Advanced Cloud Security and Applied DevSecOps Pre-Class Setup and Required Lab

Required setup to ensure you have the best classroom experience

April 3, 2019

Is this pre-work really required?

ABSOLUTELY!!! Security and cloud practitioners have a wide range of skills and specialties. This is an advanced training that requires both a minimum skills set and pre-class setup work to support the class labs. *It is your responsibility as a student to ensure you have the right experience and have configured your training environment.*

If you find this assessment and setup too difficult we highly recommend you attend a **Cloud Security Alliance CCSK Plus training class** (including the Cloud Security Hands-On class we offer at Black Hat) and spend a few months working hands-on in cloud or take additional platform training offered by your cloud provider or a third party. Completing the CCSK alone will not guarantee you have the skills for the best Advanced training experience.

Background and Course Objective

The Securosis Advanced Cloud Security and Applied DevSecOps training is a fast-paced, lab-centric experience that covers a wide range of cloud security and DevOps principles. The objective of the course is to level-up both cloud and security professionals who posses existing cloud security skills and provide a foundation for advanced practice.

By the time you finish this training you should have the ability to start implementing cloud-native enterprise-scale cloud security and DevSecOps programs.

Consider this course an accelerator. *There is no way 2-3 days of training can substitute for months and years of practical experience*, but our class will introduce the fundamental skills needed for advanced practice and show a vision of how modern cloud security and DevSecOps programs functions. It is then up to individual students to build on this baseline in their individual areas of expertise, from architecture to automation to incident response.

Pre-Class Setup and Assessment Expectations

We have merged our pre-class setup and an assessment lab into a single document. If you can complete all the setup items, which includes specific challenges that test your hands-on Amazon Web Services skills, you are well prepared to take the class. There are four levels of achievement which you can use to determine if you need additional practice before coming to class:

This assumes you complete the required setup within an hour or less. If it takes many hours or days you should self-assess as being one level lower:

- *Stage 0 (unable to complete the first requirements):* Please take the CCSK Plus and gain additional hands-on cloud practice or obtain equivalent experience. You will struggle to complete the labs and your required training environment is not properly configured.
- *Stage 1:* You will be able to complete 30% or more of the labs and understand all the lecture, but will likely struggle and may need to do additional work over breaks and evenings if you want to keep up. Your environment meets the minimum configuration to participate.
- *Stage 2:* You should be able to complete around 60% of the labs in the allotted classroom time but may drop off in areas. You will be able to obtain the knowledge but will likely need to finish some of the labs after training.
- *Stage 3:* You should be able to complete 90% of the labs, and should need to spend minimal time on the core labs outside the classroom. You may still struggle a bit outside your areas of experience (e.g. if you don't code, those labs will be more difficult).

Why only Amazon Web Services?

Although we discuss all three hyper scale cloud platforms (AWS/Azure/GCP) the majority of the labs are performed in AWS. This is for three reasons:

- Amazon is the most commonly-used cloud provider.
- There is too much material to replicate it across multiple providers.
  - The principles will apply across all providers, even if you only implement them in one.
  - However, we do have an optional Azure lab we will deliver during the lunch break. See the end of this document for more information.
- Nearly everything we do is in the free tier for a new account; the average AWS charges are under $10 and it is easy to shut everything down after class to prevent further charges.

If you are experienced on Azure or GCP you should still get a lot out of the training. *Most of the DevSecOps content, in particular, translates directly to any of the big 3 cloud providers.*

Why so few screenshots?

This document combines both setup and assessment to help students determine if they are ready for the advanced material and the pace of training. This is not meant to be instructional; don't worry, we have plenty of screenshots and video in the actual training.

Why can't I use a corporate/dev/organization's AWS account? Why don't you provide me an account?

Our labs cover the entirety of configuring a secure, enterprise-scale AWS baseline. This includes using multiple accounts under AWS Organizations configured in accordance with best practices. There is no way to do this unless you have full administrative privileges for your AWS Organization master. If you do have those privileges, you know why you don't want to be messing with your real accounts for a training class.

Since we require you complete a pre-class lab that includes an organizations master we can't effectively provide prospective students with accounts. Also, a large percentage of students keep these accounts for practice and experimentation after the training is complete, so the best option is to have all students create their own accounts. Especially since the cost is well below what you might pay for a single breakfast in Las Vegas.

What you will do

This setup and lab includes three stages:

1. Basic Setup (*completing this is the minimum requirement to attend training)*
   - Create a new AWS account and set it to be an Organizations master
   - Create a required IAM role
   - Run a CloudFormation Stack to create a new VPC
   - Fix the configuration to connect to a public instance
   - Run a script in the home directory. This will send us a message giving us a record that you completed Stage 1
2. Fix the VPC
   - Repair the configuration.
   - Connect to a second instance in a private subnet.
   - Use the AWS metadata service to retrieve a token
   - Run a script in the public instance to send us a message with the token
3. Add NAT to the private subnet and use the command line tools
   - Fix the private subnet so it can reach the Internet via NAT
   - Connect to the private instance again
   - Use the AWS command line or metadata service to retrieve a token
   - Run a script that sends us a message that you completed Stage 3
4. *Optional setup for Azure*
   - This year we have an optional Azure lab we will deliver over one of the lunch breaks. You'll just need to create an Azure account ahead of time and we will take it from there.

Pre-class Lab

If you are experienced in AWS this should take less than an hour. Highly experienced students can complete all steps in 15-20 minutes. If it takes more than a few hours to complete this lab you will want to work on your skills. You can also contact us at info@securosis.com if you get stuck or feel there is a bug in the lab.

Minimum system requirements:

- The same laptop you will be bringing to class
- Any operating system
- Permissions to connect to arbitrary WiFi networks
- The ability to make SSH connections to arbitrary destinations (AWS)
- The ability to make connections without using a VPN. Many students who have to use a corporate VPN backhaul find that their traffic is blocked and IP addresses change in ways that impede the labs

Additional hardware for class:

- This training uses only digital documentation. You can email your instructor a few days before class if you would like early access to print yourself.
- ***We highly encourage all students who can to bring a tablet to read the lab PDFs***

Stage 1

In this stage you will create an account for training, set it to be your AWS Organizations master, run a CloudFormation template that creates a VPC for this lab, and connect to an instance in that VPC. You will finish by running a script that sends us a message (using SQS) that you have completed stage 1.

1. Create a new AWS account

Before creating your account you will need access to 3 unique email addresses! AWS requires a unique email address for every account, and we will need 3 accounts for our labs. Remember, we are covering techniques for securing enterprise-scale deployments which always involve multiple accounts.

The easiest way to do this is to create a new Google Mail account at *https://www.google.com/gmail/about/*. Gmail accounts support "*name+variable@gmail.com*", which means instead of having multiple email accounts you simply use your gmail address and add a + sign and additional characters. These emails will automatically appear in your gmail account.

For example, if I owned *aaa@gmail.com* I could use *aaa+awsaccount1@gmail.com*, *aaa+awsaccount2@gmail.com* and so on. All of those messages will still deliver to *aaa@gmail.com*.

Do not use this for enterprise accounts! We will explain why in class

Then go to ***https://portal.aws.amazon.com/billing/signup?#/start*** to create your new AWS account. You will be required to have your credit card and your phone nearby.

2. Create the required IAM role

We will use this specific IAM role for multiple labs. In class you will also need to create it in each of your additional accounts.

- Create a new IAM role
- Name it Dev (case matters)
- Give it that AdministratorAccess AWS managed policy

3. Create a Key Pair (host key) and configure it for your OS

Since this is a new account you will need a new SSH key pair (which is sometimes referred to as the host key in AWS documentation) to connect to Linux instances. If we've already lost you then we highly suggest you consider the CCSK Plus training class instead.

- Make sure you are in the us-west-2 (Oregon) region. *The lab will fail if you don't!*
- Create a key pair in the EC2 console and download it
  - For Mac/Linux:
    - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#having-ec2-create-your-key-pair
  - For Windows:
    - You have 3 options. PuTTY is the most common, but newer Windows 10 systems may have SSH installed:
      - Choose from this table- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html

3. Run the CloudFormation stack

- Go into the CloudFormation console
- Make sure you are in the us-west-2 (Oregon) region. *The lab will fail if you don't!*
- Create a stack
  - Choose to specify an S3 template URL
  - Use the following URL: https://advanced-cloudsec.s3.amazonaws.com/preclass_lab.template
  - Enter the name of your host key in the labelled field. ***Do not include the .pem extension, use the exact name as it appears in the EC2 console under Key Pairs.***
- Wait for it to finish, it will take a few minutes
  - Refresh every few minutes if it seems to stall; the AWS console rarely refreshes like you would expect.

The two most common errors at this point are using the wrong IAM role name (Dev), or being in the wrong region.

4. Connect to the public instance

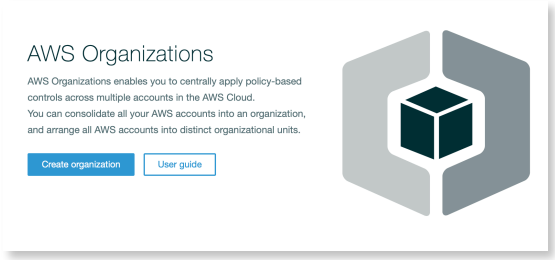
The CloudFormation template creates a VPC with public and private subnets, with instances in each subnet.

- Identify the public instance
- Try to connect over SSH

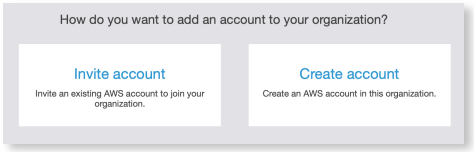
- If you don't fix something pretty basic related to your ability to connect to things over the network, it won't work.
- Do not disconnect as you complete step 5:

5. Set up your account for AWS Organizations

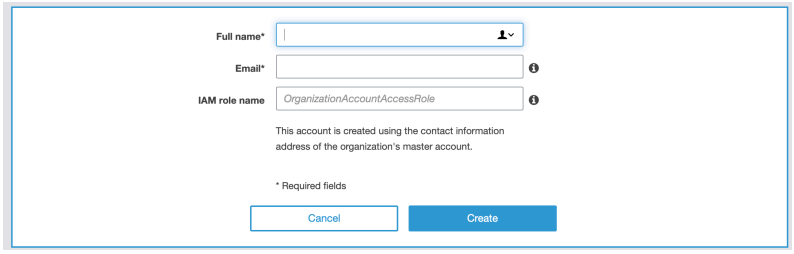
- In the console, go to Organizations and configure your account to be the org master



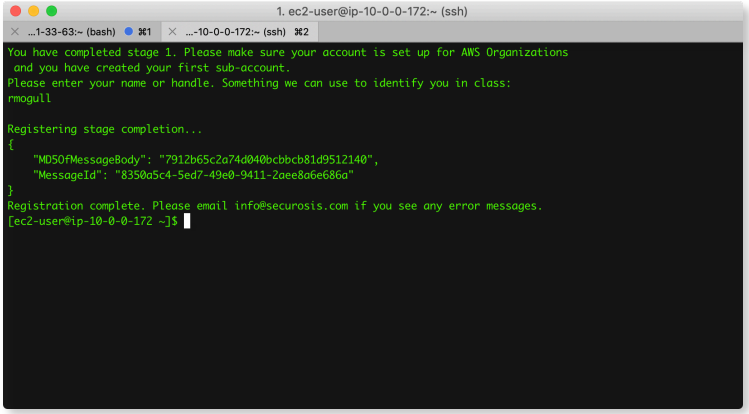
- Create a second account:
  - WARNING! You will likely have to wait an hour to create the account after activating Organizations. You can come back to this section later.



  - Name it "SharedServices"
  - Use the "name+management@gmail.com" or an equivalent unique email address
  - Leave the IAM role as-is



  - Go back to your terminal session
  - Run the following command line and enter your name **without spaces** (or handle, anything we can use to verify you in the classroom)
    - `stage1.sh`



Stage 2

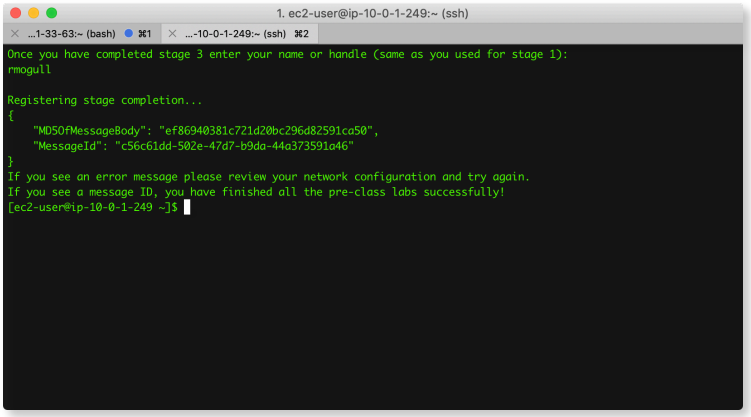
Now that you are logged into your public instance it's time to connect to the instance in your private subnet. This stage is pretty quick and all about making sure you have some basic Unix skills.

- While still logged into the public instance, ssh into the private instance.
- The key is pre-loaded in the public instance home directory.
  - The username is `ec2-user`
- Once logged into the private instance, use either the aws metadata service for aws command line tools to *retrieve the secret word* in the user-data field.
  - Yes, there are other ways to get this but those don't ensure you have the skills you'll need for class.
  - *The AWS CLI won't work until you fix something else* that you will need in stage 3, but the metadata service will work just fine.
- Then close your connection to the private instance, or open a second connection to the public instance, and enter the following command:
  - `stage2.sh`

Stage 3

At this point you have set up your account, set up the required IAM role, deployed the CloudFormation template, logged into the public server, logged into the private server, and retrieved a secret (barely) token using the metadata service or the command line. For stage 3:

- Make sure you are logged into the Private instance.
- The subnet's connectivity to the Internet via NAT is broken. Fix it.
- Run the following command from the private instance:
  - `stage3.sh`
  - That command will stall or error out if you did not properly fix the network.



Cleanup

Everything was created using the CloudFormation template. You can delete all the running resources and the VPC by deleting the stack from the CloudFormation console.

Azure Prep

We will hold an optional Azure lab over lunch on the second day of training. This is more about seeing the differences in the platforms and covering a few fundamentals. If you want to participate, set up a personal Azure account before the training.

You can also (mostly) participate if you have the tenant-level Reader role, or Owner at a subscription level. Exactly which parts you can complete will vary if you don't own the tenant (and pay as you go is fine, you don't need an EA account) but you will be able to walk through everything even if you don't implement changes.

If you own your Azure AD tenant you can also optionally participate in an additional federated identity lab.

Conclusion and Additional Prep

As a reminder, you can participate in Advanced Cloud Security and Applied DevSecOps if you successfully completed stage 1. However, if you did not complete stages 2 or 3 you will likely struggle through more of the material and have to spend time on your own to complete the labs due to the rapid pace of training.

If you completed stage 2 you should be in solid shape to finish most labs in the allotted time. If you completed stage 3 you are well prepared to finish nearly all the labs during class. That said, not everyone has the same skills or focus areas. The following skills are recommended to get the most out of class, but even without them, and even without finishing all the labs, everyone is able to pick up the principles:

- Familiarity with the AWS console and the ability to create VPCs, autoscaling groups, and load balancers.
- A basic understanding to AWS IAM, including policies, roles, and users.
- Experience with basic Linux commands (ssh, file management, permissions, running Linux applications and general command lines).
- Basic python programming (or equivalent in another language).
- A solid understanding of enterprise security principles.

Finally, students can take home all the labs to review, practice, or complete material on their own.

If you have any questions or issues please email info@securosis.com and we will see you in class!