New-AzCosmosDbClientEncryptionKey'

PS:\>Get-HELP New-AzCosmosDbClientEncryptionKey -Full

NAME

New-AzCosmosDbClientEncryptionKey

SYNOPSIS

Creates a new CosmosDB Client Encryption Key.

SYNTAX

New-AzCosmosDbClientEncryptionKey -AccountName <System.String> -DatabaseName <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -EncryptionAlgorithmName <System.String> [-KeyEncryptionKeyResolver <Azure.Core.Cryptography.IKeyEncryptionKeyResolver>] -KeyWrapMetadata <Microsoft.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata> -Name <System.String> -ResourceGroupName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzCosmosDbClientEncryptionKey [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -EncryptionAlgorithmName <System.String> [-KeyEncryptionKeyResolver <Azure.Core.Cryptography.IKeyEncryptionKeyResolver>]

-KeyWrapMetadata

<Microsoft.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata> -Name <System.String> -SqlDatabaseObject

<Microsoft.Azure.Commands.CosmosDB.Models.PSSqlDatabaseGetResults> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzCosmosDbClientEncryptionKey creates a new CosmosDB Client Encryption Key.

PARAMETERS

-AccountName <System.String>

Name of the Cosmos DB database account.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DatabaseName <System.String>

Database name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EncryptionAlgorithmName <System.String>

Client Encryption Algorithm name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-KeyEncryptionKeyResolver <Azure.Core.Cryptography.IKeyEncryptionKeyResolver>

IKeyEncryptionKeyResolver interface of type Azure.Core.Cryptography.IKeyEncryptionKeyResolver

Required? false

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-KeyWrapMetadata <Microsoft.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata>

KeyWrapMetaData Object of type Microsoft.Azure.Commands.CosmosDB.PSSqlKeyWrapMetadata.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Client Encryption Key name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Name of resource group.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SqlDatabaseObject <Microsoft.Azure.Commands.CosmosDB.Models.PSSqlDatabaseGetResults>

Sql Database object.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

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.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata

System.Byte[]

Microsoft.Data.Encryption.Cryptography.EncryptionKeyStoreProvider

Microsoft.Azure.Commands.CosmosDB.Models.PSSqlDatabaseGetResults

OUTPUTS

Microsoft.Azure.Commands.CosmosDB.Models.PSSqlClientEncryptionKeyGetResults

Microsoft.Azure.Commands.CosmosDB.Exceptions.ConflictingResourceException

NOTES

---------- Example 1 ----------

$myKeyWrapMetadataObject =

[Microsoft.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata]::new([Microsoft.Azure.Management.CosmosDB.Models.KeyWrapMetadata]::new("myKekV1","AZURE_KEY_VAULT",

"https://contoso.vault.azure.net/keys/myKekV1/78deebed173b48e48f55abf87ed4cf71", "RSA-OAEP"))

New-AzCosmosDbClientEncryptionKey -AccountName myAccountName -DatabaseName myDatabaseName -ResourceGroupName myRgName -Name myClientEncryptionKeyName

-EncryptionAlgorithmName "AEAD_AES_256_CBC_HMAC_SHA256" -KeyWrapMetadata $myKeyWrapMetadataObject

Name : myContainerName

Id : /subscriptions/mySubscriptionId/resourceGroups/myRgName/providers/Microsoft.DocumentDB/databaseAccounts/myAccountName/sqlDatabases/myDatabaseName/clientEncr

yptionKeys/myClientEncryptionKeyName

Resource : Microsoft.Azure.Commands.CosmosDB.Models.PSSqlClientEncryptionKeyGetPropertiesResource

This example shows how a new key is created. If KeyEncryptionKeyResolver is not passed Azure Key Vault KeyResolver is used by default. The first command creates a

KeyWrapMetadata object with name myKekV1 of type AZURE_KEY_VAULT with value set to key id

https://contoso.vault.azure.net/keys/myKekV1/78deebed173b48e48f55abf87ed4cf71 and algorithm type "RSA-OAEP" used to encrypt the key. In the second command a new key

is created with name as set in myClientEncryptionKeyName variable and with KeyWrapMetadata set to value returned by first command.

---------- Example 2 ----------

$myKeyWrapMetadataObject =

[Microsoft.Azure.Commands.CosmosDB.Models.PSSqlKeyWrapMetadata]::new([Microsoft.Azure.Management.CosmosDB.Models.KeyWrapMetadata]::new("myKekV1","AZURE_KEY_VAULT",

"https://contoso.vault.azure.net/keys/myKekV1/78deebed173b48e48f55abf87ed4cf71", "RSA-OAEP"))

$azureKeyVaultKeyResolver = [Azure.Security.KeyVault.Keys.Cryptography.KeyResolver]::new([Azure.Identity.DefaultAzureCredential]::new())

New-AzCosmosDbClientEncryptionKey -AccountName myAccountName -DatabaseName myDatabaseName -ResourceGroupName myRgName -Name myClientEncryptionKeyName

-EncryptionAlgorithmName "AEAD_AES_256_CBC_HMAC_SHA256" -KeyWrapMetadata $myKeyWrapMetadataObject -KeyEncryptionKeyResolver $azureKeyVaultKeyResolver

Name : myContainerName

Id : /subscriptions/mySubscriptionId/resourceGroups/myRgName/providers/Microsoft.DocumentDB/databaseAccounts/myAccountName/sqlDatabases/myDatabaseName/clientEncr

yptionKeys/myClientEncryptionKeyName

Resource : Microsoft.Azure.Commands.CosmosDB.Models.PSSqlClientEncryptionKeyGetPropertiesResource

This example shows how a new key is created and how KeyEncryptionKeyResolver can be passed as a parameter. The first command creates a KeyWrapMetadata object with

name myKekV1 of type AZURE_KEY_VAULT with value set to key id https://contoso.vault.azure.net/keys/myKekV1/78deebed173b48e48f55abf87ed4cf71 and algorithm type

"RSA-OAEP" used to encrypt the key. The second command creates a Azure Key Vault KeyResolver object using the Azure Default credentials. In the third command a new

key is created with name as set in myClientEncryptionKeyName variable, KeyWrapMetadata set to value returned by first command and KeyEncryptionKeyResolver value set

to KeyResolver object obtained via the second command.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.cosmosdb/new-azcosmosdbclientencryptionkey

Get-AzCosmosDbClientEncryptionKey

Update-AzCosmosDbClientEncryptionKey