Unit 5

Exercise - Manage secrets in your ARM template

Deploy Azure Key Vault

У Azure Key Vault створюю сховище ключів і додаю пароль віртуальної машини як безпечний секрет. Для цього: Створюю змінну Bash, яка зберігатиме назву сховища ключів.

```
558e34946478:/# KVNAME=panchenko-secrets$RANDOM
```

Виконую наступну команду az keyvault create, щоб створити сховище ключів:

```
558e34946478:/# az keyvault create --name $KVNAME --enabled-for-template-deployment true
We will enable rbac authorization by default in the near future, please manually specify --enable-rbac-au
thorization if you want to overwrite the default value.
Resource provider 'Microsoft.KeyVault' used by this operation is not registered. We are registering for y
ou.
Registration succeeded.
{
  "id": "/subscriptions/83e76598-1d8e-490d-92ea-741241e0e33e/resourceGroups/panchenko-serhii_group3/provi
ders/Microsoft.KeyVault/vaults/panchenko-secrets10315",
  "location": "canadacentral",
  "name": "panchenko-secrets10315",
  "properties": {
    "accessPolicies": [
      {
        "applicationId": null,
        "objectId": "2c3f12ff-35d0-4554-83dc-5f5eb0f9bff1",
        "permissions": {
          "certificates": [
```

Виконую наступну команду az keyvault secret set, щоб створити секрет у сховищі ключів.


```
558e34946478:/# az keyvault create --name $KVNAME --enabled-for-template-deployment true
We will enable rbac authorization by default in the near future, please manually specify --enable-rbac-au
thorization if you want to overwrite the default value.
Resource provider 'Microsoft.KeyVault' used by this operation is not registered. We are registering for y
ou.
Registration succeeded.
{
  "id": "/subscriptions/83e76598-1d8e-490d-92ea-741241e0e33e/resourceGroups/panchenko-serhii_group3/provi
ders/Microsoft.KeyVault/vaults/panchenko-secrets10315",
  "location": "canadacentral",
  "name": "panchenko-secrets10315",
  "properties": {
    "accessPolicies": [
      {
        "applicationId": null,
        "objectId": "2c3f12ff-35d0-4554-83dc-5f5eb0f9bff1",
        "permissions": {
          "certificates": [
            "all"
          ],
          "keys": [
```

Create the parameter file

Тут я створюю файл параметрів, який містить ім'я VM, ім'я адміністратора та посилання на пароль VM у сховищі ключів. Я можу передавати параметри до шаблонів з командного рядка. Згадайте, що файл параметрів - це альтернативний спосіб передачі параметрів до вашого ARM шаблону під час розгортання. Файл параметрів дозволяє мені отримувати доступ до секретів сховища ключів з мого шаблону.

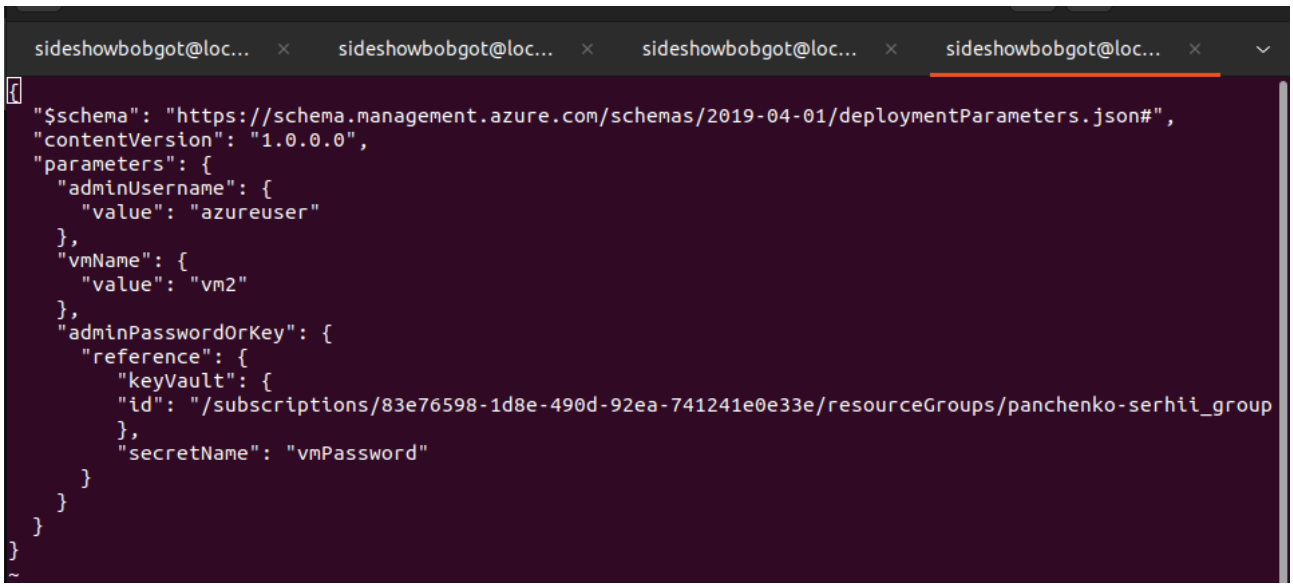
Виконую наступну команду az keyvault show, щоб вивести мій ідентифікатор сховища ключів:

```
558e34946478:/# az keyvault show --name $KVNAME --query id --output tsv
/subscriptions/83e76598-1d8e-490d-92ea-741241e0e33e/resourceGroups/panchenko-serhii_group3/providers/Micr
osoft.KeyVault/vaults/panchenko-secrets10315
558e34946478:/#
```

Додаю ці вміст до azuredeploy.parameters.json:

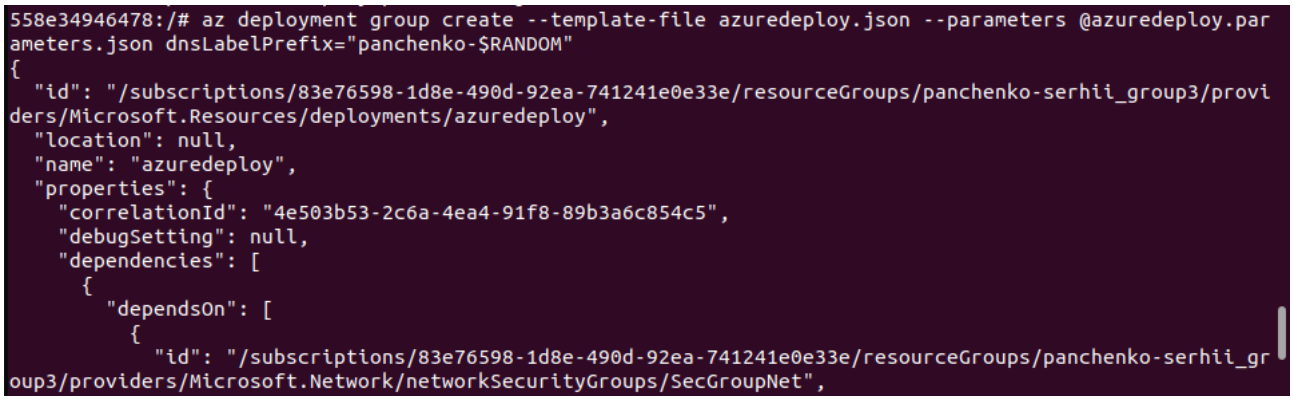
```
sideshowbobgot@loc...  sideshowbobgot@loc...  sideshowbobgot@loc...  sideshowbobgot@loc...
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "adminUsername": {
      "value": "azureuser"
    },
    "vmName": {
      "value": "vm2"
    },
    "adminPasswordOrKey": {
      "reference": {
         "keyVault": {
         "id": ""
         },
         "secretName": "vmPassword"
      }
    }
  }
}
~
```

Замінюю значення id (порожній рядок) на значення, яке я скопіював на попередньому кроці. Потім зберігаю файл.



Deploy a Linux VM

Тут я розгортаю той самий шаблон ARM, що я розгортав у попередньому завданні. Цього разу я надаю файл параметрів, який посилається на пароль VM у сховищі ключів. Виконую наступну команду az deployment group create, щоб розгорнути шаблон:



Як я робив у попередньому завданні, перевіряю, що VM створено і доступно через SSH. Для стислості цього разу я пропущу деякі проміжні кроки.

Виконую наступне, щоб підключитися до своєї VM через SSH:

```
sideshowbobgot@localhost:~/university/Infrastracture/Lab1/7_ManageComplexCloud$ $(az deployment group sho
w --name azuredeploy -g panchenko-serhii_group3 --query properties.outputs.sshCommand.value --output tsv)
The authenticity of host 'panchenko-10031.canadacentral.cloudapp.azure.com (52.233.29.67)' can't be estab
lished.
ED25519 key fingerprint is SHA256:Vy6DbI9BfN1IYS5xlB30LERZBhSKGPsxu++61Ko+rNI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'panchenko-10031.canadacentral.cloudapp.azure.com' (ED25519) to the list of kn
own hosts.
azureuser@panchenko-10031.canadacentral.cloudapp.azure.com's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1057-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Sun Mar  3 18:05:01 UTC 2024

  System load:  0.17              Processes:             119
  Usage of /:   5.3% of 28.89GB   Users logged in:       0
  Memory usage: 3%                IPv4 address for eth0: 10.1.0.4
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@vm2:~$
```

З мого SSH з'єднання з VM виконую команду hostname, щоб вивести ім'я хоста VM:

```
azureuser@vm2:~$ hostname
vm2
azureuser@vm2:~$
```

Виконую exit, щоб залишити мою SSH сесію.

```
azureuser@vm2:~$ exit
logout
Connection to panchenko-10031.canadacentral.cloudapp.azure.com closed.
sideshowbobgot@localhost:~/university/Infrastracture/Lab1/7_ManageComplexCloud$
```