AWS VPC:
Virtual Private Confusion?

Steven Lembark
Workhorse Computing
lembark@wrkhors.com

It used to be simple

You went to AWS.

Created a new node.

Maybe added some disk to it.

And off you went, computing happily ever after.

Too simple

Catch: Everyone’s nodes were in one subnet.

We could all see one another.

Maybe your neighbor wasn’t pretty.

Maybe they’d been cracked.

Whatever reason, you want *privacy*.

Private, no longer simple

OK, but no more ‘just create a node’.

Creation starts with a “Virtual Private Cloud”.

Then you get to create subnets, security rules, IP gateways, NAT Gateways in multiple availability zones in multiple regions... Got that?

AWS Nomenclature

AWS services are provided in “Regions”.

- “us-east”, “us-west”, “canada”.

Regions have “Availability Zones”.

- Designed to fail separately.
- Redundancy uses multiple zones within a region.
- EC2 & subnets make heavy use of zones.

What you end up with

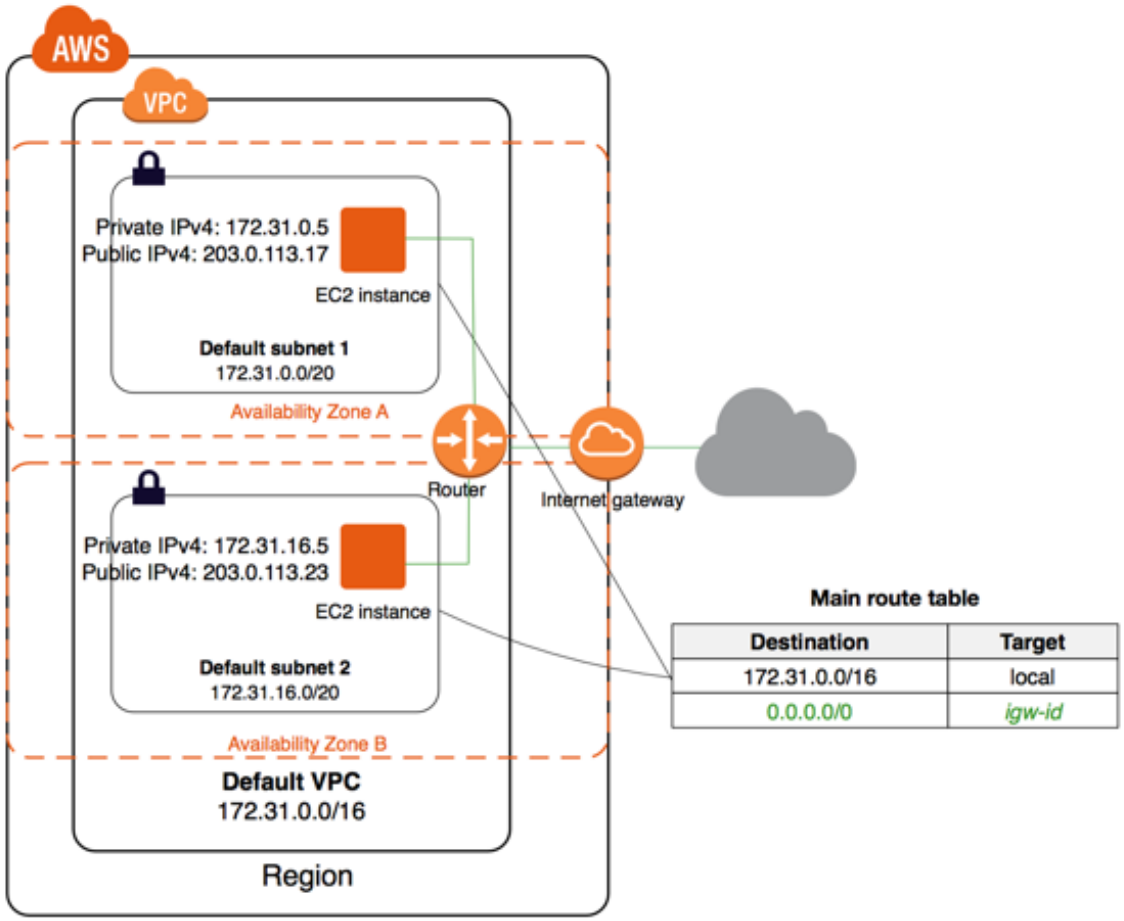
From the AWS docs:

Public & private subnets.

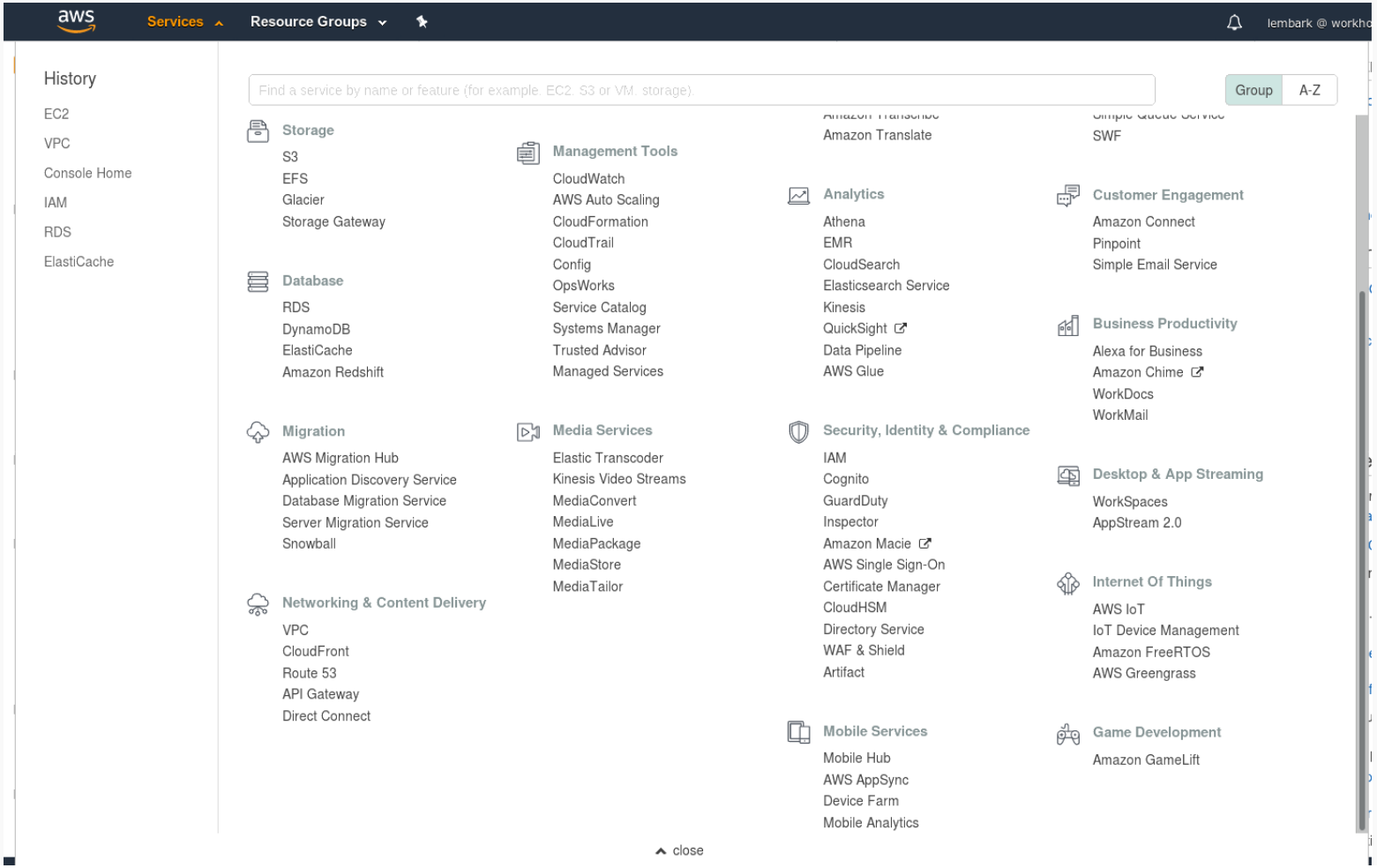
Gateways (“public”).

NAT gateways (“private”).

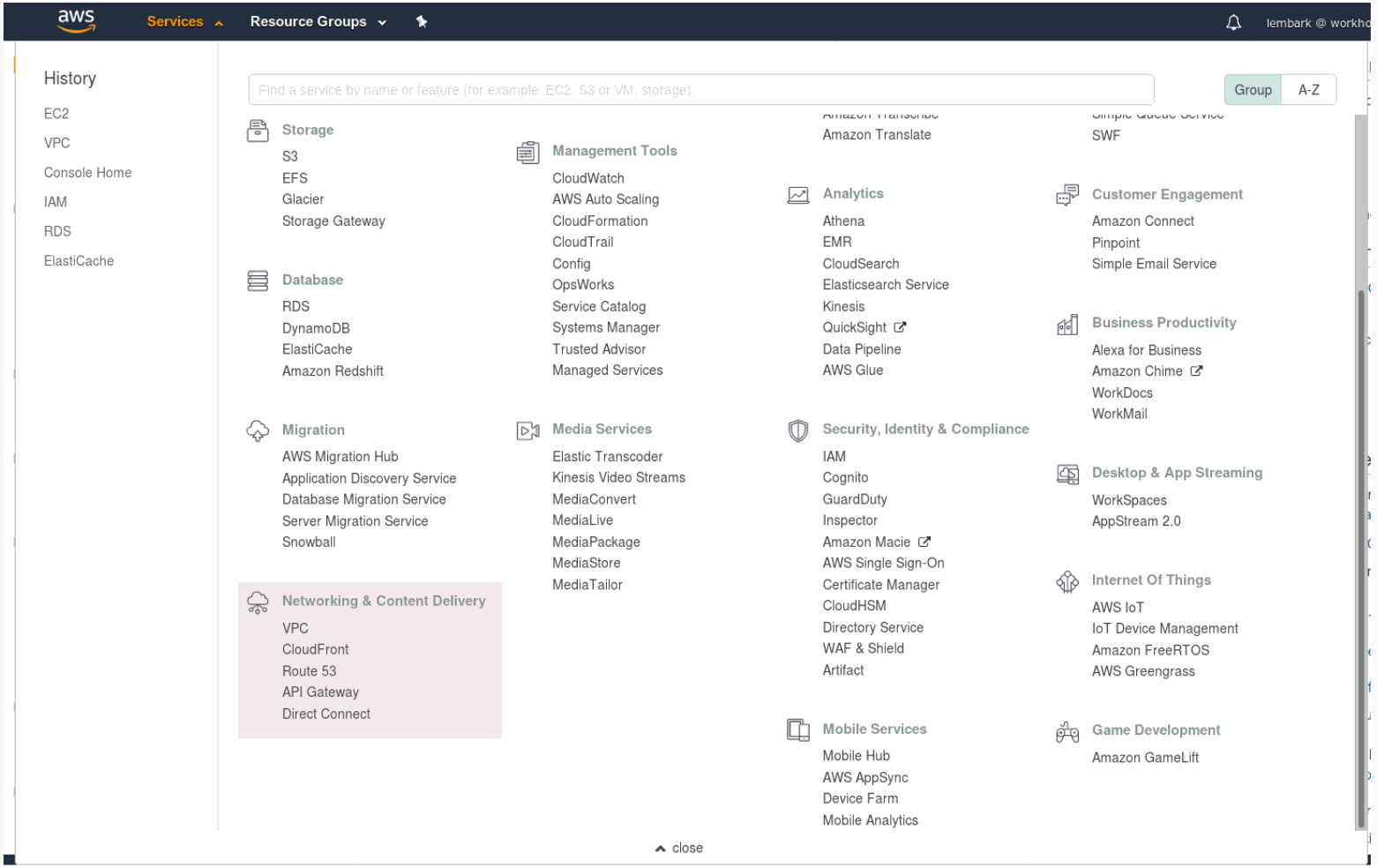
Security rules.



The AWS Console



Networking Options



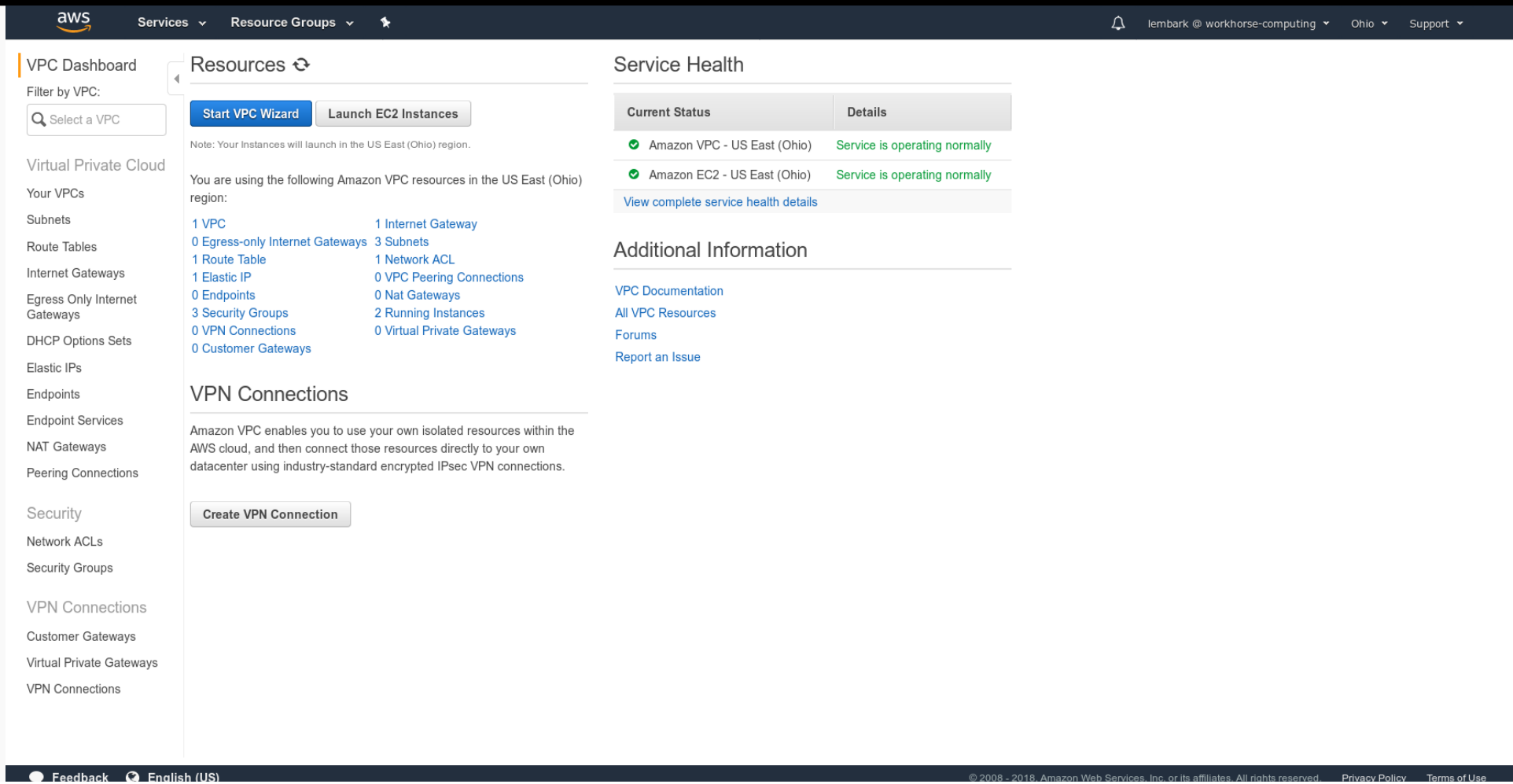
Create your VPC

Multiple VPCs possible.

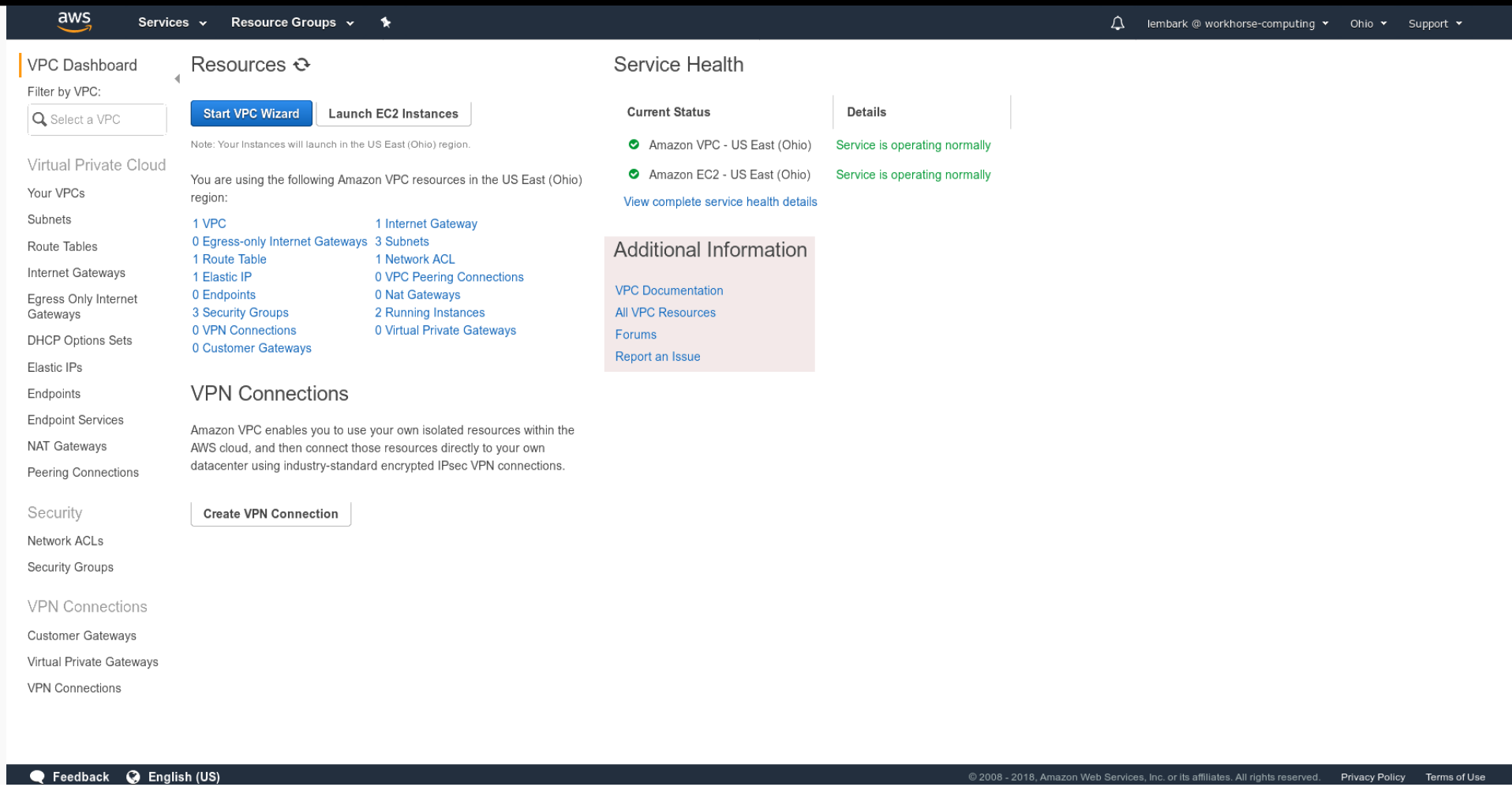
- Different regions
- Per client.
- By use: Dev. vs. QA vs. Prod.
- Free-tier only vs. paid.

Split up to match your use case.

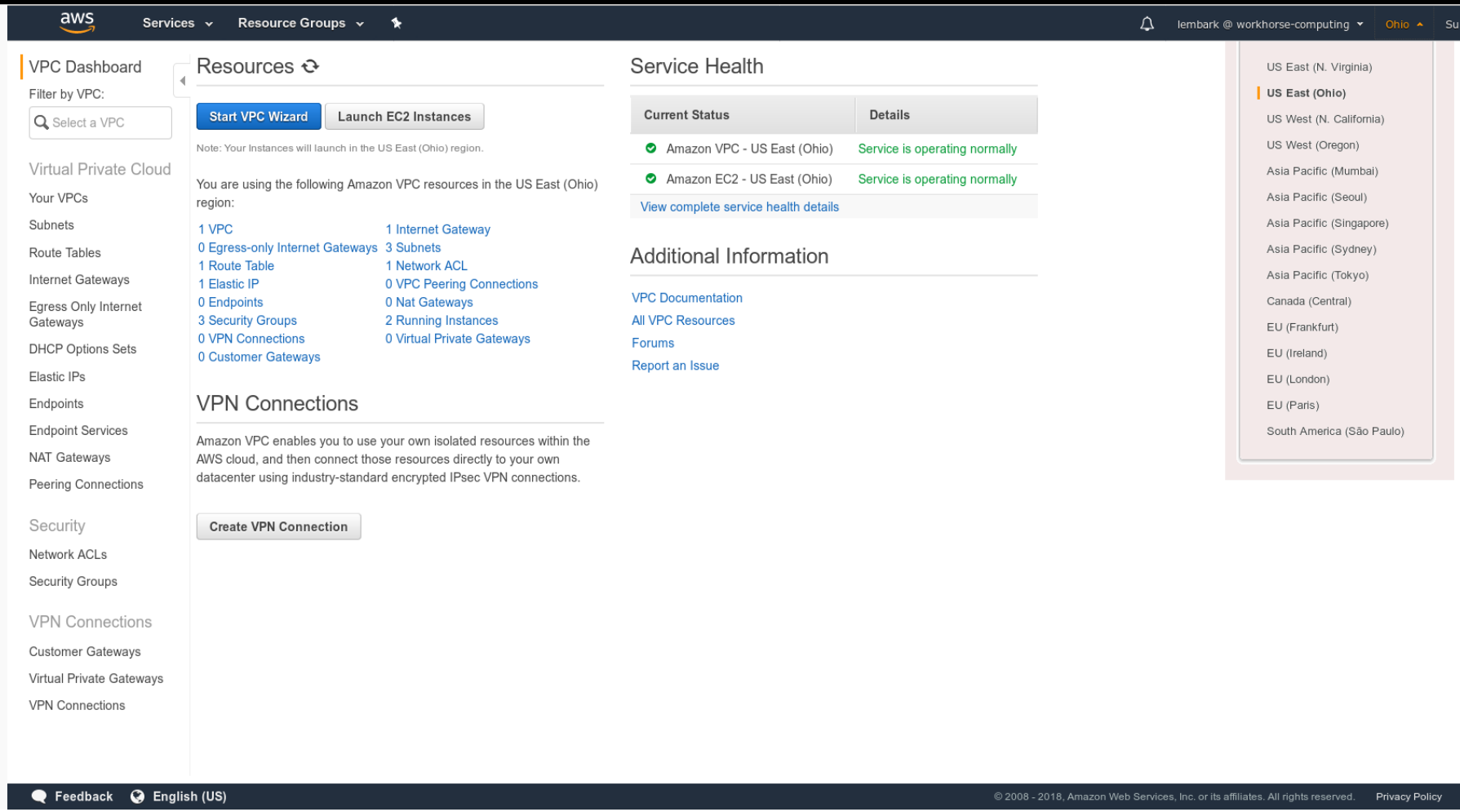
VPC Dashboard



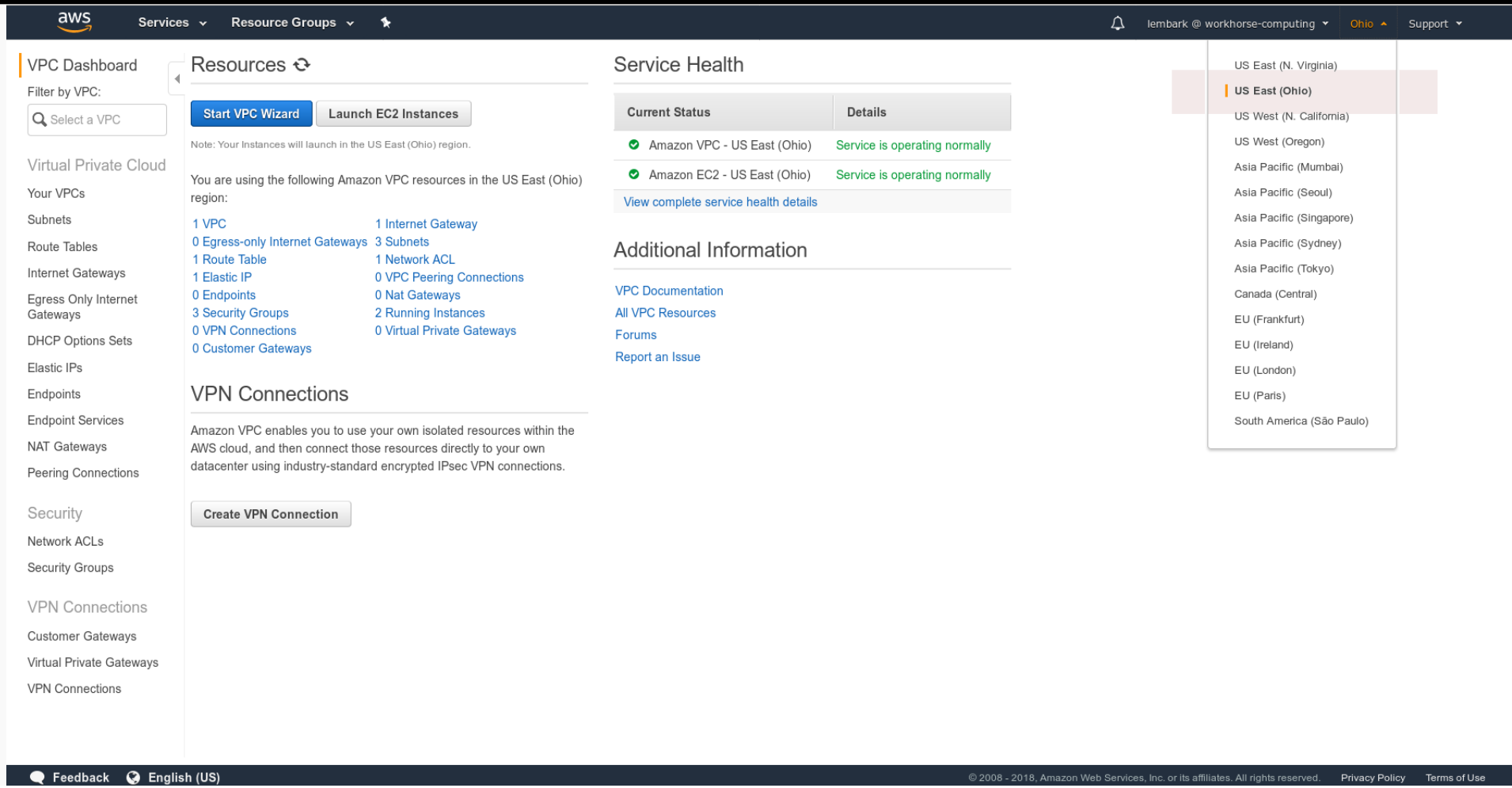
Your best friend



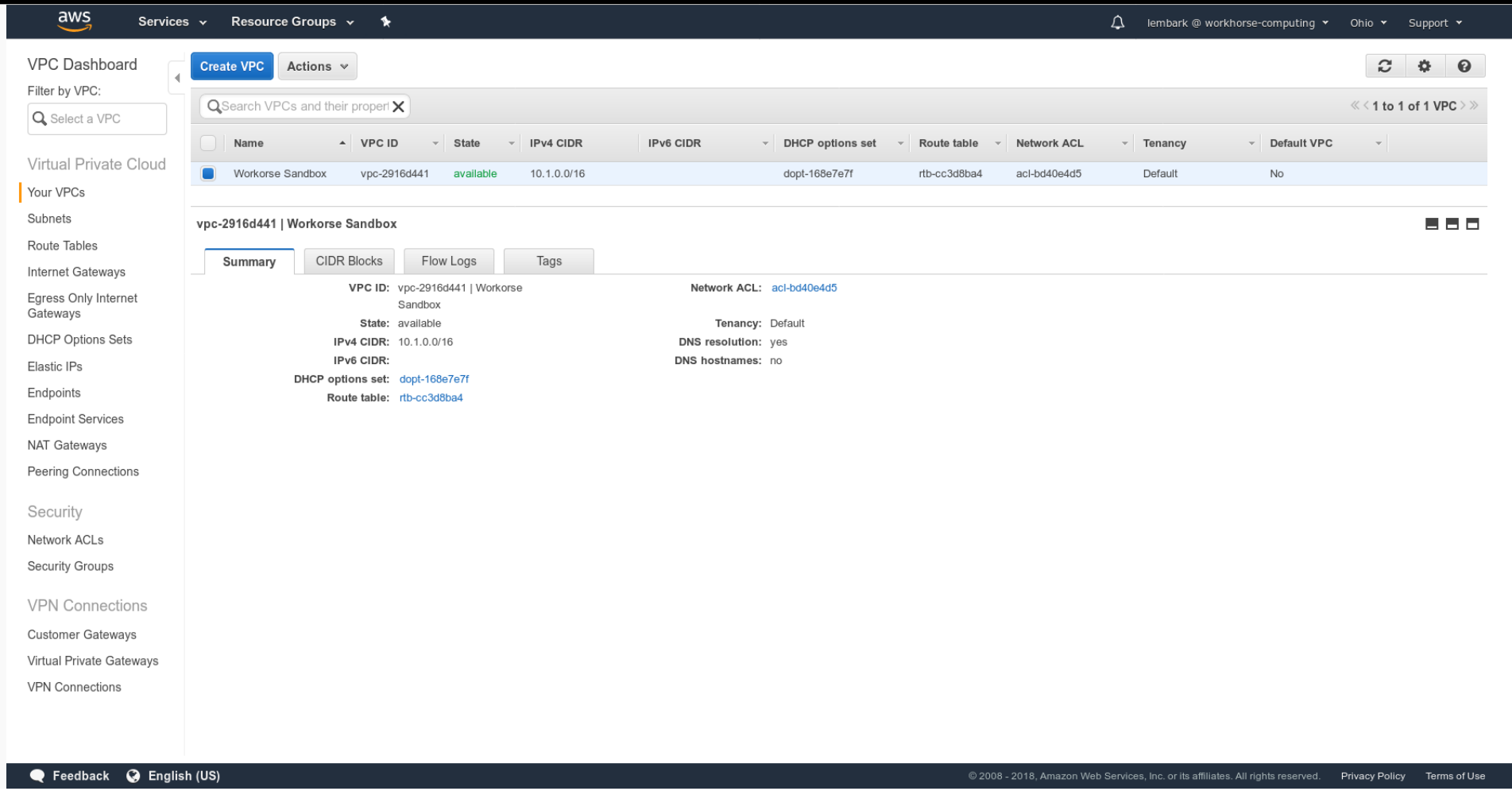
Where ya at?


aws
Services
Resource Groups
lembark @ workhorse-computing
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Resources
Start VPC Wizard
Launch EC2 Instances
Note: Your instances will launch in the US East (Ohio) region.
You are using the following Amazon VPC resources in the US East (Ohio) region:
1 VPC
0 Egress-only Internet Gateways
1 Route Table
1 Elastic IP
0 Endpoints
3 Security Groups
0 VPN Connections
0 Customer Gateways
1 Internet Gateway
3 Subnets
1 Network ACL
0 VPC Peering Connections
0 Nat Gateways
2 Running Instances
0 Virtual Private Gateways
VPN Connections
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.
Create VPN Connection
Service Health
Current Status
Details
Amazon VPC - US East (Ohio)
Service is operating normally
Amazon EC2 - US East (Ohio)
Service is operating normally
View complete service health details
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue
US East (N. Virginia)
US East (Ohio)
US West (N. California)
US West (Oregon)
Asia Pacific (Mumbai)
Asia Pacific (Seoul)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
Canada (Central)
EU (Frankfurt)
EU (Ireland)
EU (London)
EU (Paris)
South America (São Paulo)
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

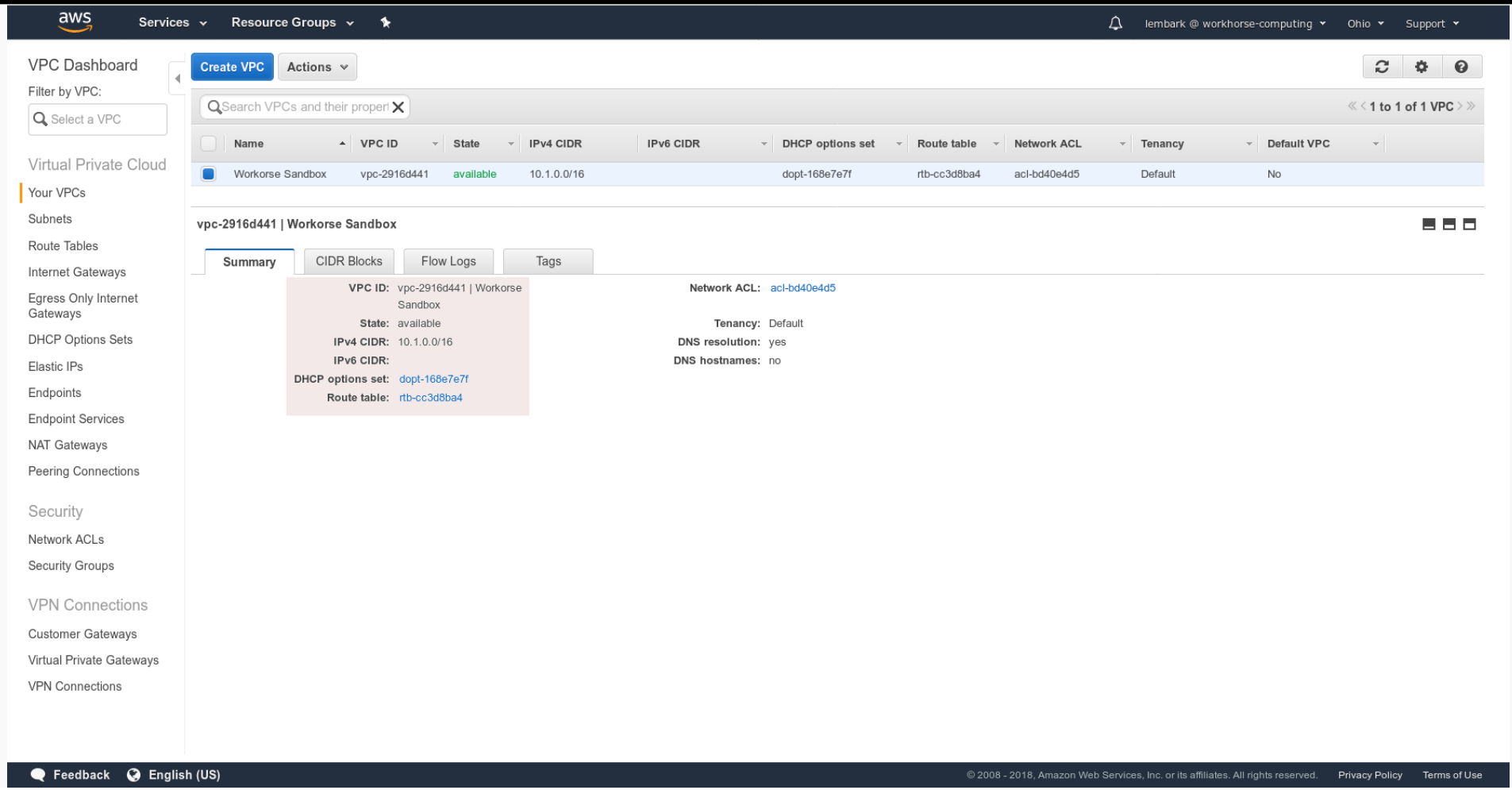
Where ya at?


aws
Services
Resource Groups
lembark @ workhorse-computing
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Resources
Start VPC Wizard
Launch EC2 Instances
Note: Your Instances will launch in the US East (Ohio) region.
You are using the following Amazon VPC resources in the US East (Ohio) region:
1 VPC
0 Egress-only Internet Gateways
1 Route Table
1 Elastic IP
0 Endpoints
3 Security Groups
0 VPN Connections
0 Customer Gateways
1 Internet Gateway
3 Subnets
1 Network ACL
0 VPC Peering Connections
0 Nat Gateways
2 Running Instances
0 Virtual Private Gateways
VPN Connections
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.
Create VPN Connection
Service Health
Current Status
Details
Amazon VPC - US East (Ohio)
Service is operating normally
Amazon EC2 - US East (Ohio)
Service is operating normally
View complete service health details
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue
US East (N. Virginia)
US East (Ohio)
US West (N. California)
US West (Oregon)
Asia Pacific (Mumbai)
Asia Pacific (Seoul)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
Canada (Central)
EU (Frankfurt)
EU (Ireland)
EU (London)
EU (Paris)
South America (São Paulo)
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

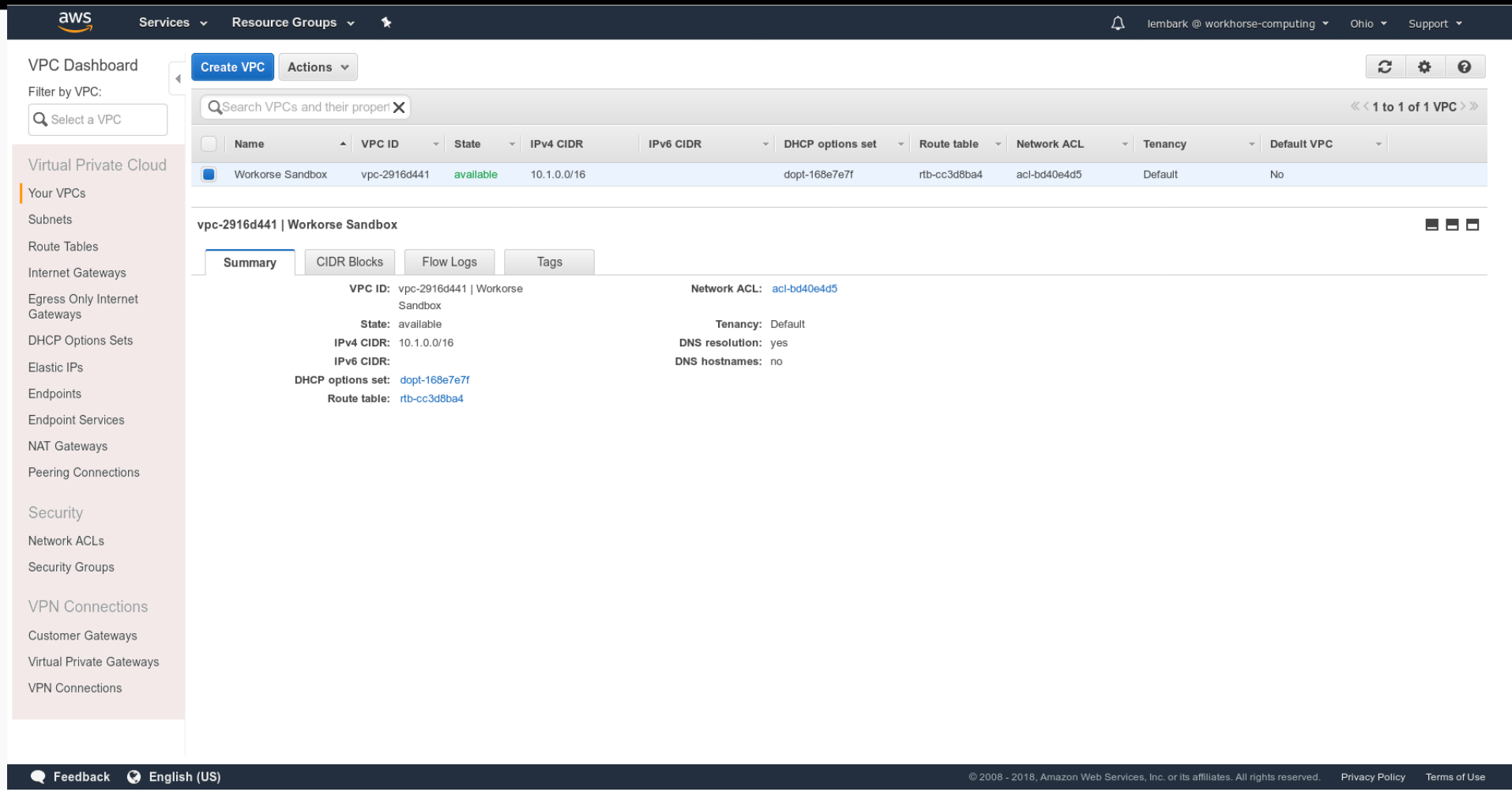
Whatcha got?


aws
Services
Resource Groups
lembark @ workhorse-computing
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create VPC
Actions
Search VPCs and their proper
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
Default VPC
Workorse Sandbox
vpc-2916d441
available
10.1.0.0/16
dopt-168e7e7f
rtb-cc3d8ba4
acl-bd40e4d5
Default
No
vpc-2916d441 | Workorse Sandbox
Summary
CIDR Blocks
Flow Logs
Tags
VPC ID: vpc-2916d441 | Workorse Sandbox
State: available
IPv4 CIDR: 10.1.0.0/16
IPv6 CIDR:
DHCP options set: dopt-168e7e7f
Route table: rtb-cc3d8ba4
Network ACL: acl-bd40e4d5
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

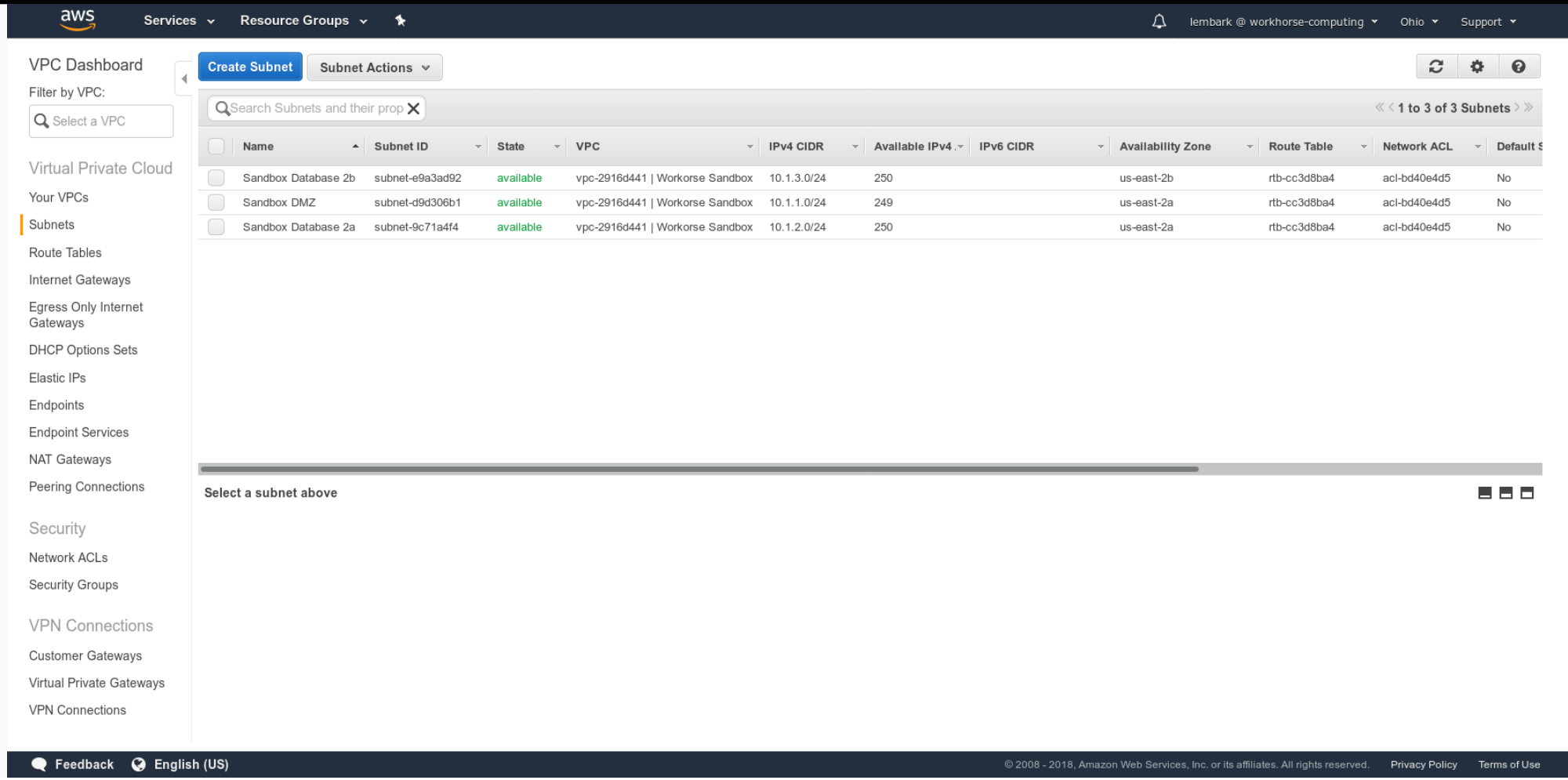
Whatcha got?


aws
Services
Resource Groups
lembark @ workhorse-computing
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create VPC
Actions
Search VPCs and their propert
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
Default VPC
Workorse Sandbox
vpc-2916d441
available
10.1.0.0/16
dopt-168e7e7f
rtb-cc3d8ba4
acl-bd40e4d5
Default
No
vpc-2916d441 | Workorse Sandbox
Summary
CIDR Blocks
Flow Logs
Tags
VPC ID: vpc-2916d441 | Workorse Sandbox
State: available
IPv4 CIDR: 10.1.0.0/16
IPv6 CIDR:
DHCP options set: dopt-168e7e7f
Route table: rtb-cc3d8ba4
Network ACL: acl-bd40e4d5
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

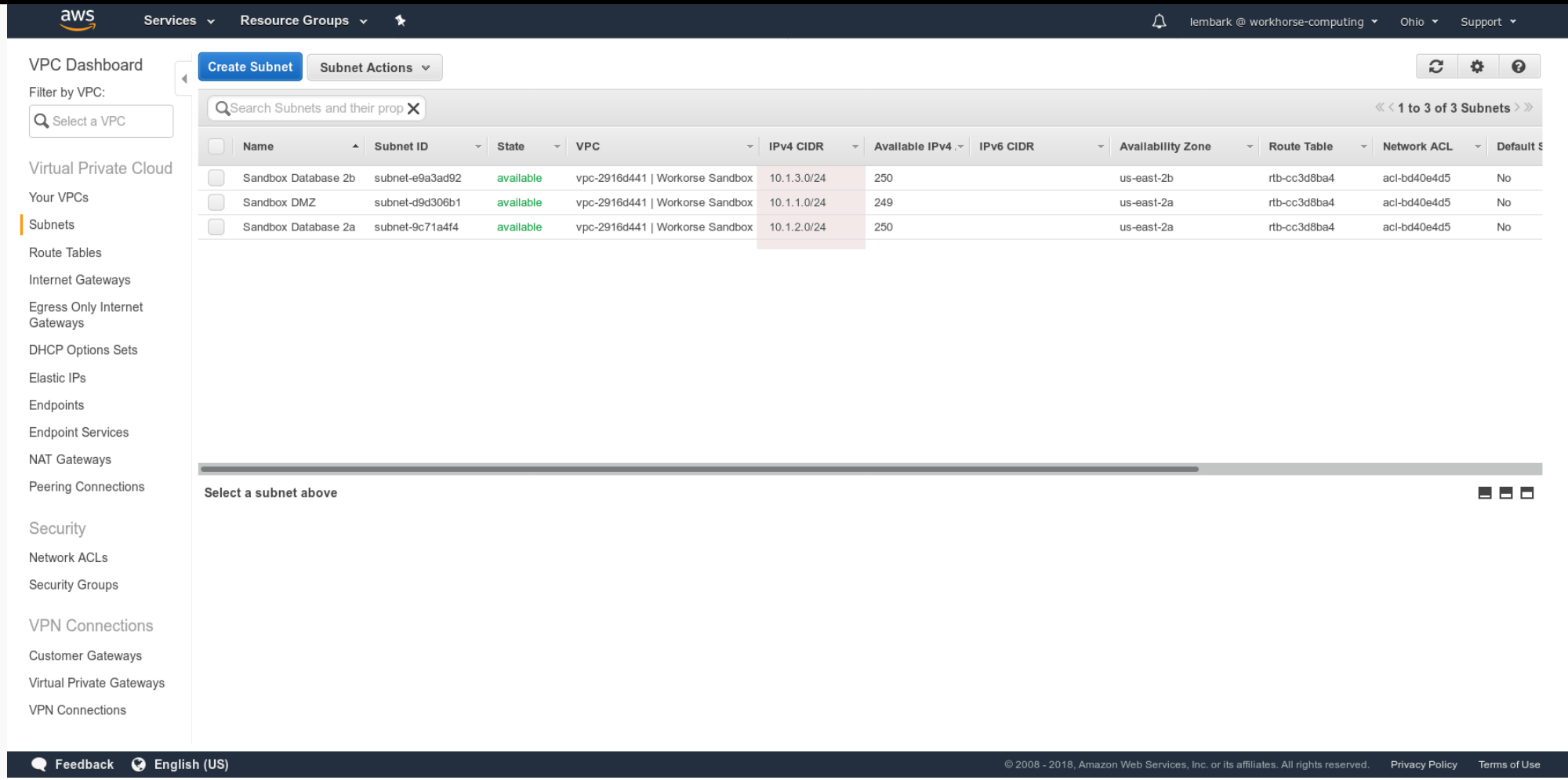
Whatcha doin'?



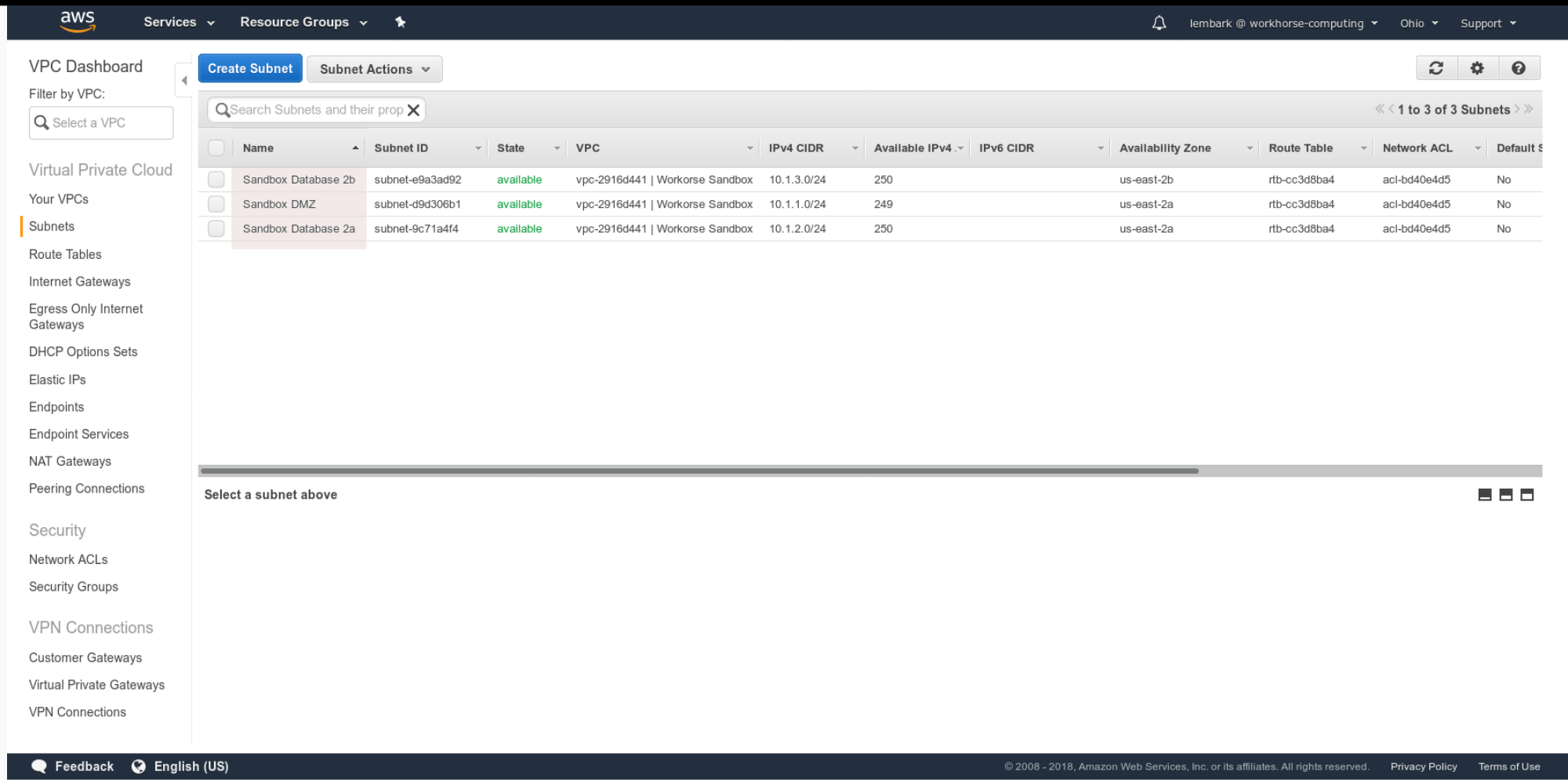
What's inside?



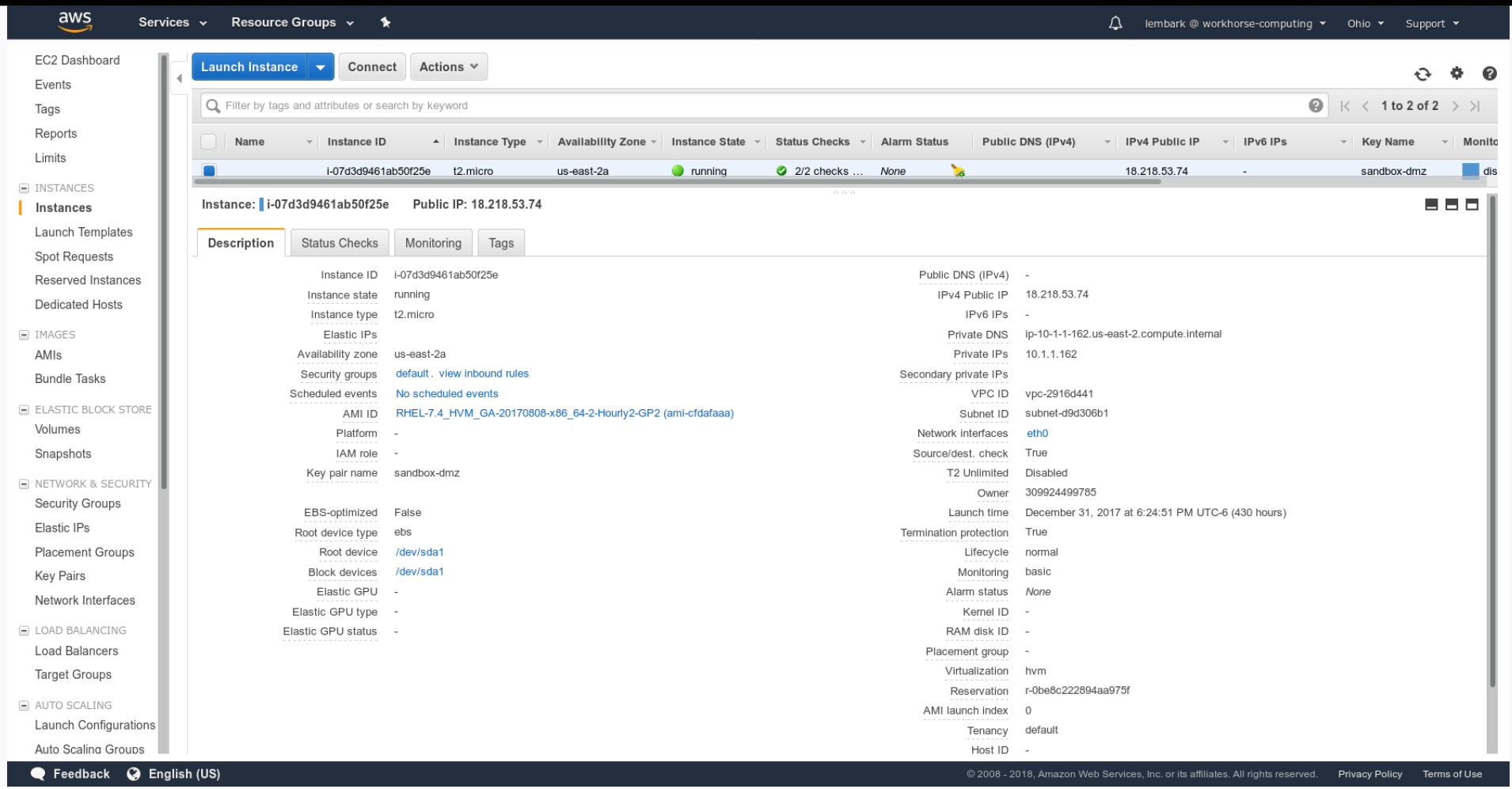
What's inside?



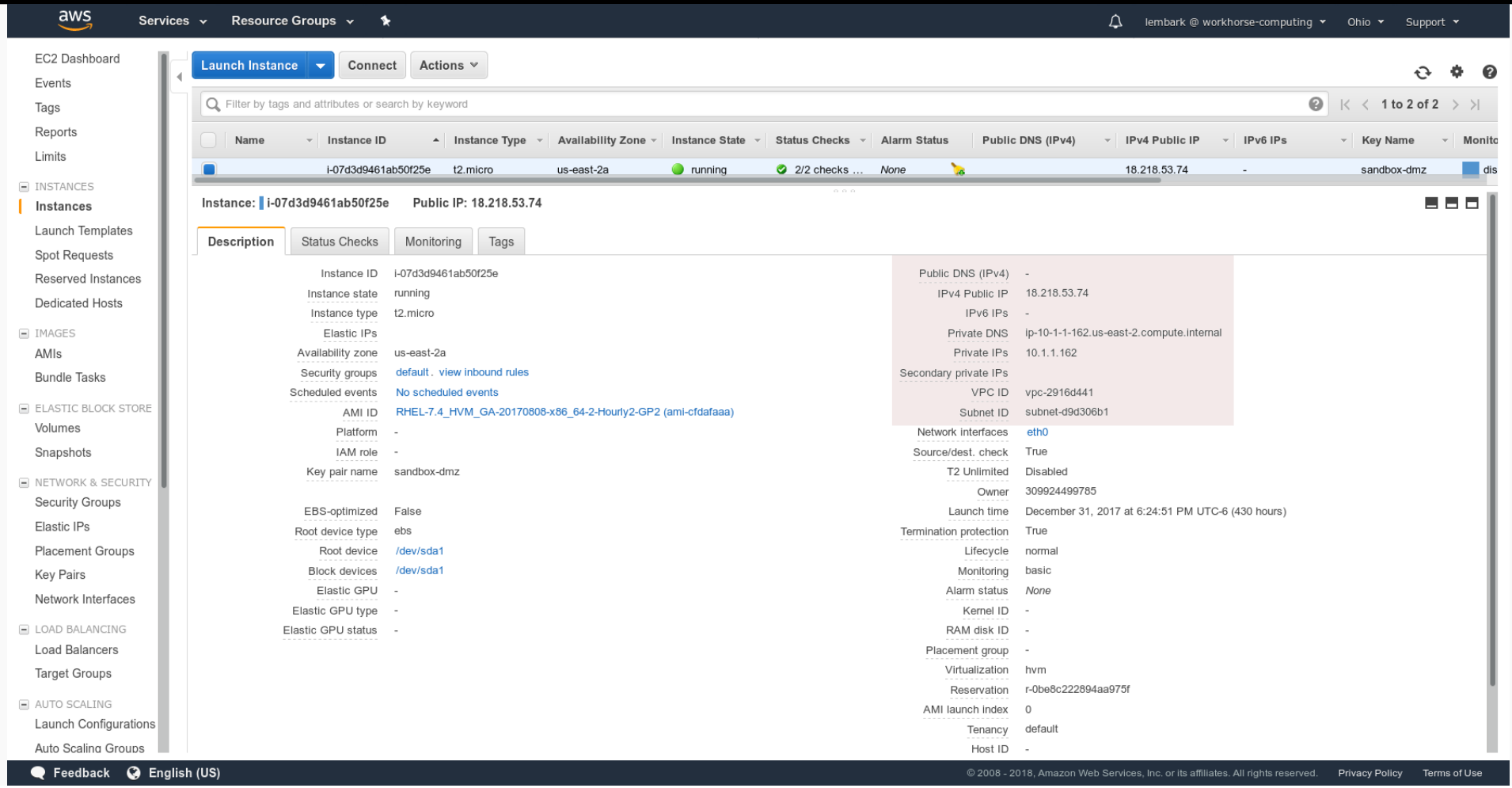
What's inside?



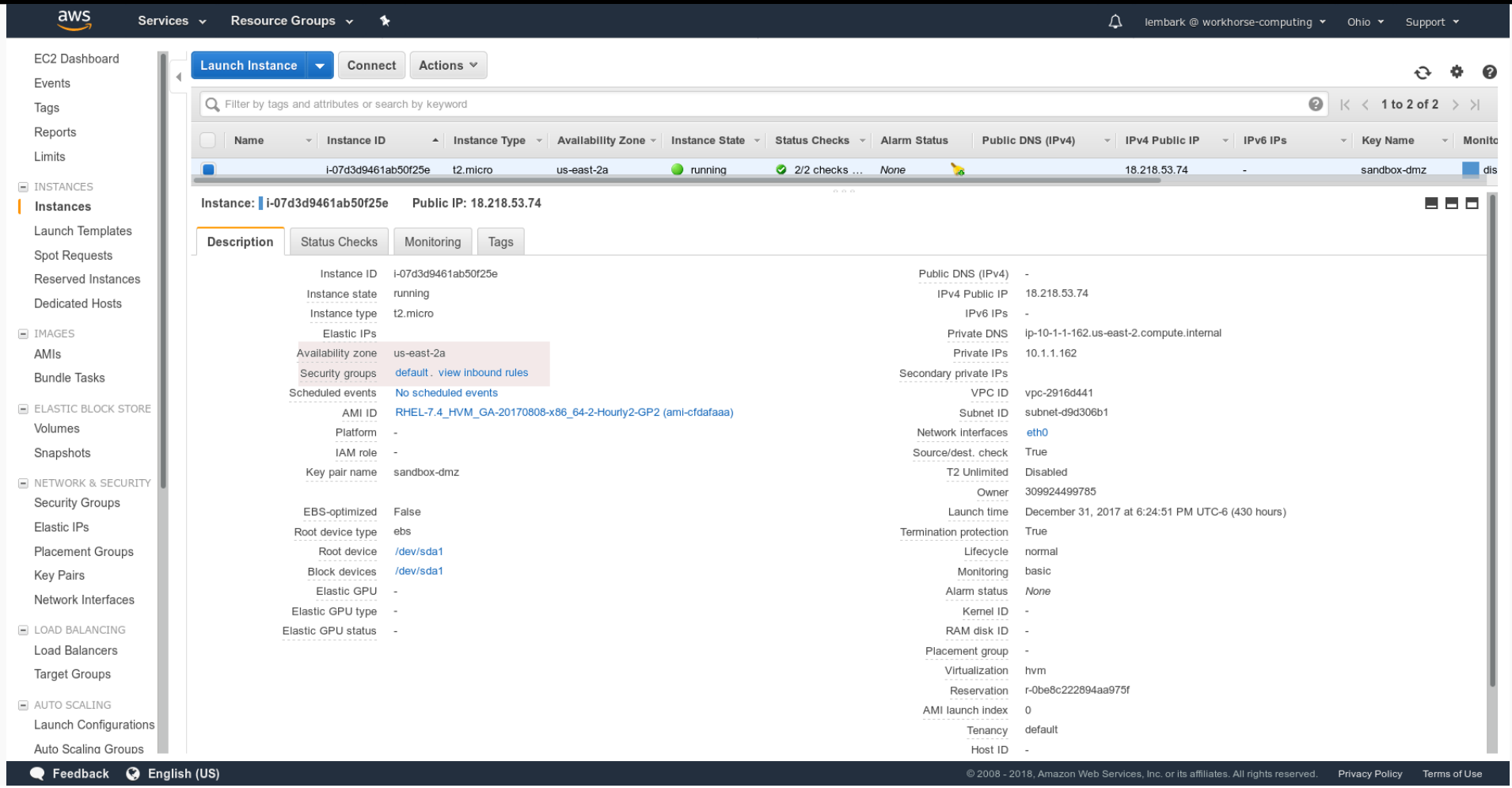
Whatcha running?



Whatcha running?



Whatcha running?



See it for real...

- Create a new VPC.
  - Add subnets.
  - Add security.
  - Start an instance.

Summary

Lots of docs.

VPC starts it all.

- 10.X.0.0/16 good start.

Subnets break up.

- 10.X.Y.0/24 works well.

Availability zones & subnets work together.