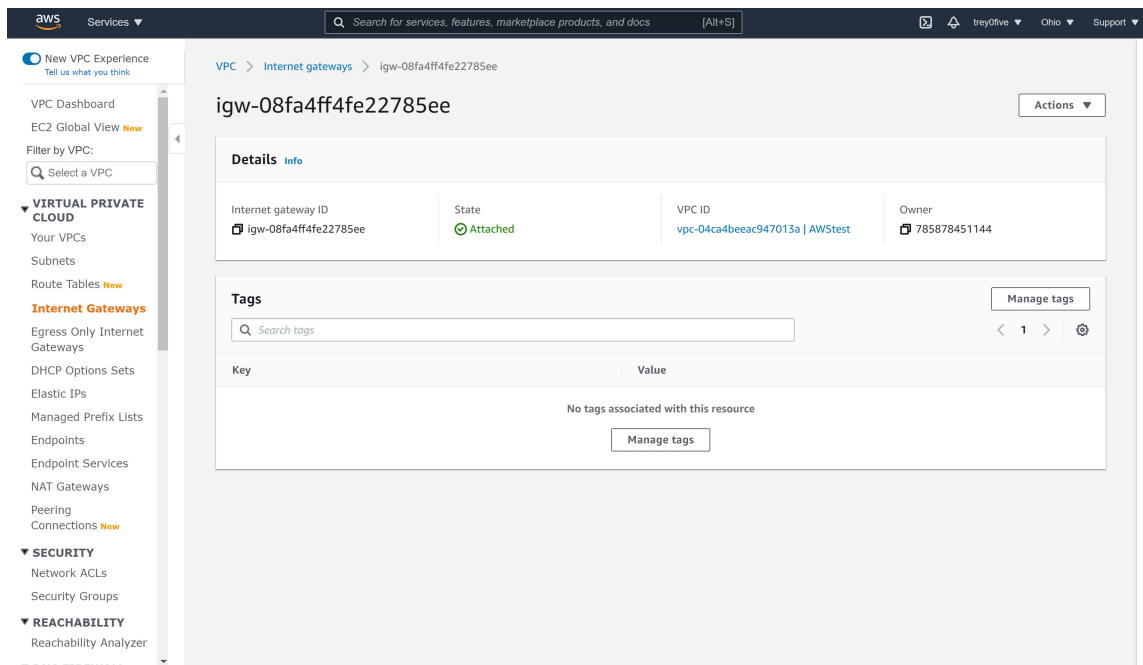
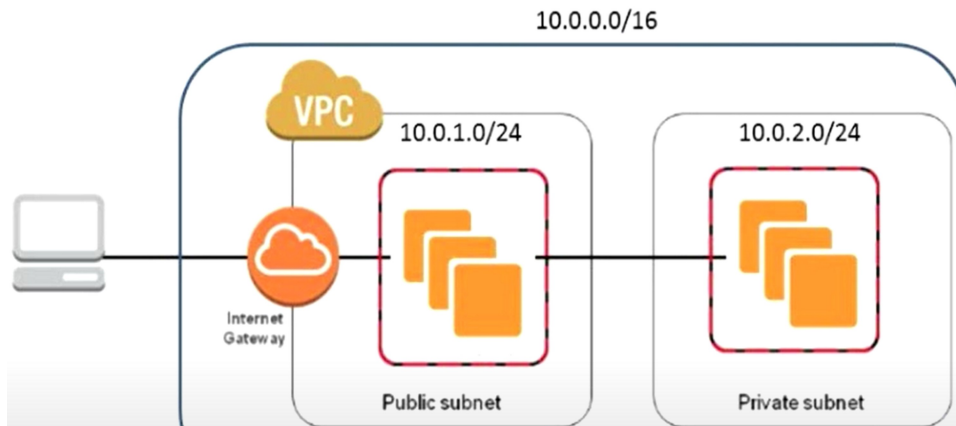
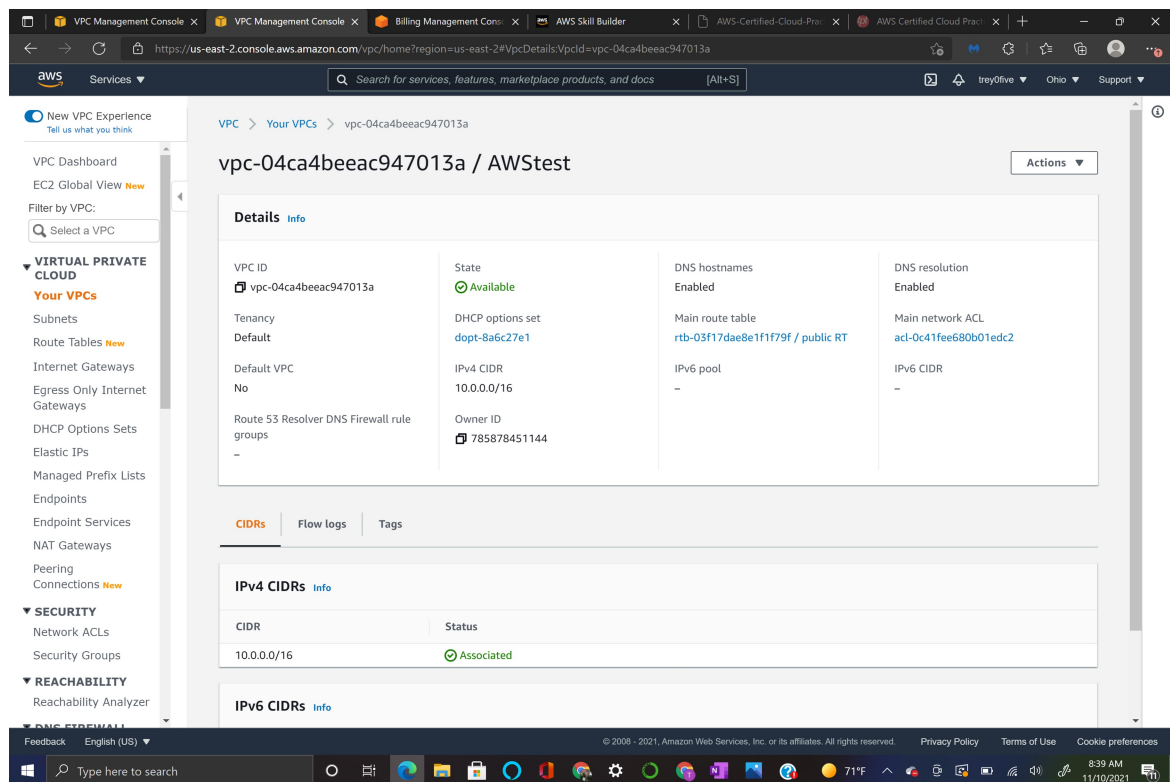


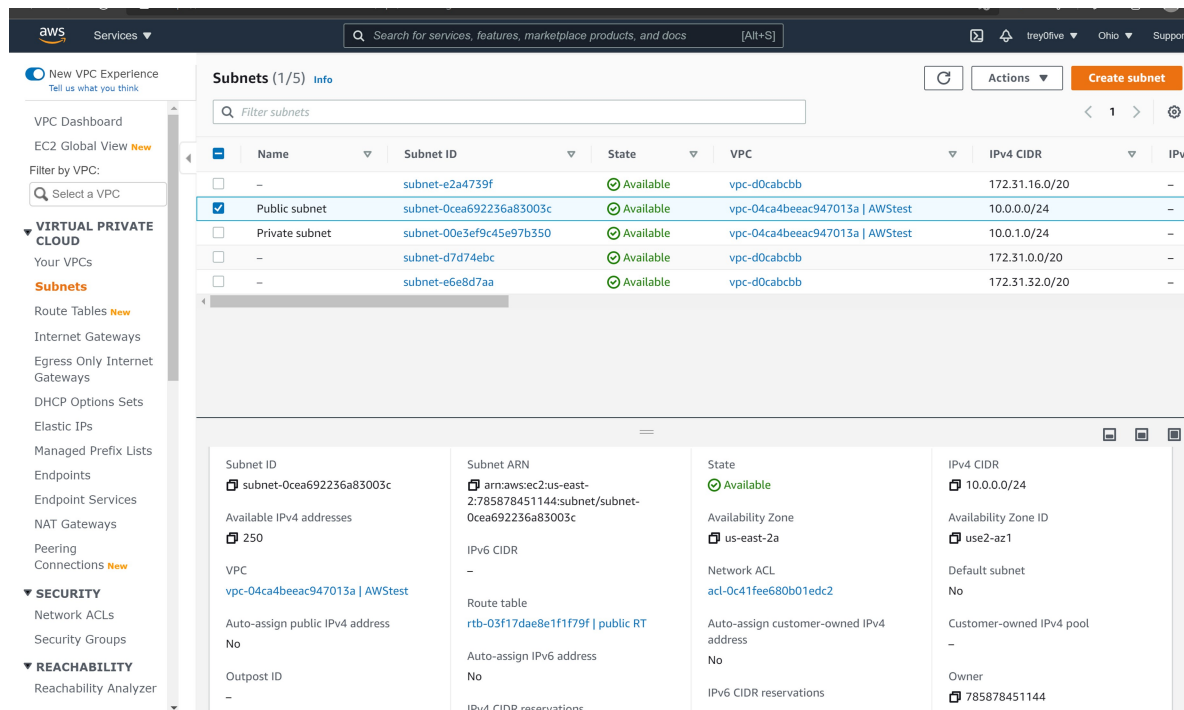
AWS project



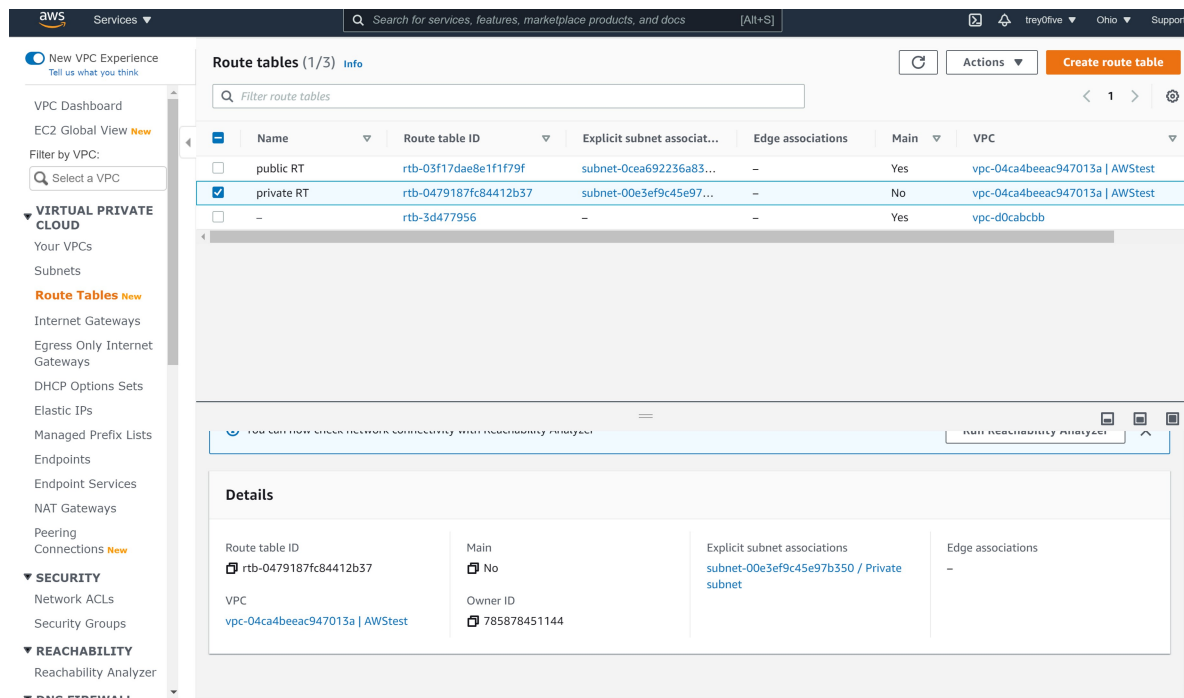
I created an internet gateway that routes to a public network to handle all incoming and outgoing web traffic. The private subnet only processes commands from the public subnet and will likely be for a database.



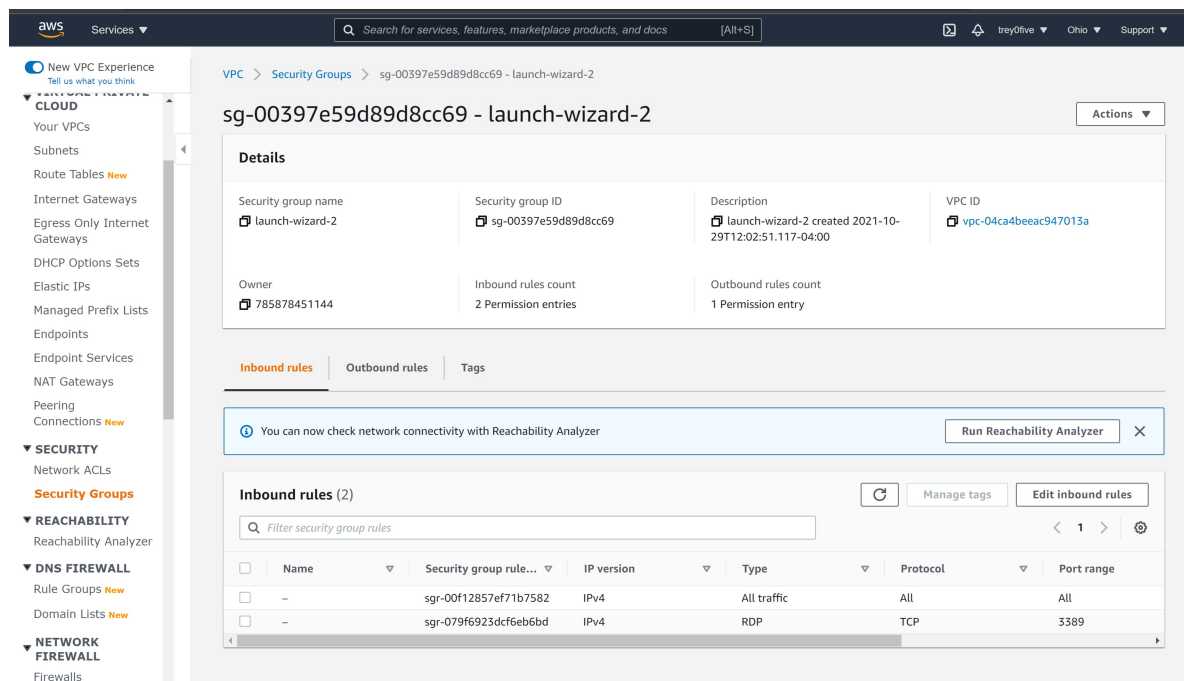
VPC named AWSTest that's connected to the public route table that was created.



These are the private and public subnets created for the VPC entitled AWSTest



Route tables created for the public and private subnets. Each are explicitly associated with the respected subnet.



Security group created for the VPC. Currently it allows all incoming and outgoing traffic between the instances.

aws Services Search for services, features, marketplace products, and docs [Alt+S] treyOlve Ohio Support

New VPC Experience Tell us what you think

CLOUD

- Your VPCs
- Subnets
- Route Tables **New**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering
- Connections **New**

SECURITY

- Network ACLs**
- Security Groups

REACHABILITY

- Reachability Analyzer

DNS FIREWALL

- Rule Groups **New**
- Domain Lists **New**

NETWORK FIREWALL

- Firewalls

VPC > Network ACLs > acl-0c41fee680b01edc2

acl-0c41fee680b01edc2

Actions

Details info

Network ACL ID acl-0c41fee680b01edc2	Associated with 2 Subnets	Default Yes	VPC ID vpc-04ca4beac947013a / AWSTest
Owner 785878451144			

Inbound rules | Outbound rules | Subnet associations | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules (2) [Edit inbound rules](#)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Network ACLs which currently allow all incoming and outgoing traffic in the VPC.

aws Services Search for services, features, marketplace products, and docs [Alt+S] treyOlve Global Support

Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analizers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

IAM dashboard

Security recommendations

- Root user has MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.
- Root user has no active access keys**
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	1	3	0	0

What's new [View all](#)

Updates for features in IAM

- IAM Access Analyzer** helps you generate fine-grained policies that specify the required actions for more than 50 services. 3 months ago
- IAM Access Analyzer** helps you generate IAM policies based on access activity found in your organization trail. 3 months ago
- IAM Access Analyzer** adds new policy checks to help validate conditions during IAM policy authoring. 4 months ago
- AWS Amplify** announces support for IAM permissions boundaries on Amplify-generated IAM roles. 5 months ago

[more](#)

AWS Account

Account ID
785878451144

Account Alias
785878451144 [Create](#)

Sign-in URL for IAM users in this account
<https://785878451144.signin.aws.amazon.com/console>

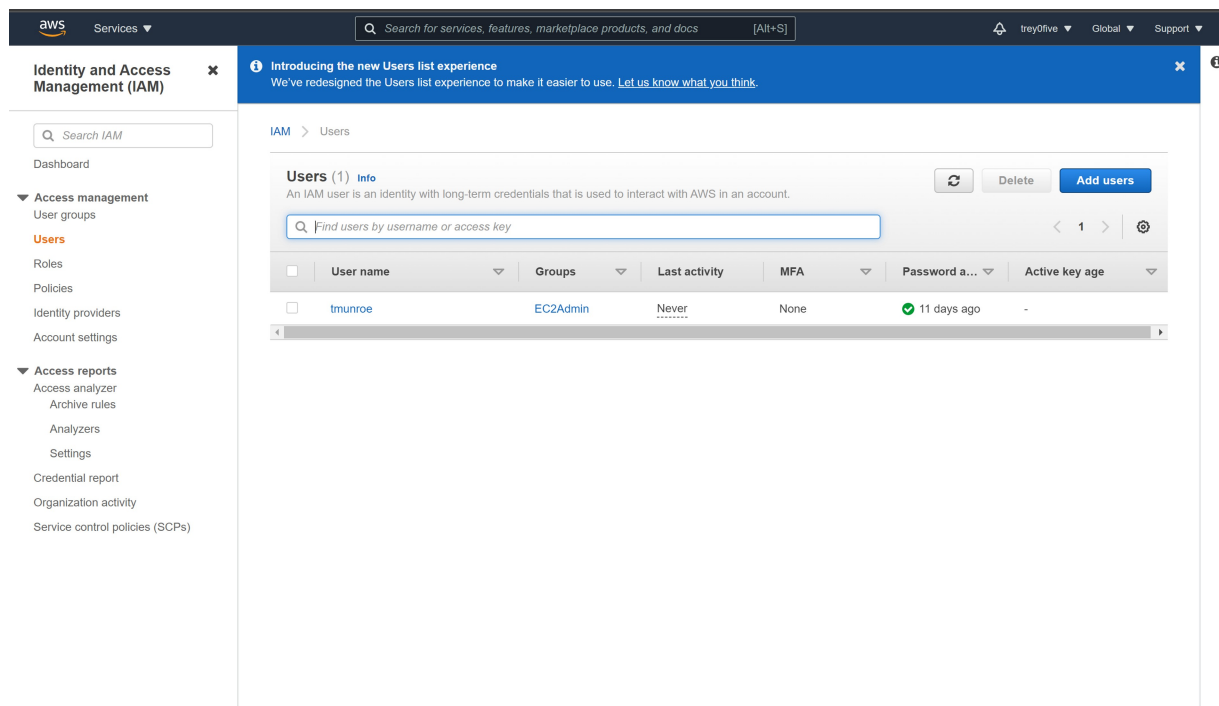
Quick Links

- [My security credentials](#)
Manage your access keys, multi-factor authentication (MFA) and other credentials.

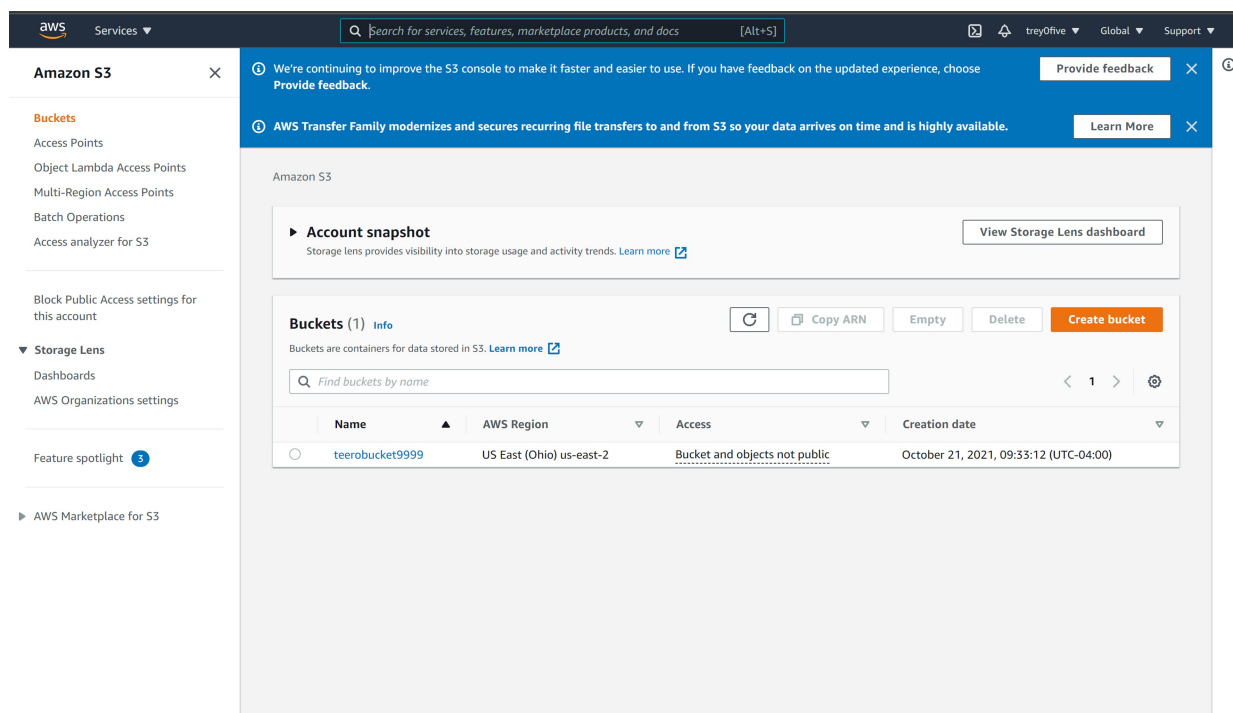
Tools

- Policy simulator**
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
- Web identity federation playground**
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API

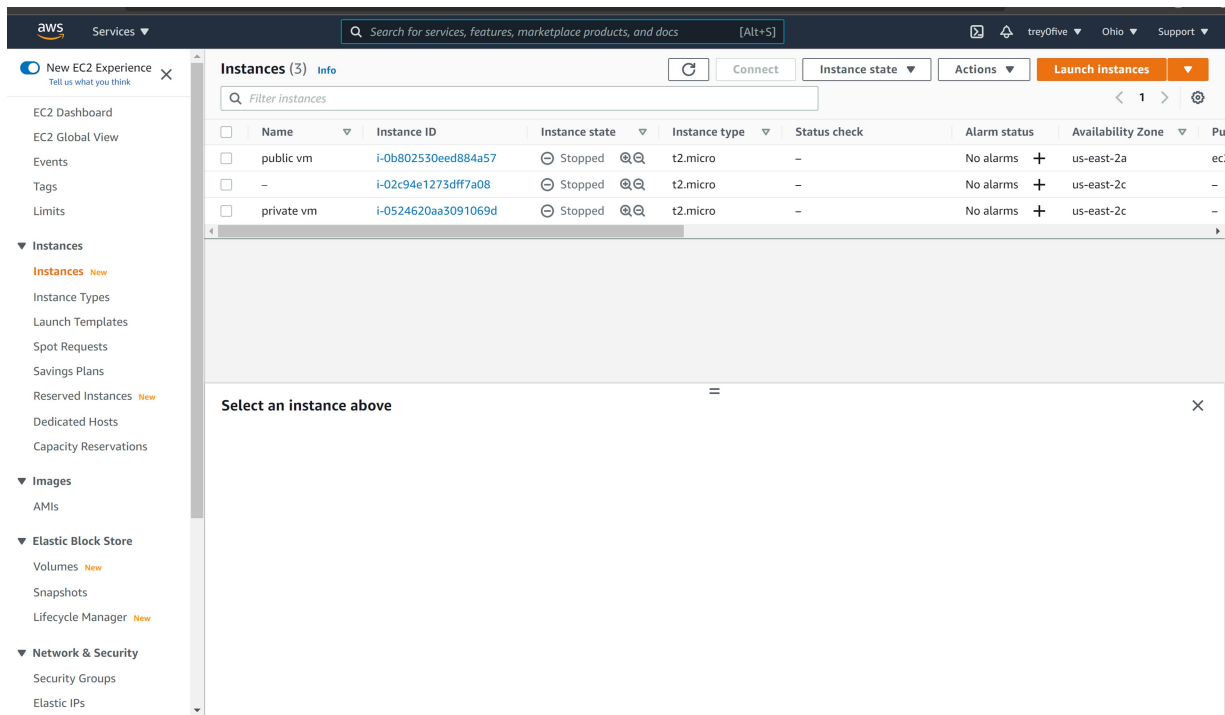
IAM dashboard that shows security recommendations and also confirms MFA config



Created an IAM user that gives said user full access to EC2 components



Created an S3 standard bucket for object based storage needs.



Public and private instances created with the free tier t2.micro option. Both instances are running Microsoft Windows 2016 Server and are connected to the AWSTest VPC