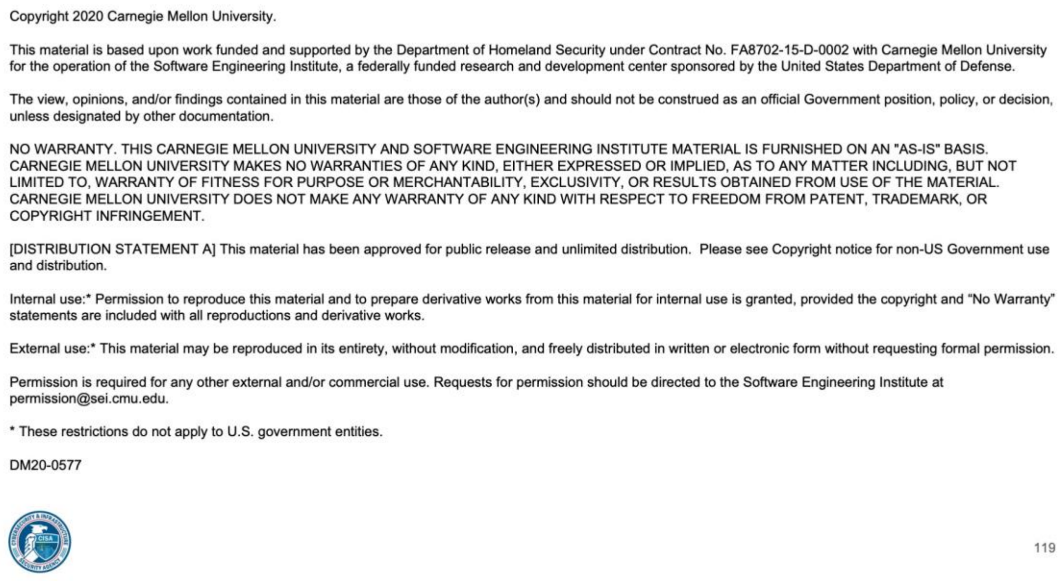
Review of Monitoring and Security Configurations

Demo



119

Instructor: In this demonstration we're going to set up an EC2 instance on AWS and take a quick review of some of the monitoring and security configurations. So the first thing we're going to do is click Launch Instance. You can review the various AMI's or Amazon Machine Images that are available. Some will have a cost associated with them, while others are free. That cost generally depends on the size of the instance and if there's any applications in there that might need to be licensed. So if we look at the Amazon Marketplace, we'll take a quick look at one of these instances here, the Trend Micro one, and can see it provides some of the hourly rates, billing details, those types of things. It also has the end user licensing agreement, which you can review, and this will be different based off of the AMI and the vendor associated with it. So you'd want to take a close look at that and make sure it applies to what your needs are. There's also some samples for you here in various categories like business apps, DevOps, infrastructure, software, those types of things, to help organize the AMIs and make it easy to find what you're looking for. There's also a search capability if you're looking for something specific.

We'll go ahead and start a Windows server instance. We're going to make it as small as possible. We just want to demonstrate our ability to get this fired up so we can see it. So We'll go with the Free Tier version of that. Keep in mind, it is Windows so It'll be under-resourced and that might hurt us later on, but we're just doing it for testing. We'll establish our VPC, our virtual private cloud, which is our default one, and we could select a subnet within our VPC if we wanted to, but we'll let it auto choose for us, along with some of these other settings. We don't need to configure anything specific to a domain joining or a specific IAM rule. We're going to check the box for CloudWatch, to enable some detailed reporting, and we're going to use a shared instance.

So there's different pricing here. If you were going to have a dedicated instance where it's running in its own hardware isolated, further isolated from other customers, you can use that option, but again that costs little bit more money, and then there's some other enhancements in terms of enhanced graphics and whatnot. While at storage, we're just going to accept the default here, but you can see there's a couple different storage options available for your SSD storage. You can also configure the size of that. A lot of it depends on what your performance needs might be, and if you want the Elastic Block Storage drive to be deleted upon instance termination you would keep this box checked.

And next we'll review a security group configuration. These are the permissions that you would allow access into this virtual machine. So it has by default RDP and SSH, assuming that you'd want those management ports open, but they're also by default open to the world, so that's something that you need to consider changing, whether you have a specific IP address for your organization or your trusted host. You might want to configure that in here at this time. You could also do it afterward.

So we'll review our instant settings, and when we're ready we'll go ahead and click Launch. There is an option here for key pairs generating these, so you can access the virtual machine once it comes up. You'll need to generate the key pair unless you know what the admin password is, so we'll go ahead and create a new key pair. Give it a name, and then we can download this key pair and we'll see how to use that in just a moment, and our instance is launching. Once that gets initialized you'll see we're taken to another page with how to connect to your instance, some other information for getting started.

Next we're going to look at our billing preference real quick and make sure that we set these up. We want to make sure that we get usage alerts. We have a Free Tier that we're signed up for, so if anything goes beyond that Free Tier or if there's any unforeseen expenses, I want to know about them right away.

Let's return to our instance and connect. We're going to use a standalone remote desktop client. We also need to get this password. So using that key pair that we generated we can load that key pair, decrypt the password, and then it shows us what that administrator password is and then we can now copy that and use that when we connect the RDP. We're using an image that somebody else created, so knowing that administrator password, we just don't know it to start out with. So this is a mechanism that allows you to generate that. So a lot of it depends on the AMI that you're using as well.

So as we connect to the Windows server, we're not going to do a whole lot in here except look at IP addresses. So you see our internet

IP is highlighted here. We just went out to the internet from that desktop, and we also have a local IP. We'll go ahead and close this and see how we can verify that within our EC2 dashboard. So here we're going to look at networking and mange IP addresses, and you see where our private and public IP is listed. It's also down in the bottom in the description and details.

Let's now go take a look at this CloudWatch monitoring option that we enabled. So we're going to add a new alarm and we're going to notify ourselves once a certain threshold is met. So right now we just going to enter name of our alarm. We're going to put in an email address, and what do we want it to do? In some cases we might want it to stop or terminate or reboot the instance. It just depends on what it is. We might not need to take an action, but there is the option to do that here, and then we're going to set our thresholds, whether that's a greater than or equal to a certain percentage, whether that's CPU memory or whatever it might be. So there we're alerting on CPU utilization. We're going to take an action, including a notification, and we have established a new EC2 instance along with a security key for accessing that instance and access control lists that allow only RDP from a specific IP address.