AWS Security Lab Guide

Setting up VPC

1. Select VPC from the services screen
2. On the VPC screen, from the menu, select Your VPC
3. Click on create VPC
4. Give the name for the VPC
5. Give the CIDR block as 10.0.0.0/16
6. Select Subnets from the menu
7. Create two subnets
    a. Name one subnet as Public Subnet, CIDR 10.0.0.0/24
    b. Name another as Private Subnet, CIDR 10.0.1.0/24
8. Select Internet Gateway from menu and click on Create Internet Gateway
9. Attach Gateway to the VPC
10. Selecting Route Table from the Menu
11. Click on Create Route Table
12. Give the Route Table the name 'Public Route'
13. After the route table is created, select the route table and check the bottom part. Select the Routes tab
14. Add the following entry to the route table
    a. 0.0.0.0/0   InternetGateway
15. Our VPC is ready

Connecting to VPC through VPN Gateway

1. Have the public/static IP address of your VPN device ready
2. In the VPC screen, select Customer Gateway from the menu on the left side
3. Input the name for this Gateway and the IP address of the VPN device
4. Select Virtual Private Gateway from the menu and click on create Virtual Private Gateway
5. Click on Site-to-Site from the menu and click on Create VPN Connection
6. If everything is setup right, the link become active soon.
7. On this screen, click on "Download Configuration File'
8. Select your VPN device from the drop down list
9. Download the configuration file
10. Provide the downloaded configuration file to the Network Administrator and ask him/her to configure the VPN
11. In the route table of your VPC, add a route to VPN connection. The target IP range will be the range of your datacenter
12. In your data center router, add a route to the VPN router for all traffic going to the VPC IP addresses

Enabling VPC FlowLogs

1. Create a Log Group in CloudWatch
2. In the VPC screen, select the VPC and in actions, select 'Create Flow Logs'
3. In Filter, select 'All'

4. Select the Log Group created earlier
5. Select the appropriate role (Check with instructor)
6. Click on Create to create the Flow Log

AWS Inspector on Windows Instances

1. To install the agent on a Windows-based EC2 instance
2. On the AWS EC2 Windows Instance
3. Download the following .exe file:
4. https://inspector-agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe
5. Open a command prompt window (with administrative permissions), navigate to the location where you saved the downloaded AWSAgentInstall.exe, and run the .exe file to install the agent.
6. Run services.msc and check if AWS Agent Service and AWS Agent Service Updater service are running

AWS Inspector

7. Under services search and start AWS Inspector
8. Select both Network Assessment and Host Assessments and then click Run Once

To create an assessment target

9. In the navigation pane, choose Assessment Targets, and then choose Create.
10. For Name, enter a name for your assessment target.
11. *Do one of the following:*
12. To include all EC2 instances in this AWS account and Region in this assessment target, select the All instances check box.
13. To choose the EC2 instances that you want to include in this assessment target, for Use Tags, enter the tag key names and key-value pairs.

Now create an assessment template

14. In the navigation pane, choose Assessment Templates, and then choose Create
15. For Name, enter a name for your assessment template
16. For Target name, choose an assessment target to analyze
17. For Rules packages, choose one or more rules packages to include in your assessment template.
18. For Duration, specify the duration for your assessment template.

AWS Config

1. You can use the AWS Management Console to get started with AWS Config to do the following:
2. Specify the resource types you want AWS Config to record.
3. Set up Amazon SNS to notify you of configuration changes.
4. Specify an Amazon S3 bucket to receive configuration information.
5. Add AWS Config managed rules to evaluate the resource types.
6. The AWS Config getting started page provides an overview of the service.
7. Choose Get Started Now.
8. On the Settings page, for Resource types to record, specify all the resource types you want AWS Config to record. These resource types are AWS resources or third-party resources or custom resources.
9. All resources – AWS Config records all supported resources with the following options:
10. Record all resources supported in this region – AWS Config records configuration changes for supported AWS resource types as well as third-party resource types registered in AWS CloudFormation registry. AWS Config automatically starts recording new supported AWS resource types. It also automatically starts recording third-party resource types that are managed (i.e. created/updated/deleted) through AWS CloudFormation.
11. For Amazon S3 Bucket, choose the Amazon S3 bucket to which AWS Config sends configuration history and configuration snapshot files:
12. Choose a bucket from your account – For Bucket Name, choose your preferred bucket.
13. For Amazon SNS Topic, choose whether AWS Config streams information by selecting the Stream configuration changes and notifications to an Amazon SNS topic. AWS Config sends notifications such as configuration history delivery, configuration snapshot delivery, and compliance.
14. Choose a topic from your account – For Topic Name, select your preferred topic.
15. For AWS Config role, choose the IAM role that grants AWS Config permission to record configuration information and send this information to Amazon S3 and Amazon SNS:

Installing and running a log agent for Linux

1. Start a Linux Instance
2. Attach the correct role to the instance (The role must have the permission to write to CloudWatch Logs)
3. sudo yum update -y
4. sudo yum install -y awslogs
5. By default, the /etc/awslogs/awscli.conf points to the us-east-1 region. To push your logs to a different region, edit the awscli.conf file and specify that region.
6. sudo service awslogs start
7. Check CloudWatch to see if this appears in the CloudWatch Logs

Using KMS Key

1. Login into Amazon Linux2 instance
2. Setup credentials
3. aws kms generate-data-key –key-id alias/spanlabs –key-spec AES_256 –region ap-northeast-1
4. Save the plain text and the Cipher blob
5. cat datakey_plaintext_base64.txt
6. Decode Base64
7. cat <cipher_file> | base64 --decode >./<filename>
8. aws kms decrypt --ciphertext-blob fileb://<filepath> --region us-east-1
9. Copy the decrypted key and check against the initial plain text key

Parameter Store

1. Create a parameter store
2. aws ssm get-parameter <parameter name>

Session Tokens

1. Create one IAM user with S3 access permissions
2. Get a temporary session token, ‘aws sts get-session-token’
3. Create a new profile named [Test] in .aws/credentials
4. Deactivate the original key and test s3 ls. It should fail
5. Access S3 using session token   aws s3 ls –profile Test

Patching

1. Create Amazon EC2 Role for patching with two policies attached
2. AmazonEC2RoleForSSM
3. AmazonSSMFullAccess
4. Assign Roles to the EC2 Instances
5. Configure Tags to ensure patching in groups
6. In SSM, select ‘Patch Baseline’
7. Set new baseline as default if not already set
8. Create Maintenance Window

9. Register the targets
10. Register Task
11. Apply Patch Baseline for Windows
12. Select AWS Run Patch Baseline for Command Document
13. In Role Select SSMManagedInstanceProfile role

Optional (To be done if there is time)

Simple Notification Service

1. Select SNS from services
2. Click on Topics
3. Click Create Topic
4. Give me a name to the topic
5. After topic is created scroll down till you see the ‘Subscription’ button
6. Click of Subscription
7. Select email from the drop down
8. Provide your email address
9. Go to your email. You would have got a mail with confirmation link
10. Click on the confirmation link to confirm
11. Refresh the AWS screen. You should now see the screen showing subscription as ‘Confirmed’

Lambda

1. Select Lambda services from services
2. Click on create function
3. Give a name to the function
4. Select ‘Python 3.8’ in the run time
5. Expand the role area and select the appropriate role (check with the instructor on this)
6. Create the function
7. After function is created, you will see the code. Add a line to the code
    a. print(event)
8. Setup a test template and test the code
9. Check the CloudWatch Logs for the execution of this function