Lab: Deploying an EC2 Windows Server

Author: Luis Molina

Draft version 0.1

Abstract

In this lab, you will configure your AWS Account and create a new EC2 Windows Server instance. You will configure an IAM policy and the underlying VPC network configuration. You will then connect to the windows server using Remote Desktop Connection.

Introduction

Amazon Web Services offers you the flexibility to run Microsoft Windows Server for as much or as little time as you need. You have many versions of Windows to choose from and the ability to specify server and network performance capabilities based on your requirements.

Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Microsoft and Amazon have jointly developed a set of Amazon Machine Images (AMIs) for some of the more popular Microsoft solutions. For more information on the available Windows AMIs go to: <https://aws.amazon.com/windows/resources/amis/>

Lab Overview

In this lab, you will create a VPC and define a public network subnet within it. Then you will create an IAM policy to restrict EC2 instance launch to a specific region and assign this policy to a user. Finally you will launch a Windows EC2 instance and connect to it remotely via Remote Desktop Connect.

Prerequisites

To complete the lab, you need the following requirements:

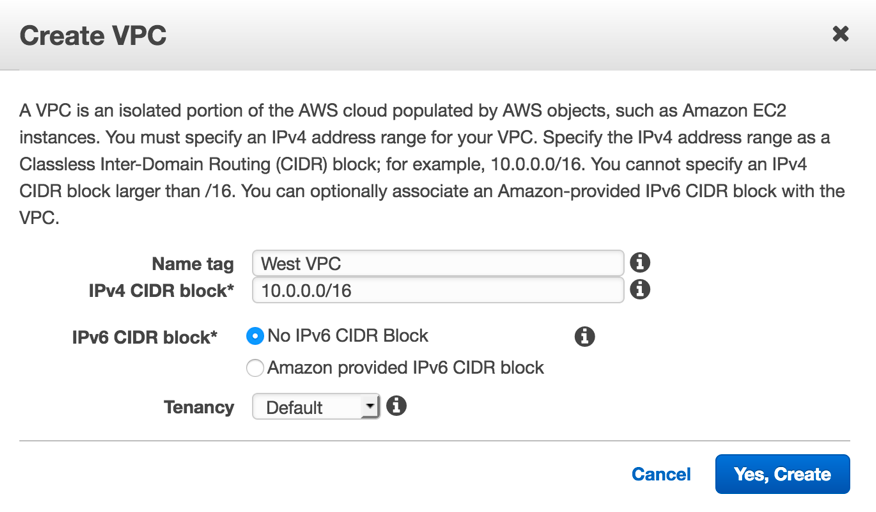
1. Microsoft Remote Desktop Connect installed on your local computer.
2. An AWS Account
3. An AWS IAM user with rights to create a Virtual Private Cloud (VPC) in your AWS account and ability to create Routes/Internet Gateway.
4. An AWS IAM user with privileges to create/modify EC2 instances and create IAM users.

Configure Network

Before launching a new instance, you will need to configure a new VPC, subnet, internet gateway and routes. All activities should be performed in the **us-west-1** region (N. California).

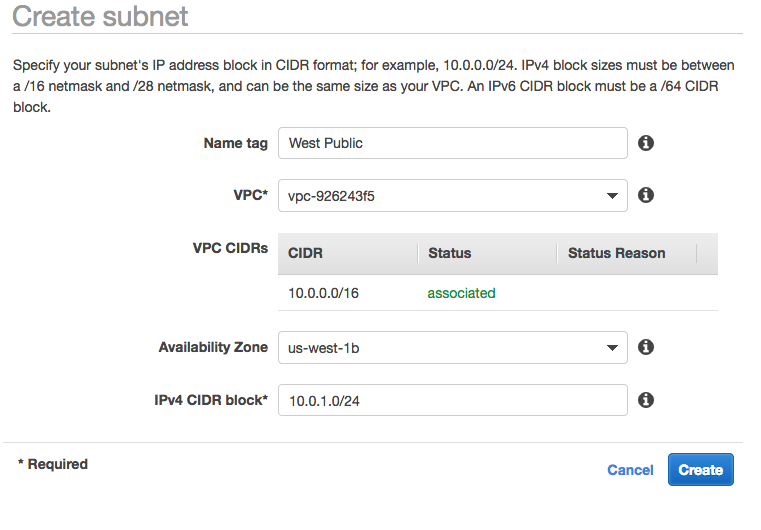
1. In AWS console ensure that you are accessing the West-1 region, navigate to VPC.
2. In the left navigation pane click “Your VPCs”
3. Click **Create VPC** then configure:

* Name tag: West VPC
* IPv4 CIDR block: 10.0.0.0/16
* Click Yes,Create



Next you will define and configure a public subnet in the “West VPC” you created:

1. From the VPC Dashboard, navigate to the left pane and click **Subnets**
2. Click the **Create Subnet** button then enter the following configuration:
   * Name tag: West Public
   * VPC\*: West VPC
   * Availability Zone: Select the first AZ in the list
   * IPv4 CIDR Block: 10.0.1.0/24
   * Click Create



1. Back in the VPC Dashboard in the Subnet view: select “West Public”.
2. In the **Actions** menu, select **Modify auto-assign IP Settings**
3. Select **Enable auto-assign public IPv4 addresses** – This setting provides a public iPV4 address for all instances launched into the “West Public” Subnet.

The “West Public” subnet is not publicly accessible until you associate it with an Internet Gateway. The Internet Gateway is a VPC component that allows communication between instances in your VPC and the internet. An Internet Gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

In the next step you will create and assign an Internet Gateway to allow remote connectivity to your EC2 instance.

1. Navigate to the left side of the VPC dashboard and click: **Internet Gateways**
2. Click **Create Internet Gateway** then configure the following settings:
   * Name Tag: West IG
   * Click Create
   * Click Close
3. Select the Internet Gateway you just created “West IG”, in the **Actions** menu select **Attach to VPC**
   * VPC: West VPC
   * Click **Attach**

You now have an Internet Gateway attached to your VPC. Now you need to enable traffic flow between your public subnet and the internet.

Next you will create a route table for internet-bound traffic and add a route to the table to direct internet bound traffic to your internet gateway and finally associate your public subnet with the route table.

1. Navigate to the VPC Dashboard, on the left side click **Route Tables**

* You will see a route table for the default VPC and also one for the “West VPC” you created earlier, these facilitate local VPC traffic

1. Click the **Create Route Table** button then configure:
   * + Name Tag: West Public Route Table
     + VPC: West VPC
     + Click **Yes,Create** button
2. Select “West Public Route Table” and click the **Routes** tab in the bottom half of the page.
3. Click **Edit** button then **Add another Route** button and configure:
   * + Destination: 0.0.0.0/0
     + Target: West IG
     + Click **Save** – This route will direct non local traffic to the Internet Gateway
4. Click the **Subnet Associations** Tab

* Click **Edit**
* Click **Save**
* **Select** “West Public” Subnet – the subnet is now public

# Configure a Security Group

You will now create a security group which will allow remote desktop (RDP) access to an EC2 instance.

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

1. From the VPC dashboard, navigate left and under Security click **Security Groups**
2. Click **Create Security Group** then configure:

* Name Tag: RDP Access
* Group Name: RDP Access
* Description: Remote Desktop Access Group
* VPC: West VPC
* Click **Yes, Create**

1. Select **RDP Access** Security Group
2. Click the **Inbound Rules** Tab
3. Click **Edit** then configure:

* Type : RDP (3389)
* Source: 0.0.0.0/0
* Click Save

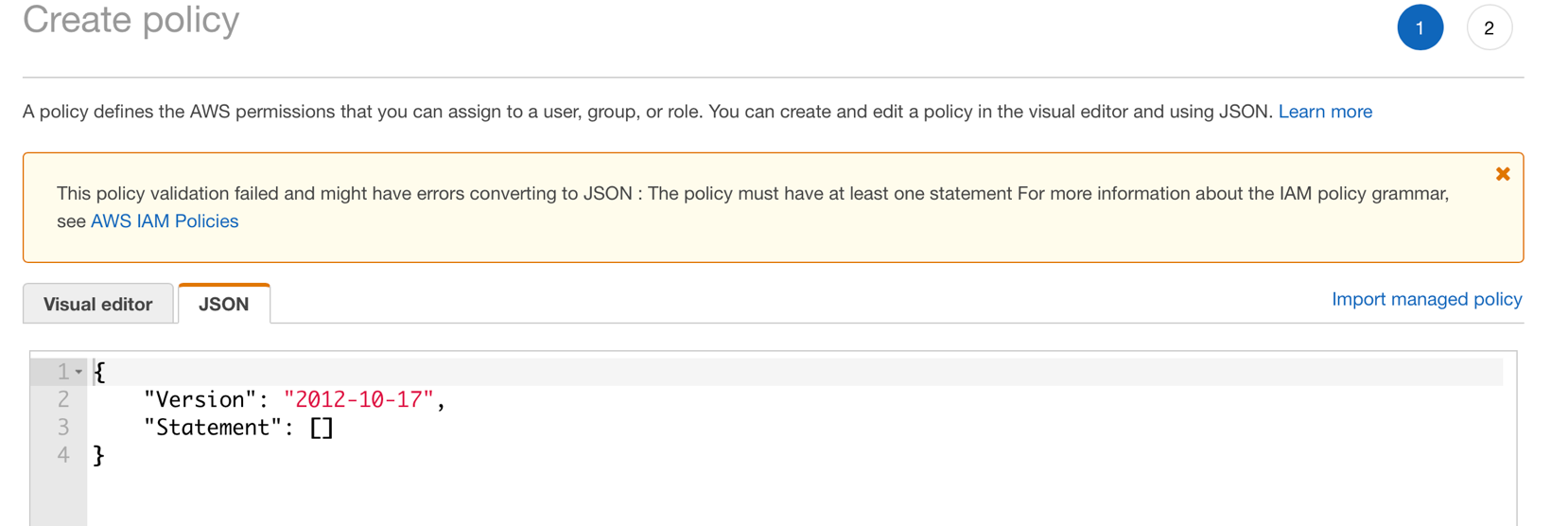
(Note: This rule will open RDP port access to the entire internet, this is not recommended in a production environment. It is recommended that you scope this down to your local IP or subnet range if you plan to keep this configuration running after you complete the lab.

You have now completed the network configuration. You now have a VPC in the us-west-1 region with a public subnet routed to an internet gateway. You have also created a security group which will allow RDP access from the internet to its members.

# Configure an IAM User and Policy

Next you will work in the Identity and Access Management service (IAM) to create a user and define a custom policy which will restrict EC2 instance launch to a specific (US-West-1) region.

1. Navigate to the IAM console
2. In the IAM console click **Policies** on the left
3. Click **Create Policy**
4. **In the Create Policy** page, click the **JSON** tab.



1. Copy the following following text and replace all of the text in the JSON tab:

{

"Version": "2012-10-17",

"Statement": [

{

"Action": "ec2:\*",

"Resource": "\*",

"Effect": "Allow",

"Condition": {

"StringEquals": {

"ec2:Region": "us-west-1"

}

}

}

]

}

1. The JSON tab should look like this now:



This policy will restrict EC2 Instance launch to the us-west-1 (N. California) region to whichever user it is assigned to.

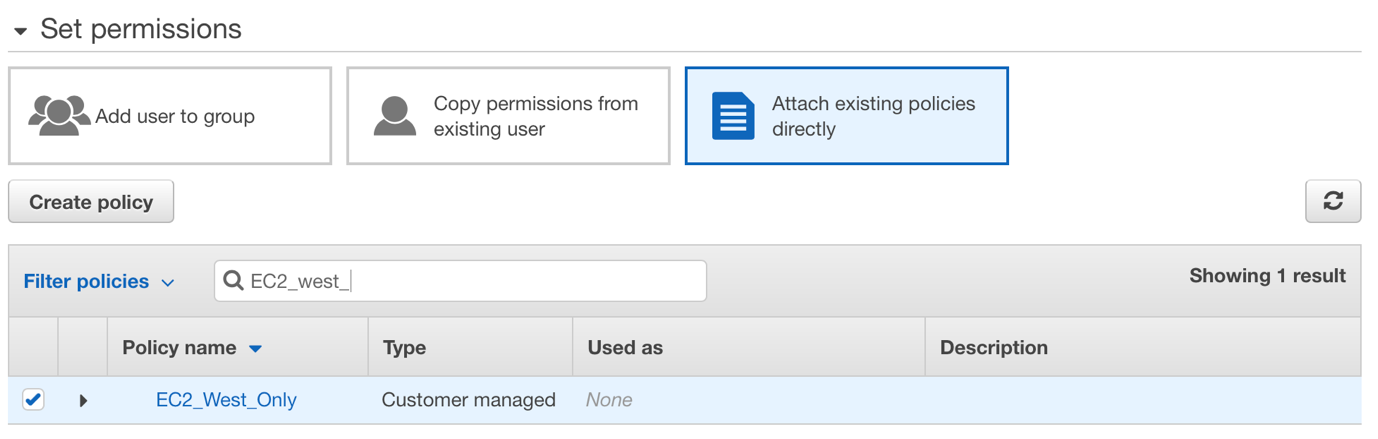
1. Click **Review Policy**
2. Name the Policy: EC2\_West\_Only

* Review the Policy, it is safe to ignore the “This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition” notification.
* Click **Create Policy**

1. Navigate to the left and click on **Users**
2. Click **Add User**
3. In the Set User Details Page configure:

* Username: West\_Admin
* Access Type: AWS Management Console Access
* Console Password Click **Custom** and enter a complex password
* Uncheck require password reset
* Click **Next: Permissions**

1. In the **Set Permissions** page select **Attach Existing Policies Directly**
2. In the **Filter Policies** search field enter: EC2\_West\_Only and select the result



1. Click **Review**
2. Click **Create User** then **Close**

You have now created a new user (West\_User) and restricted it from creating EC2 instances outside of the us-west-1 region

Create a Windows EC2 Instance

In this task, you will create a Windows Server 2016 EC2 instance in the **us-west-1** (N.California) region. You will perform the following steps as the newly created “West\_Admin” user.

1. In a new browser session (Private browsing or from another maching) log in as **West\_Admin**
2. Ensure that you are working in the **us-west-1** region (N.California)
3. Navigate to EC2 Console and click “Launch Instance”
4. In the search field type: Windows
5. Hit enter and scroll through the Windows AMI’s, select **Windows 2016 Base**
6. You can now choose an instance type, at the minimum select T2.Micro. Click **Next: Configure Instance Details**
7. In the **Instance Details** page configure:

* Network: **West VPC**
* Subnet: **West Public**
* Click: **“Next Add Storage”**

1. In the Add Storage leave the defaults and click **Next: Add Tags**
2. You can add a tag if you like, otherwise click **Next: Configure Security Group**
3. In the Security Group page, click **Select an existing Security Group**
4. In the Security Group selection, check the **RDP Access** Security Group
5. Click **Review and Launch** – You may see a “Improve your instances security” notification. This will appear if you configured your RDP Security group to allow all IP’s, as mentioned earlier this is only being used for lab purposes. For a production or post lab environment, you should scope this rule down to a specific IP or range.
6. Click **Launch**
7. You may be prompted to select an existing or create a new key pair, this allows you to securely connect to your instance. If you already have a key pair generated you can re-use that, otherwise select **Create a new key pair**. Download the .pem file and make note of where you save it, you will need it to connect later.
8. Click **Launch Instance**
9. Navigate back to the EC2 Dasboard, on the left click **Instances**
10. You should see your instance being created, mouse over the **Name** field and click on the pencil icon and name the instance: Windows West
11. Once the “Status Checks” shows “2/2 checks passed” your instance will be ready to connect.
12. Click on you new Instance **Windows West**, click **Actions** and select **Get Windows Password**
13. You will be prompted for the key pair you specified/created when you launched the instance, browse to it and select it.
14. Click **Decrypt Password**
15. Copy the username/password information and click **Close**
16. Click on the **Windows West** instance, copy it’s public IP Address
17. Launch a Windows Remote Desktop app and connect to your new **Windows West** instance using the public IP and credentials from the AWS EC2 console.

Congratulations, you have successfully launched and connected to a Windows EC2 instance.

# Validate IAM Policy

In this task, you will attempt to create a Windows Server 2016 EC2 instance in the **us-east-1 region** (N.Virginia). You will perform the following steps as the newly created “West\_Admin” user.

1. In a new browser session (Private browsing or from another maching) log in as **West\_Admin**
2. Ensure that you are working in the **us-east-1** (N.Virginia) region Navigate to EC2 Console and click “Launch Instance”
3. In the search field type: Windows
4. Hit enter and scroll through the Windows AMI’s, select **Windows 2016 Base**
5. Click **Select**
6. Take note of the error message, this is due to the region restriction policy you created earlier.

# Cleanup

Steps to remove lab content from your AWS account:

* Log back into the console as your primary admin account (not West\_Admin)
* From EC2 – Terminate **Windows West** Instance
* From VPC – Delete **West VPC**
* From IAM – Delete **West\_Admin** user and **EC2\_West\_Only** policy

Done