**########## Challenge 1 ############**

1) Deploy the stack

- verify that the stack has completed successfully

2) Navigate to Fleet Manager and verify that the ec2 instance just created isn't yet managed.

3) Go to the vpc and create an endpoint by selecting "Endpoints" on the left hand menu

4) we'll create the ssm endpoint first

- name the endpoint `ssm-endpoint`

- Make sure that AWS Services is selected

- in the search box, search for "ssm". Make sure you choose the correct one, it should be named "com.amazonaws.{region}.ssm"

- click the radio button next to it

- select the correct vpc (the one created by the stack) in the dropdown menu

- using the check box, select both of the subnets available, and then select the subnet id from the dropdown menu

- select IPv4 for IP Address Type

- For Security Groups, choose the one named "endpoint-sg"

- leave the policy blank

- click "create endpoint" and then wait for it to be in the "available status"

5) Reboot the EC2 instance and wait about 5 min.

6) Navigate to Fleet Manager and confirm that the ec2 instance is now showing up as being managed.

Note: it may take 5-10 minutes for this to reflect in Fleet Manager

7) Find the "Run Command" console under Systems Manager. Click the orange Run Command button. In the search box, type in `Shell` and hit enter. Select the radio button for the one named `AWS-RunShellScript`.

8) Scroll down and in the Command Parameters text box, type the following `hostname`. Under target selection, click Choose Instances manually. Select the `Week-03 Instance` instance.

9) Under output options, de-select "Enable an S3 bucket". Then scroll down to the bottom and hit "Run". You'll notice that this is "In Progress" but delayed. This is because while the SSM Endpoint is active,

it can't communicate without the "ec2-messages" endpoint. Let's configure that.

10) Let's cancel this command before we get the endpoint set up. Hit Cancel Command and then confirm it.

10) Repeat step 4 but now do it for "ec2messages".

11) Repeat steps 8 and 9. The command should succeed now that we've got the "ec2\_messages" enabled.

12) Move back to the EC2 Instances screen and attempt to connect to the Instance. Notice that the Session Manager says it's unable to connect. Why is this? We've set up the ec2\_messages and the ssm endpoints.

While this can allow Systems Manager to execute Run Commands and mange the instance, the Session Manager required the "ssm-messages" endpoint to facilitate connection. Let's set up that endpoint.

13) Repeat steps 8 and 9, but use the "ssm-messages" instead.

11) Reboot the EC2 instance and wait about 5 min.

12) Attempt to connect to the EC2 instance by using Session Manager

**########## Challenge 2 ############**

1) Connect to the instance and run the `aws s3 ls` command.

2) The command will fail. Why?

3) Navigate to the subnet that the EC2 instance is attached to

- Can view this under "Details" and "Subnet ID"

4) Select the subnet and then view the Route Table it's attached to.

5) Note the routes. There is no route from this subnet to S3.

6) Let's create another Endpoint. Navigate to VPC -> Endpoints.

7) Click Create Endpoint

8) Name it `s3-endpoint`

9) Under Services, search for `s3`

10) Choose the Gateway type of Endpoint

11) Choose the VPC for this week, and this time instead of subnets, we'll be looking at Route Tables. Make sure you select both Route Tables. Leave the Policy as full access for now. Add any tags and then click Create Endpoint.

12) Now navigate back to the Route Tables for the subnets and look at the Routes. Notice the difference? The Endpoint created a route in the Route Table that allows traffic from this VPC to the Gateway Endpoint.

13) Go back to the EC2 Instances, and log-in to the EC2 Instance. Run the `aws s3 ls` command again. What happens? A different error! Progress! Now we can presume that we're connected, but we're having permissions errors. How can we fix this? There's no bucket policy that needs to be evaluated because we're simply trying to list the buckets.

14) Go back to the EC2 Instances screen and select the EC2 Instance that we connected to. Click on "Security" and click on the IAM Role being used.

15) Click on "Add Permissions" and choose Attach Policy. Search for `S3Read`. Click the check box and then "Add Policy". Verify that the policy was added to the Role.

16) Connect back to the EC2 Instance if you've left it already. Now try the same command: `aws s3 ls` again. If everything was set up correctly, you should get an listing of the S3 Buckets in the account. If it doesn't work immediately, give it about a minute and it should work.

**########## Challenge 3 ############**

1) Navigate to the week-03-vpc and select the VPC

2) Select "Flow Logs" and then click "Create flow log"

3) Choose a name like "week-03-flow-logs"

4) Under Maximum aggregation interval, choose 1 minute

5) For the Destination log group, choose the log group named "vpc-log-group"

6) For the IAM Role, make sure you choose the vpc-flow-logs-role

7) You can add some tags if you like, but it's not required.

8) Click "Create flow log" and the logs will be created.

9) You'll need to wait a few minutes, as it gathers logs every minute. However, connect to the instance using Session Manager to generate some logs

10) Navigate to CloudWatch, on the left hand menu, Under Logs, click on Log Groups. Click on the created log group named "vpc-flow-logs"

11) Select any of the log streams and view your logs.

**########## Reachability Analyzer ############**

If you're having issues completing the labs, please utilize the VPC Reachability Analyzer. This will test the network connectivity between two points (in this case, between the instance that was created and the endpoint we created). This is a good way of determining if you IAM permission issues or network issues.

1) Search for Reachability Analyzer in the search bar.

2) Click "Create and analyze path"

3) Give it a name like "ec2 instance to ssm-endpoint"

4) Under Path Source, chose the source type. In this case, it will be Instances.

5) Under Source, choose the Instance ID of the EC2 Instance you want to check.

6) Chose "VPC Endpoints" for Destination Source and the VPC Endpoint that you wish to check. In this case, let's choose the ssmmessages endpoint.

7) Scroll down and click "Create and analyze path"

8) Give it a few minutes and it will determine if there is connectivity between the two points. It will analyze any NACLs and Security Groups that will prevent or allow access.

9) After it's complete, it will let you know if it's Reachable or Not Reachable. If it's not reachable, it will tell you why in the Path Details.

**########## Clean Up #################**

1) Make sure to delete all of the endpoints that have been created.

- This may take a few minutes.

2) Delete the vpc-flow-logs group

2) After the endpoints are deleted, make sure to delete the stack.