AZ-104 Azure RBAC - LAB Using service Principal Identity to List AD Roles

In this hands-on lab, you are tasked with gathering the role definitions and role assignments for your organization.

You do not have access to the portal, so you must collect this information via SSH connection, by using a Linux VM and a service principal. Once you have gained access to the Azure subscription, use the Azure CLI to collect the required information, and output to a file so you can email it to your manager.

Solution

Log in to the virtual machine using the credentials provided:

```
ssh cloud_user@<PUBLIC_IP_ADDRESS>
```

Log in to Azure using the Service Principal

1. Once connected to the lab VM, perform the `az login` command with the `--service-principal` flag to login to the Azure account:

```
az login --service-principal \
-u "<CLIENT_ID>" \
-p "<CLIENT_SECRET>" \
--tenant "<TENANT_ID>"
```

> **NOTE:** To get your own `Tenant ID`, search for `Tenant properties` in the Azure portal. The value will be under the `Tenant ID` field.

If you experience an error regarding invalid arguments, please see the Additional Information section for the details of a fix.

List the Role Definitions and Role Assignments

1. List the role definitions:

```
az role definition list
```

2. Output the list to a file named `roleinfo.json`:

```
az role definition list > roleinfo.json
```

3. List the role assignments:

```
az role assignment list --all
```

4. Append the list to the `roleinfo.json` file:

```
az role assignment list --all >> roleinfo.json
```

5. Verify that the file was created successfully:

```
vi roleinfo.json
```

```
cloud_user@lab-VM:~$ az login --service-principal \
> -u "4f5230cd-58fe-45d3-89bc-a14cc732d64a" \
> -p "w5cl28fSpGDA88Qy7uC.8T~t~so~f-~H-3" \
> --tenant "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d"
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
    "id": "0f39574d-d756-48cf-b622-0e27a6943bd2",
    "isDefault": true,
    "managedByTenants": [],
    "name": "P3-Real Hands-On Labs",
    "state": "Enabled",
    "tenantId": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
    "user": {
      "name": "4f5230cd-58fe-45d3-89bc-a14cc732d64a",
      "type": "servicePrincipal"
    }
  }
]
cloud_user@lab-VM:~$
```

Revision #2
Created 20 February 2024 00:12:49 by Cesar Gzz
Updated 20 February 2024 00:43:57 by Cesar Gzz