AWS Immersion Day
LAB 0

DEPLOY AVIATRIX IN YOUR LAB ACCOUNT

Aviatrix Systems
Solutions Team

aviatrix

Lab 0 Before

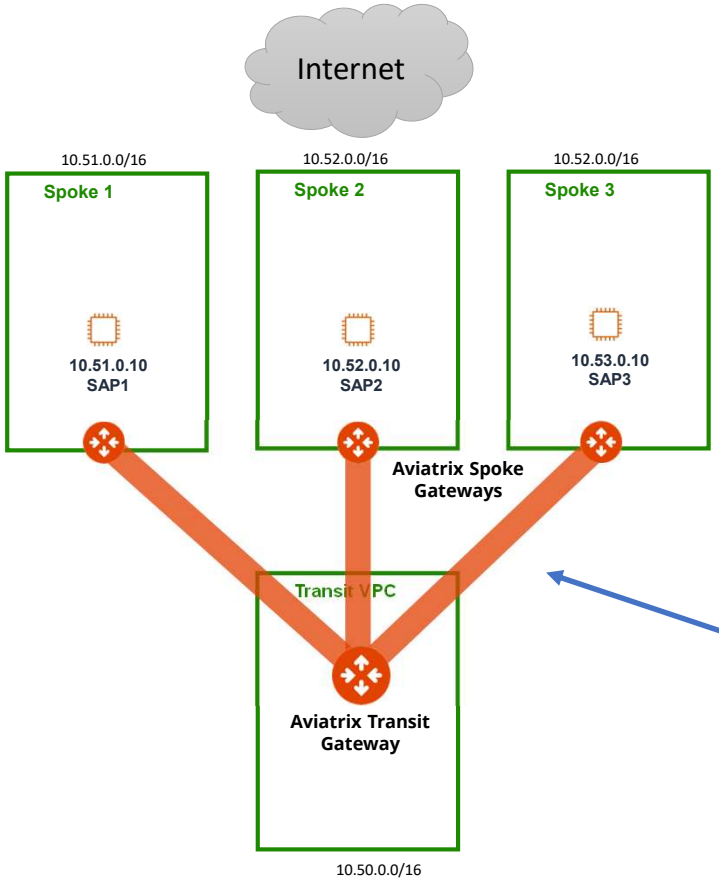
In this Immersion Day we will be using two AWS regions (us-east-1 and us-west-2)

Right now, your lab account has nothing.
No instances. No VPCs

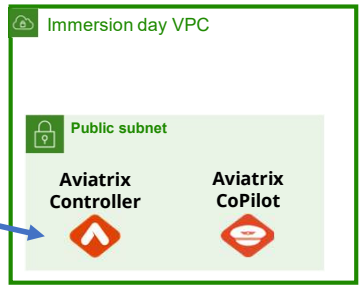
AWS us-west-2

AWS us-east-1

Lab 0 After



In this Lab you will deploy Aviatrix Controller and Copilot in us-east-1 using AWS CloudFormation.



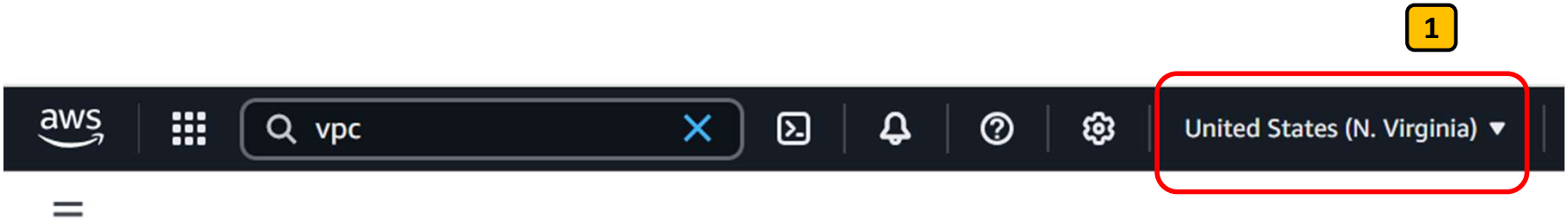
The Aviatrix Controller will then deploy VPCs and Aviatrix Gateways in us-west-2 using Terraform.

AWS us-west-2

AWS us-east-1

Lab 0: Step 0.1

Switch to US-EAST-1 region



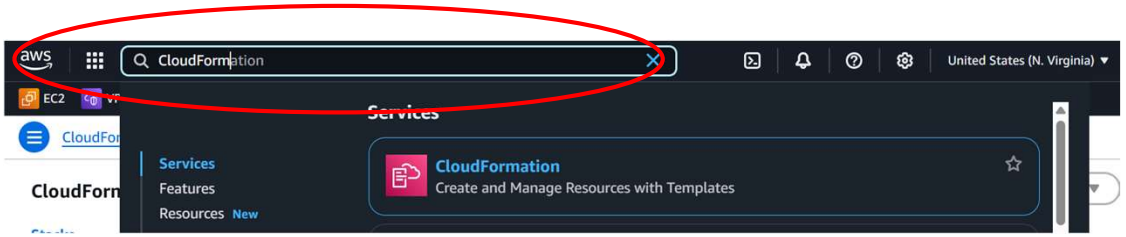
Make sure your AWS Console is in the us-east-1 **N. Virginia** region. 1

Lab 0: Step 0.2

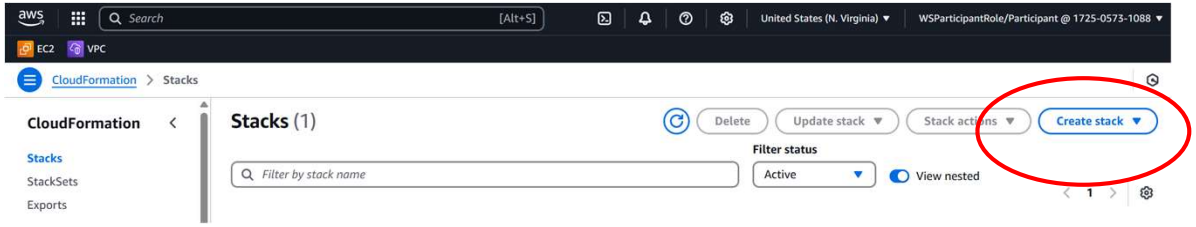
Create the stack

Make sure your AWS Console is in the us-east-1 **N. Virginia** region.

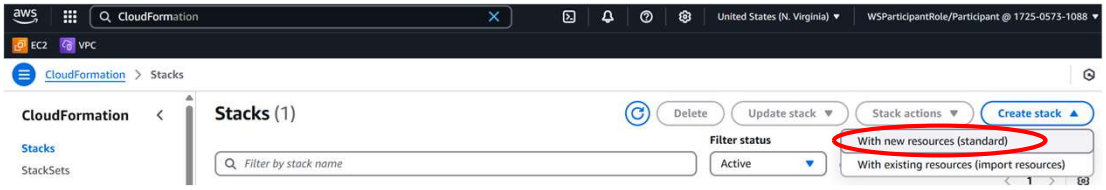
From the AWS Console go to the **CloudFormation** service. 1



Select **Create stack** 2



Select **With new resources (standard)** 3



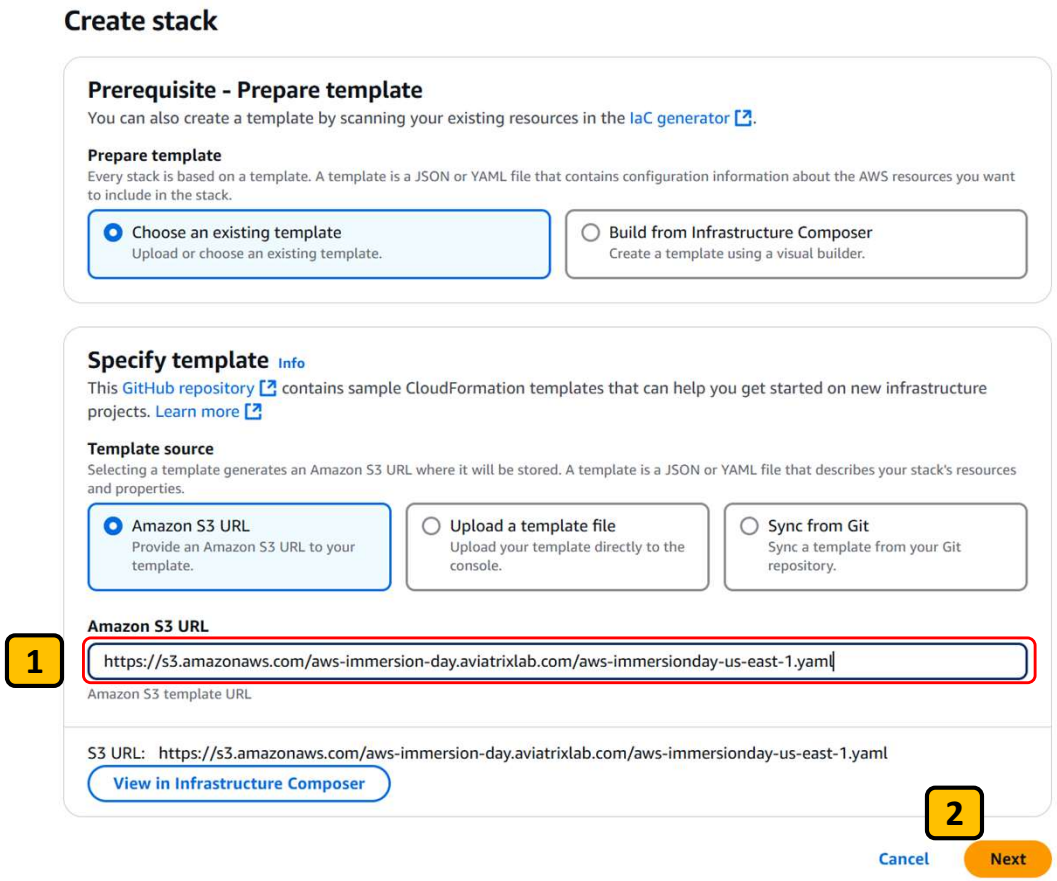
Lab 0: Step 0.3

Provide the stack URL

Keep the default settings of **Template is ready**, and **Amazon S3 URL**.

Enter the URL below in the Amazon S3 URL input field. 1

Select **Next** 2



1

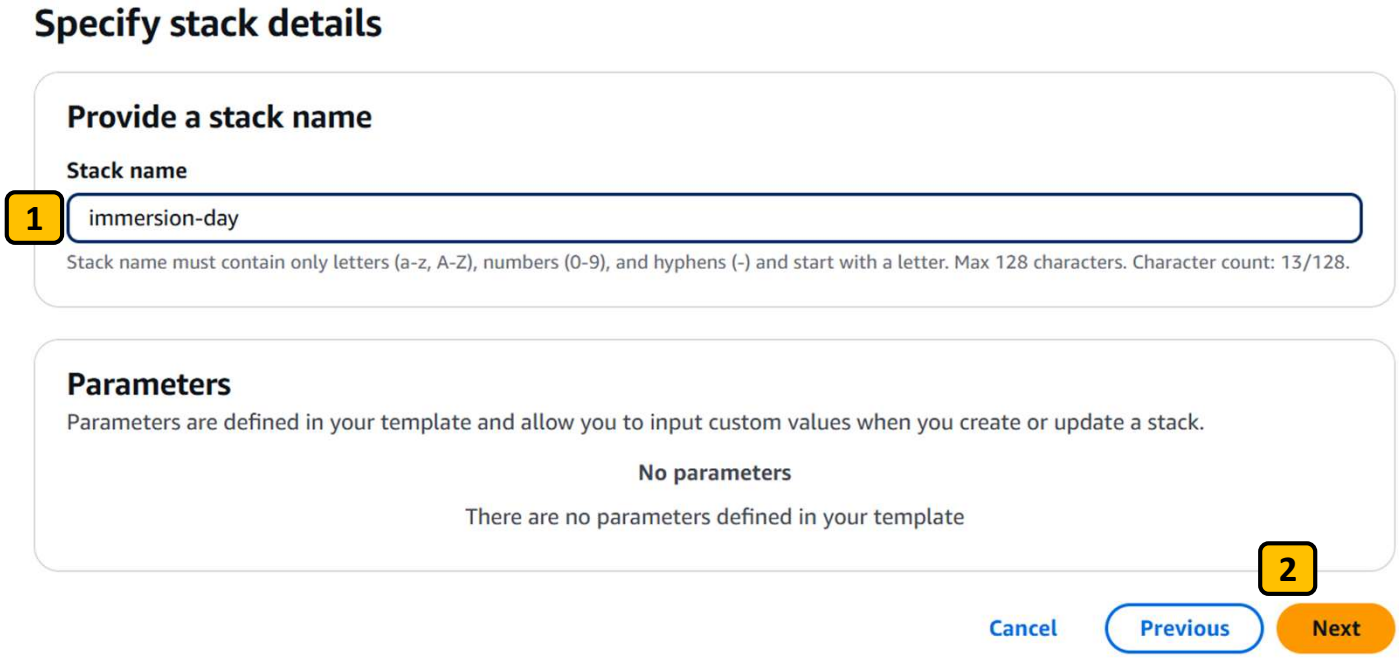
https://s3.amazonaws.com/aws-immersion-day.aviatrixlab.com/aws-immersionday-us-east-1.yaml

Lab 0: Step 0.4

Name the stack

Name the stack
immersion-day 1

Select **Next** 2

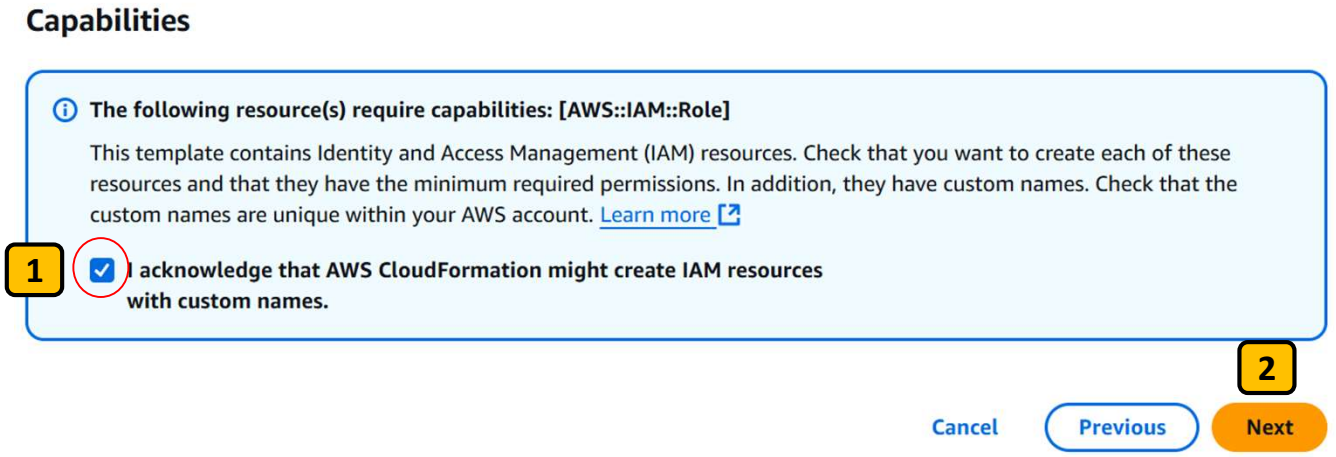


Lab 0: Step 0.5

On the next **Configure Stack Options** page just scroll down to the bottom of the page

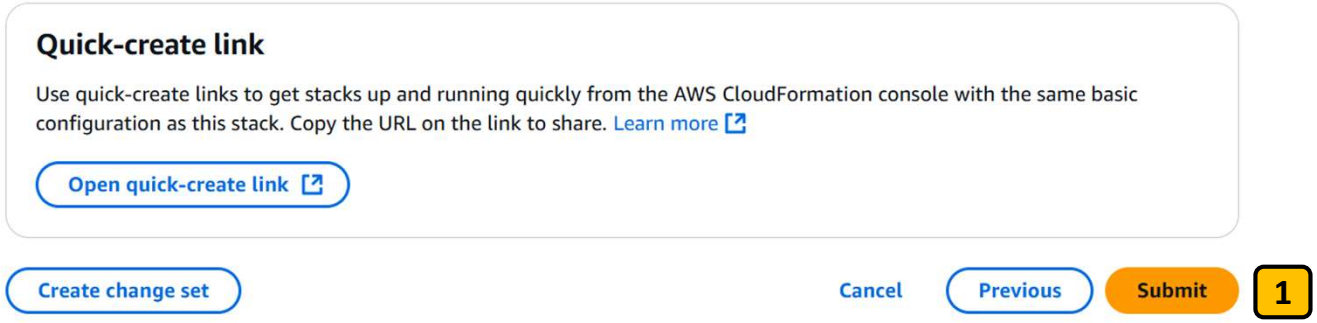
Under the **Capabilities** section select the I acknowledge 1 checkbox

Then click **Next** 2



Lab 0: Step 0.6

On the **Review and create** page just scroll down to the bottom of the page and click **Submit** 1



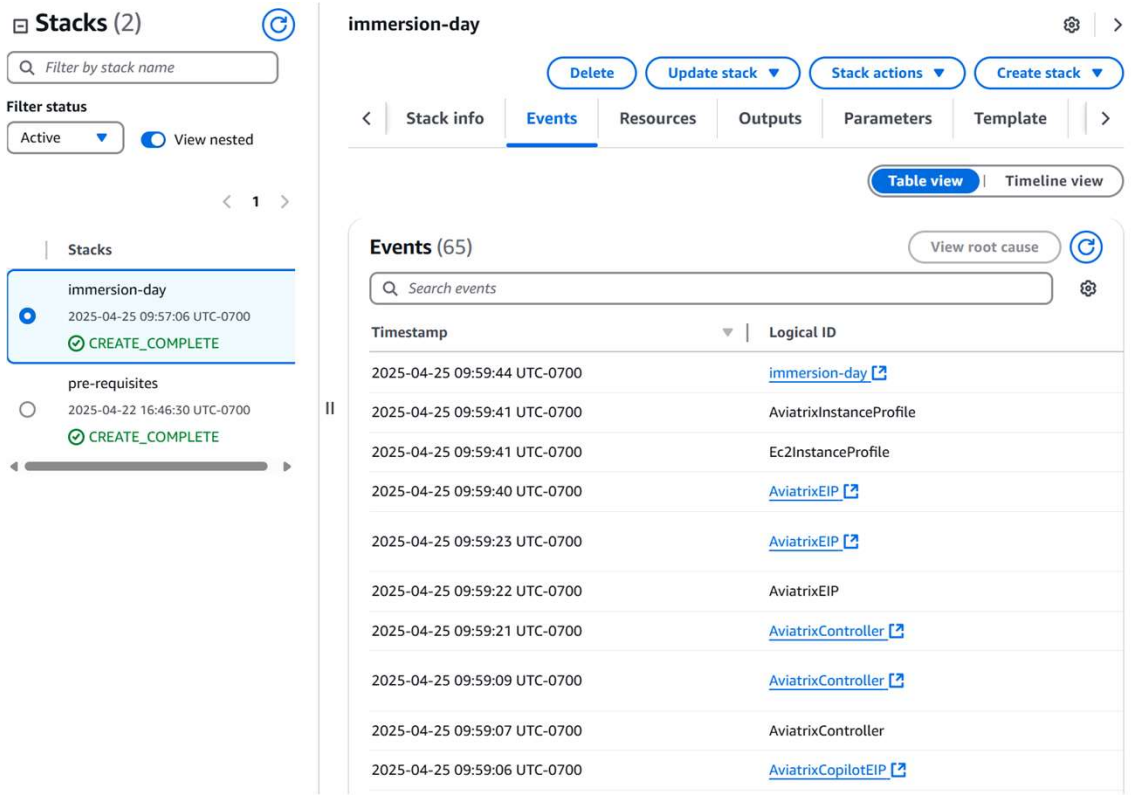
Lab 0: Step 0.7

Observe the stack deployment

On the next page you'll see your stack deploying if you select the **Events** tab

WSDefaultPolicy

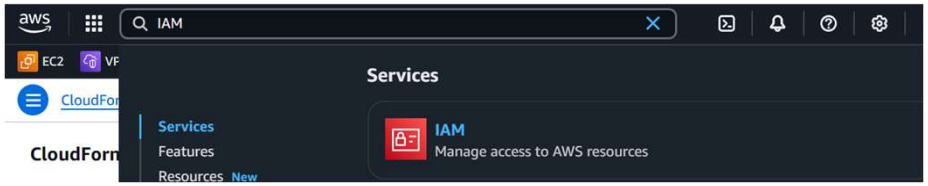
The deployment will take about 30 minutes to complete.



Lab 0: Step 0.8

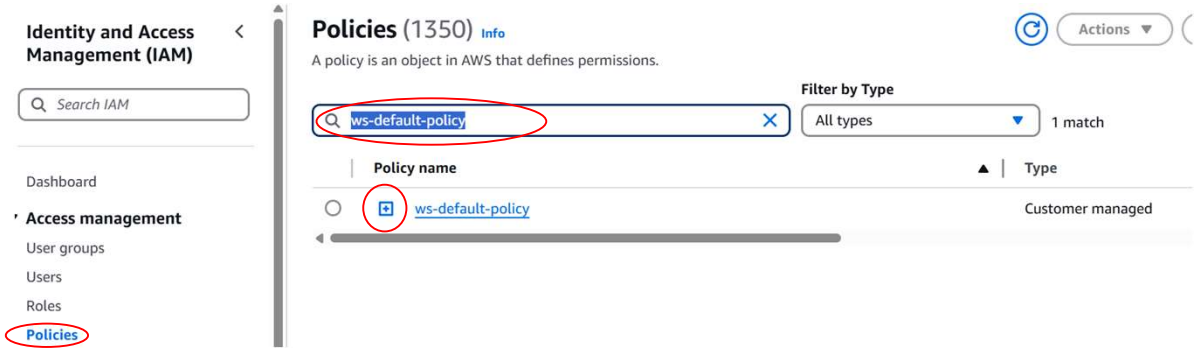
Find the IAM Policy Role Permissions

Search for and click on the **IAM** service



Click on **Policies** and search for the policy named **ws-default-policy**

Click on the + next to the policy



Click on **Edit**

Lab 0: Step 0.9

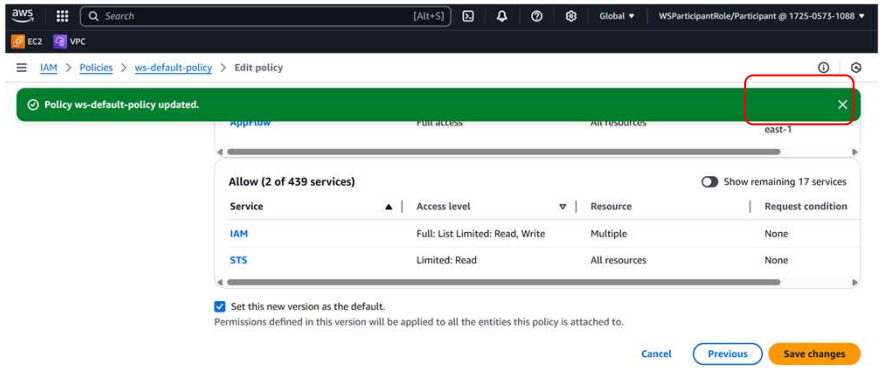
Edit the IAM Policy Role Permissions

In the Policy Editor, replace all of the policy lines with the following Policy:

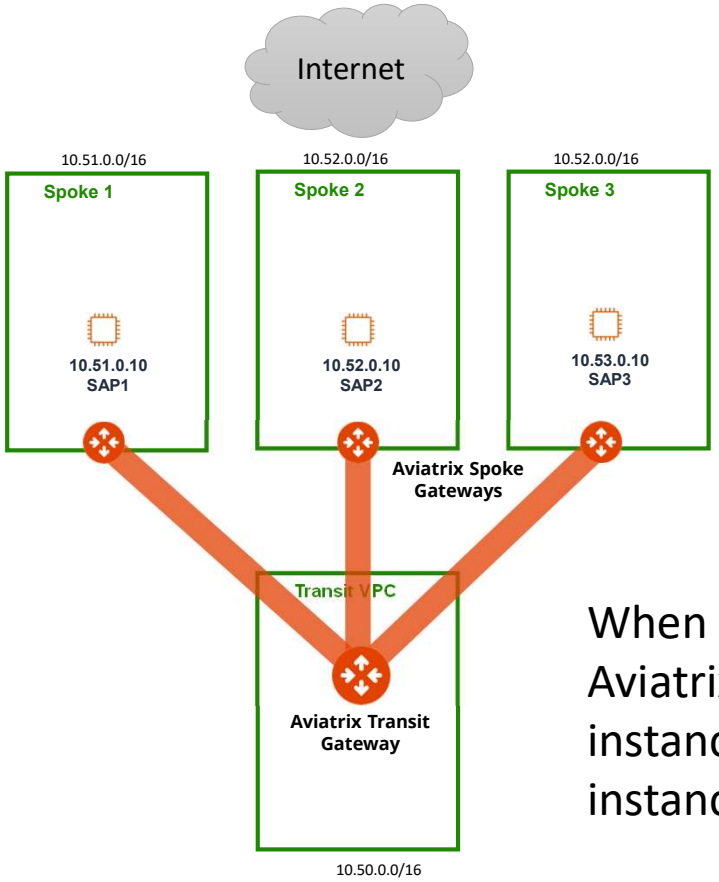

```
{
	"Version": "2012-10-17",
	"Statement": [
		{
			"Sid": "AllowIamReadOnly",
			"Effect": "Allow",
			"Action": [
				"iam:List*",
				"iam:Get*",
				"iam:Generate*",
				"sts:GetCallerIdentity"
			],
			"Resource": [
				"*"
			]
		},
		{
			"Sid": "AllowCreateSLR",
			"Effect": "Allow",
			"Action": [
				"iam:CreateServiceLinkedRole"
			],
			"Resource": [
				"arn:aws:iam::*:role/aws-service-role/*"
			]
		},
		{
			"Sid": "AllowIamPassRole",
			"Effect": "Allow",
			"Action": [
				"iam:PassRole"
			],
			"Resource": [
				"arn:aws:iam::172505731088:role/WSParticipantRole"
			]
		},
		{
			"Sid": "DenyAllOutsideAllowedRegions",
			"Effect": "Deny",
			"NotAction": [
				"iam:*",
				"sts:*",
				"s3:*",
				"do:*",
				"artifact:Get",
				"artifact:DownloadAgreement",
				"lightsail:*",
				"networkmanager:*",
				"braket:*",
				"quicksight:*",
				"cloudfront:*",
				"route53:*",
				"route53-recovery-cluster:*",
				"route53-recovery-control-config:*",
				"route53-recovery-readiness:*",
				"servicediscovery:*",
				"waf:*",
				"waf-regional:*",
				"wafv2:*",
				"cloudwatch:DescribeAlarms",
				"cloudwatch:PutMetricAlarm",
				"cloudwatch:DeleteAlarms",
				"cloudwatch:GetMetricStatistics",
				"elasticloadbalancing:DescribeLoadBalancers",
				"ec2:Describe*",
				"ecr:GetDownloadUrlForLayer",
				"ecr:BatchGetImage",
				"ecr:BatchCheckLayerAvailability",
				"ec2:AuthorizeSecurityGroupIngress",
				"ecr:GetAuthorizationToken",
				"globalaccelerator:*",
				"acm:List*",
				"acm:Describe*",
				"cloudformation:List*",
				"cloudformation:Describe*",
				"kms:Describe*",
				"kms:ReEncrypt*",
				"kms:GenerateDataKey*",
				"kms:Get*",
				"kms:List*",
				"kms:CreateGrant",
				"kms:RevokeGrant",
				"ssm:List*",
				"ssm:StartSession",
				"ssm:DescribeInstanceInformation",
				"ssm:GetConnectionStatus",
				"ssm:DescribeSessions",
				"ssm:TerminateSession",
				"directconnect:*",
				"sso:List*",
				"sso:Describe*",
				"sso:Get*",
				"bedrock:InvokeA*"
			],
			"Resource": [
				"*"
			],
			"Condition": {
				"StringNotEquals": {
					"aws:RequestedRegion": [
						"us-east-1"
					]
				}
			}
		}
	]
}
```

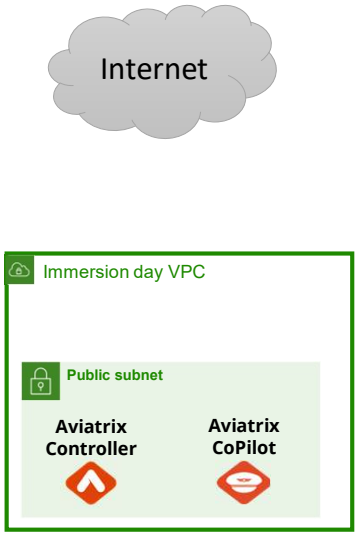

Note: Formatting in AWS Policy Editor is very specific in its formatting requirements. This must be copied exactly in order to work.

On the **Review and save** screen scroll to the bottom and click on **Save changes**



Lab 0 Done





When the deployment is done, you'll see the Aviatrix Controller and CoPilot as EC2 instances in us-east-1, and you'll see VPCs and instances, Aviatrix Gateways in us-west-2.

AWS us-west-2

AWS us-east-1