

Revalidation_Key_AzureCLI

Last updated by | Lisa Liu | Nov 6, 2020 at 10:36 AM PST

1. How to revalidate the key using Azure CLI , in our documentation the steps are not complete <https://docs.microsoft.com/en-us/azure/postgresql/howto-data-encryption-validation#from-cli>, the correct steps should be as below and we will update the documentation :

1. Need to assign identity for the server

az postgres server update --name <servername> -g <resourcegroup> --assign-identity

example :

az postgres server update --name pgservergeorep2 -g HaqelResGrp --assign-identity

```
hamza@Azure:~$ az postgres server update --name pgservergeorep2 -g HaqelResGrp --assign-identity
{
  "administratorLogin": "haqel",
  "byokEnforcement": "Enabled",
  "earliestRestoreDate": "2020-09-28T10:45:07.317000+00:00",
  "fullyQualifiedDomainName": "pgservergeorep2.postgres.database.azure.com",
  "id": "/subscriptions/2fdea10f-ac26-42ef-8147-4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Microsoft.DBforPostgreSQL/servers/pgservergeorep2",
  "identity": {
    "principalId": "56404778-76a2-4d5f-b8a9-46334036988b",
    "tenantId": "72f98867-86f1-41af-91a0-207c00110047",
    "type": "SystemAssigned"
  },
  "infrastructureEncryption": "Disabled",
  "location": "westeurope",
  "masterServerId": "/subscriptions/2fdea10f-ac26-42ef-8147-4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Microsoft.DBforPostgreSQL/servers/pgservergeorep1",
  "minimalTlsVersion": "TLSEnforcementDisabled",
  "name": "pgservergeorep2",
  "privateEndpointConnections": [],
  "publicNetworkAccess": "Enabled",
  "replicaCapacity": 0,
  "replicationRole": "Replica",
  "resourceGroup": "HaqelResGrp",
  "sku": {
    "capacity": 32,
    "family": "Gen5",
    "name": "GP_Gen5_32",
    "size": null,
    "tier": "GeneralPurpose"
  },
  "sslEnforcement": "Enabled",
  "storageProfile": {
    "backupRetentionDays": 7,
    "geoRedundantBackup": "Disabled",
    "storageAutogrow": "Enabled",
    "storageMb": 102400
  },
  "tags": null,
  "type": "Microsoft.DBforPostgreSQL/servers",
  "userVisibleState": "Ready",
  "version": "11"
}
```

2. Get the existing key:

az postgres server key list --name <servername> -g <resourcegroup>

example:

az postgres server key list --name 'pgservergeorep2' -g 'HaqelResGrp'

```
hamza@Azure:~$ az postgres server key list --name 'pgservergeorep2' -g 'HaqelResGrp'
Command group 'postgres server key' is in preview. It may be changed/removed in a future release.
[
  {
    "creationDate": "2020-09-28T10:35:22.160000+00:00",
    "id": "/subscriptions/2fdea10f-ac26-42ef-8147-4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Microsoft.DBforPostgreSQL/servers/pgservergeorep2/keys/mysqlkeyv1_mysqlkey1_7dbf9d833a004023991be0365843da48",
    "kind": "azurekeyvault",
    "location": "West Europe",
    "name": "mysqlkeyv1_mysqlkey1_7dbf9d833a004023991be0365843da48",
    "resourceGroup": "HaqelResGrp",
    "type": "Microsoft.DBforPostgreSQL/servers/keys",
    "uri": "https://mysqlkeyv1.vault.azure.net/keys/mysqlkey1/7dbf9d833a004023991be0365843da48"
  }
]
```

3. Set the policy for the new identity

az keyvault set-policy --name <keyvault> -g <resoure_group> --key-permissions get unwrapKey wrapKey --object-id <principl id of the server returned by the step 1>

example:

az keyvault set-policy --name mysqlkeyv1 -g HaqelResGrp --key-permissions get unwrapKey wrapKey --object-id 56404778-76a2-4d5f-b8a9-46334036988b

```
hamza@Azure:~$ az keyvault set-policy --name mysqlkeyv1 -g HaqelResGrp --key-permissions get unwrapKey wrapKey --object-id 56404778-76a2-4d5f-b8a9-46334036988b
{- Finished ..
  "id": "/subscriptions/2fdea10f-ac26-42ef-8147-4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Microsoft.KeyVault/vaults/mysqlkeyv1",
  "location": "westeurope",
  "name": "mysqlkeyv1",
  "properties": {
    "accessPolicies": [
      {
        "applicationId": null,
        "objectId": "e3c23f0e-e447-4c34-a4d0-167e3e95844d",
        "permissions": {
          "certificates": [
            "Get",
            "List",
            "Update",
            "Create",
            "Import",
            "Delete",
            "Recover",
            "Backup",
            "Restore",
            "ManageContacts",
            "ManageIssuers",
            "GetIssuers",
            "ListIssuers",
            "SetIssuers",
            "DeleteIssuers"
          ],
          "keys": [
            "Get",
            "List",
```

4. Set the encryption key

az postgres server key create --name <server name> -g <resoure_group> --kid <key from step2>

example :

az postgres server key create --name 'pgservergeorep2' -g 'HaqelResGrp' --kid

"<https://mysqlkeyv1.vault.azure.net/keys/mysqlenckey1/7d0f9d833a004023991be0365843da48> " "

```
hamza@Azure:~$ az postgres server key create --name 'pgservergeorep2' -g 'HaqelResGrp' --kid "https://mysqlkeyv1.vault.azure.net/keys/mysqlenckey1/7d0f9d833a004023991be0365843da48"
Command 'postgres server key' is in preview. It may be changed/removed in a future release.
{- Finished ..
  "creationDate": "2020-09-28T10:35:22.160000+00:00",
  "id": "/subscriptions/2fdea10f-ac26-42ef-8147-4b77ae49f05c/resourceGroups/HaqelResGrp/providers/Microsoft.DBforPostgreSQL/servers/pgservergeorep2/keys/mysqlkeyv1_mysqlenckey1_7d0f9d833a004023991be0365843da48",
  "kind": "azurekeyvault",
  "location": "West Europe",
  "name": "mysqlkeyv1_mysqlenckey1_7d0f9d833a004023991be0365843da48",
  "resourceGroup": "HaqelResGrp",
  "type": "Microsoft.DBforPostgreSQL/servers/keys",
  "uri": "https://mysqlkeyv1.vault.azure.net/keys/mysqlenckey1/7d0f9d833a004023991be0365843da48"
}
```

How good have you found this content?



-