# Lab 8-1 – Checkpoint

# Cloud Administration

# Total Points: 8

# Learning Outcome:

1. Implement system administration tasks on cloud platform

# Objectives:

* Develop an understanding of how to use Azure to manage virtual machines and networks.
* Automate virtual resources on Azure using powershell

**Instructions:**

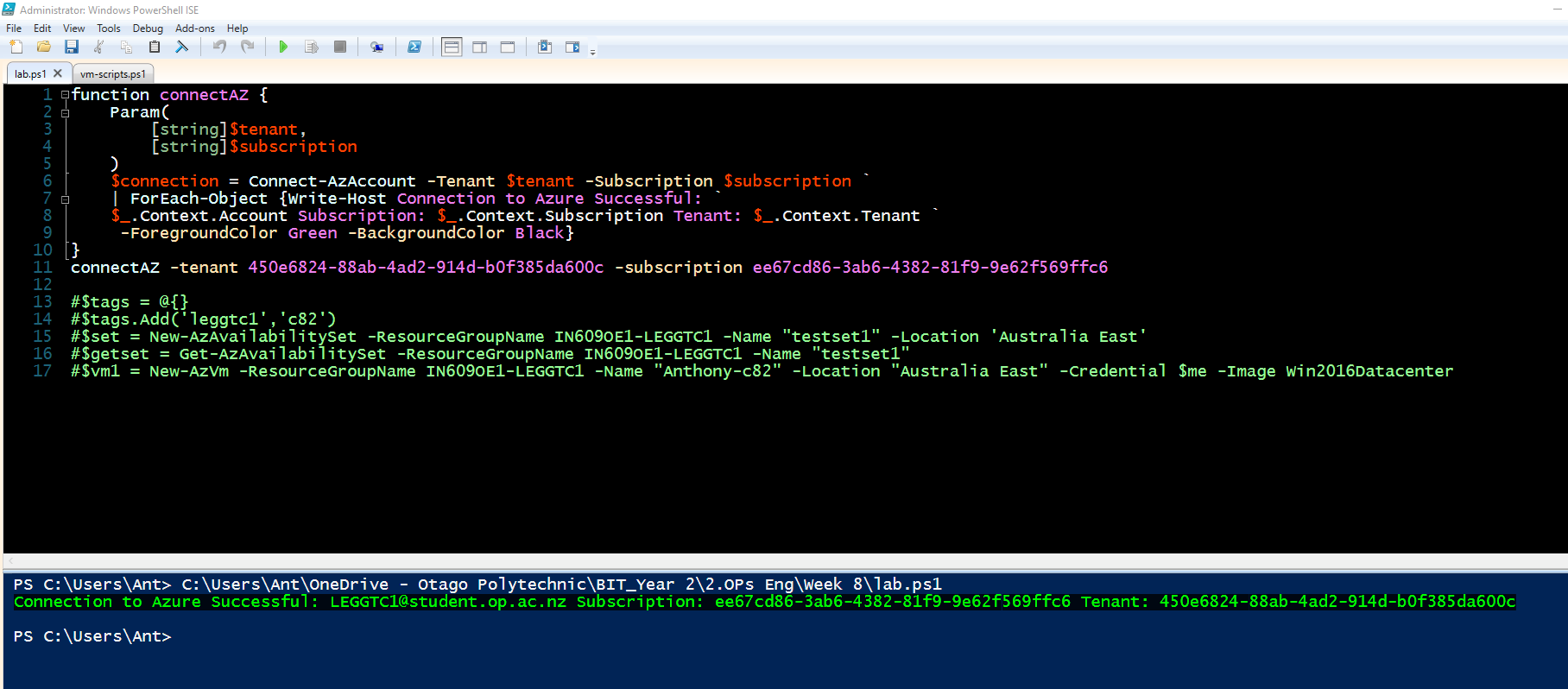
* Solve the following tasks based on the **integrated help** (get-help), **lecture slides, your submitted lab works** and PowerShell/Azure **online reference**.
* You need to complete the tasks within the allocated time (8am-950am)

Submit: Please submit your answers on teams->yoursection->checkpoint by inserting as attachment.



Answer the following questions:

1. Create a powershell script to connect to OP’s Azure subscription from your windows powersell ISE. The script should print information about the subscription it connects to. Submit the screenshot of the powershell ISE that shows the script as well as the execution output **(2 points)**



1. Create a vm on Azure with the following details:

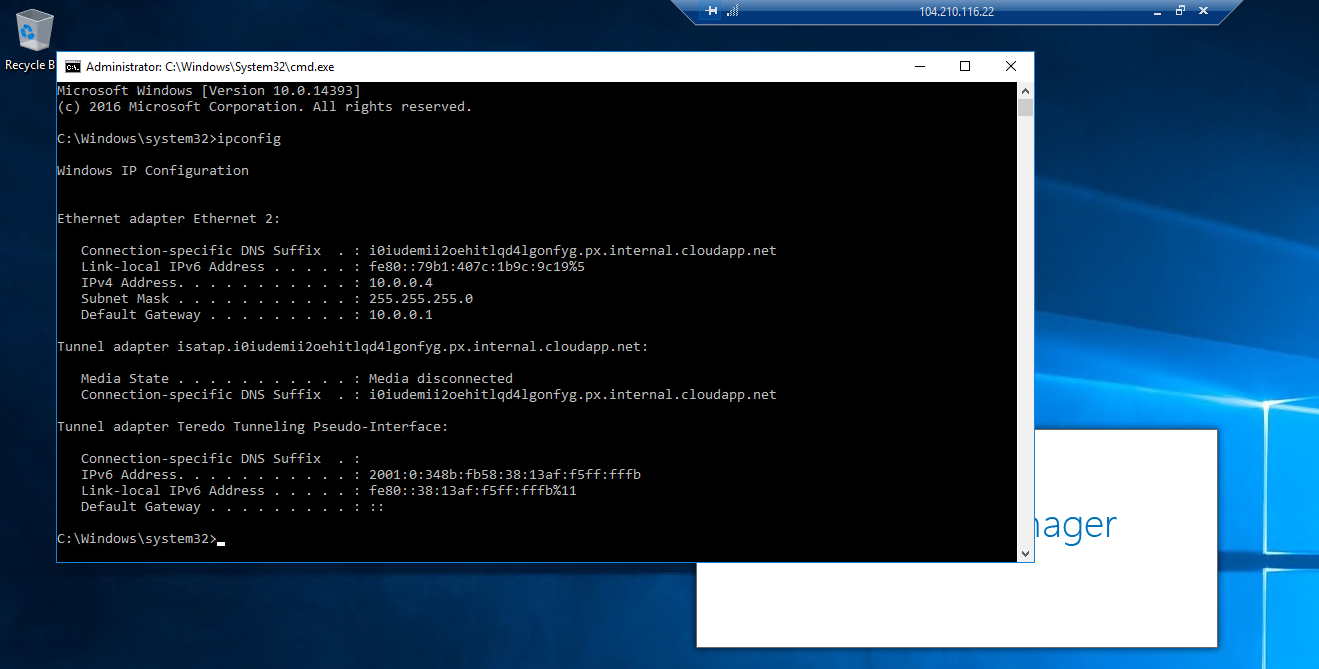
vmname= <yourfirstname>c82

vmimage=win2016Datacenter

publicip=<yourname>-publicip

the vm should have options to connect through ssh and rdp.

Connect the vm with rdp and print the screenshot below. **(2 points)**



1. Suppose you are creating an application deployment that connects to a number of database servers. You already did the following:

Created a virtual network vnet101 (10.2.20.0/16)

Created subnet1 (10.2.30.0/24) for application

Created subnet2 (10.2.40.0/24) for database servers

Created network security group *(appsec*) and

connected the apps vm and the database vms to the *appsec* security groups.

However, when you try to *ssh* to the vms you are unable to connect even though your username and passwords are correct.

What can you do to solve the connectivity issue? **(2 points)**

The network security group needs to be configured to allow ssh traffic. Port forwarding needs to be configured on the virtual network so the traffic external to the network can be permitted. Traffic can then reach the target subnet. Also check the credentials are applied to the security group.

1. In the above scenario, since your application will be connecting to multiple database servers your manager asked you to create a separate application security group for all the database servers. Is there any advantage of creating this additional security group for database servers in restricting traffic between the application and database servers? Please justify your answer. **(2 points)**

The application security group can be applied to all servers within a single security group and have differing traffic rules applied as needed on an individual server basis. Configuring traffic rules within a single group make administration and debugging much easier. Mistakes are much more likely, when creating separate security groups for each server, in the same organisation. There may only be one or two variations in each server’s port configurations, so it makes more sense to create these security rules within the same security group.