**Using Service Principal Identity to List AD Roles**

**Introduction**

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

1. Output the list to a file named roleinfo.json:

az role definition list > roleinfo.json

1. List the role assignments:

az role assignment list --all

1. Append the list to the roleinfo.json file:

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

1. Verify that the file was created successfully:

vi roleinfo.json