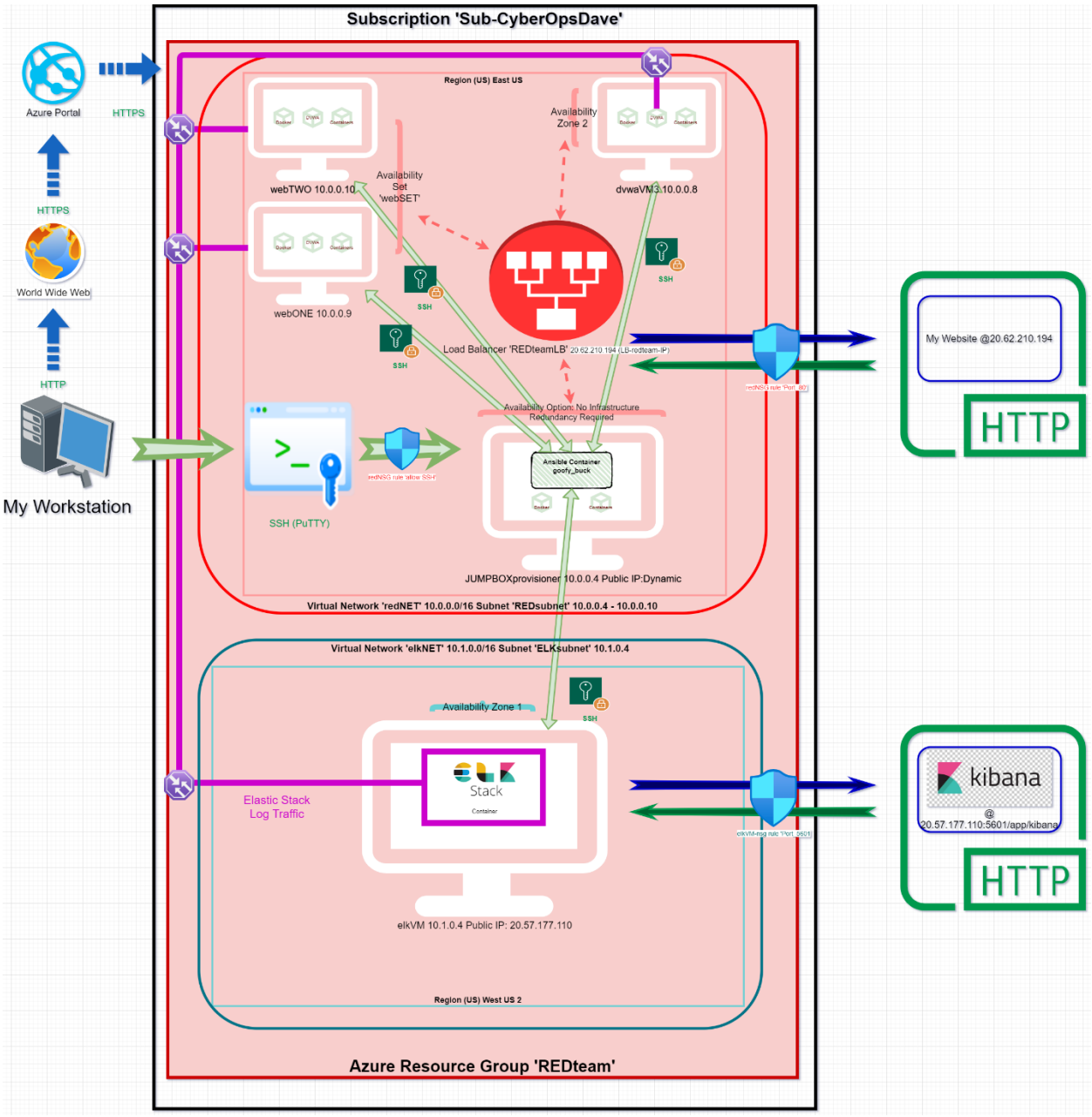
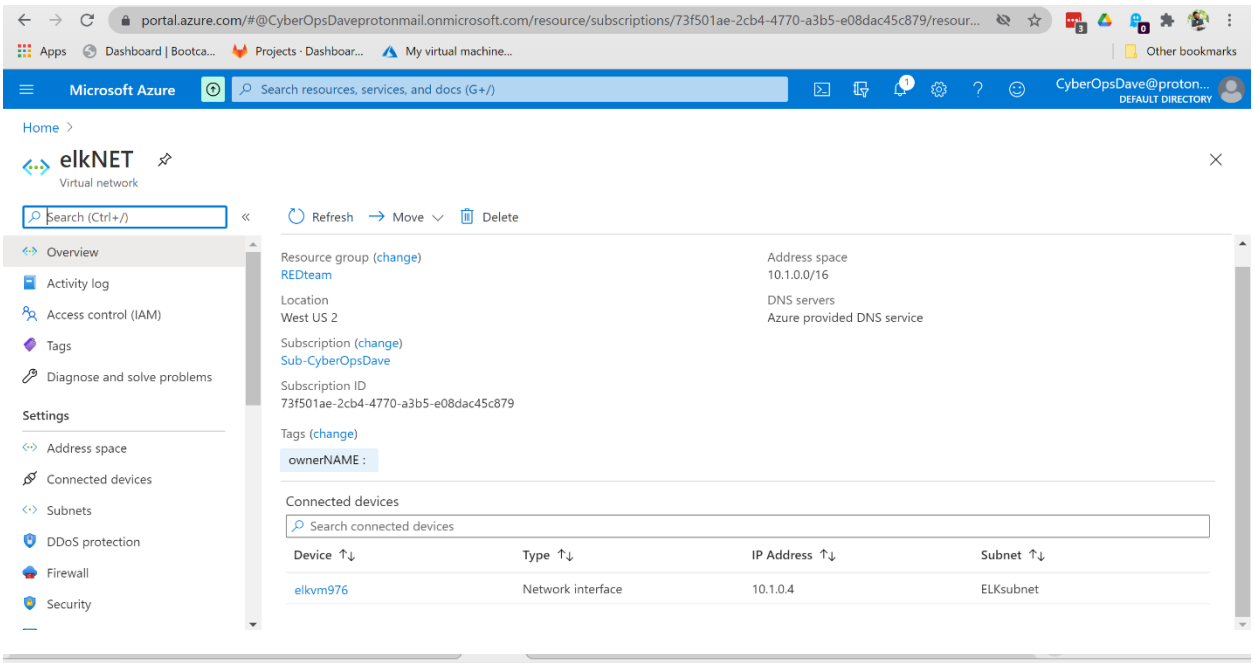
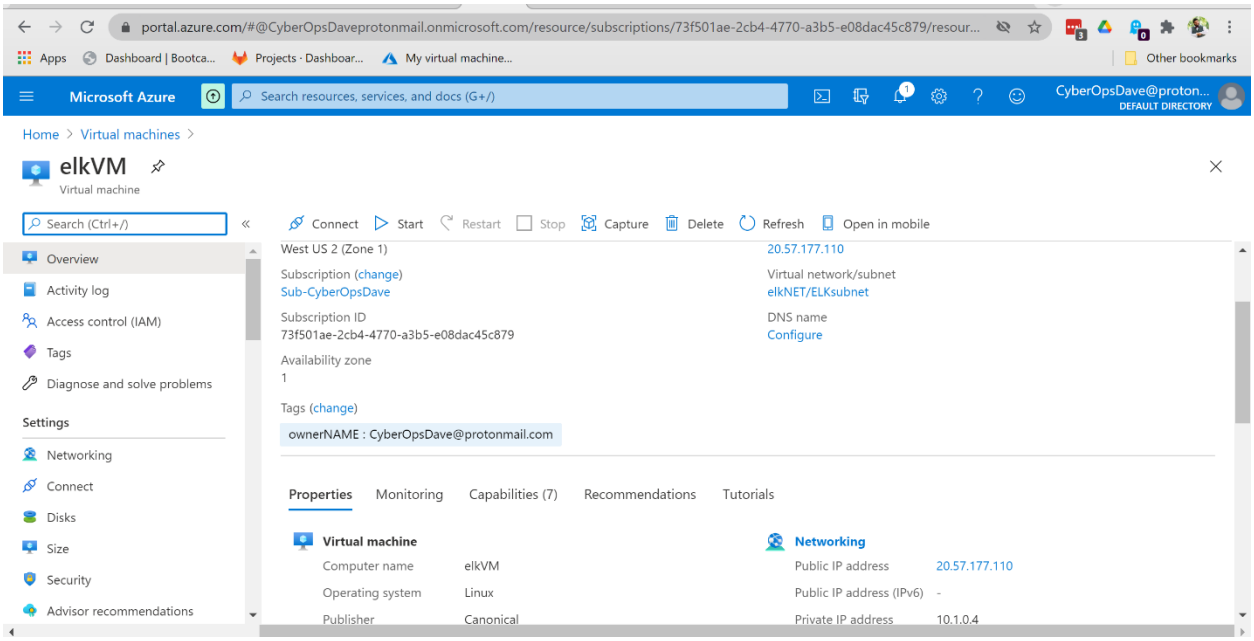
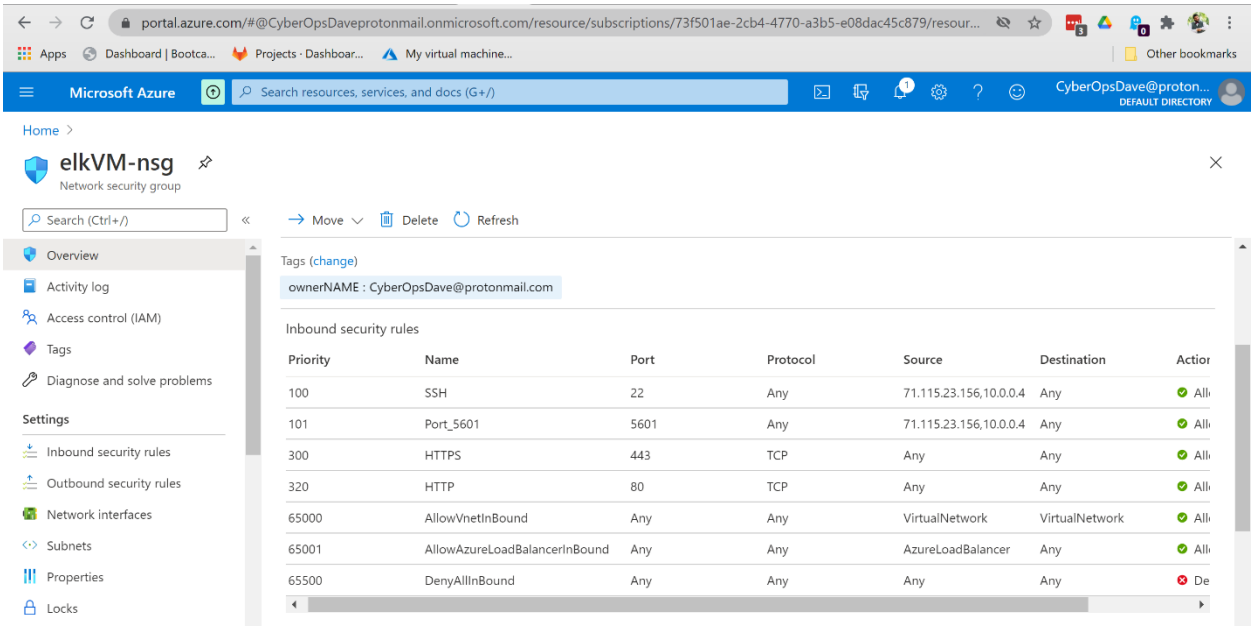
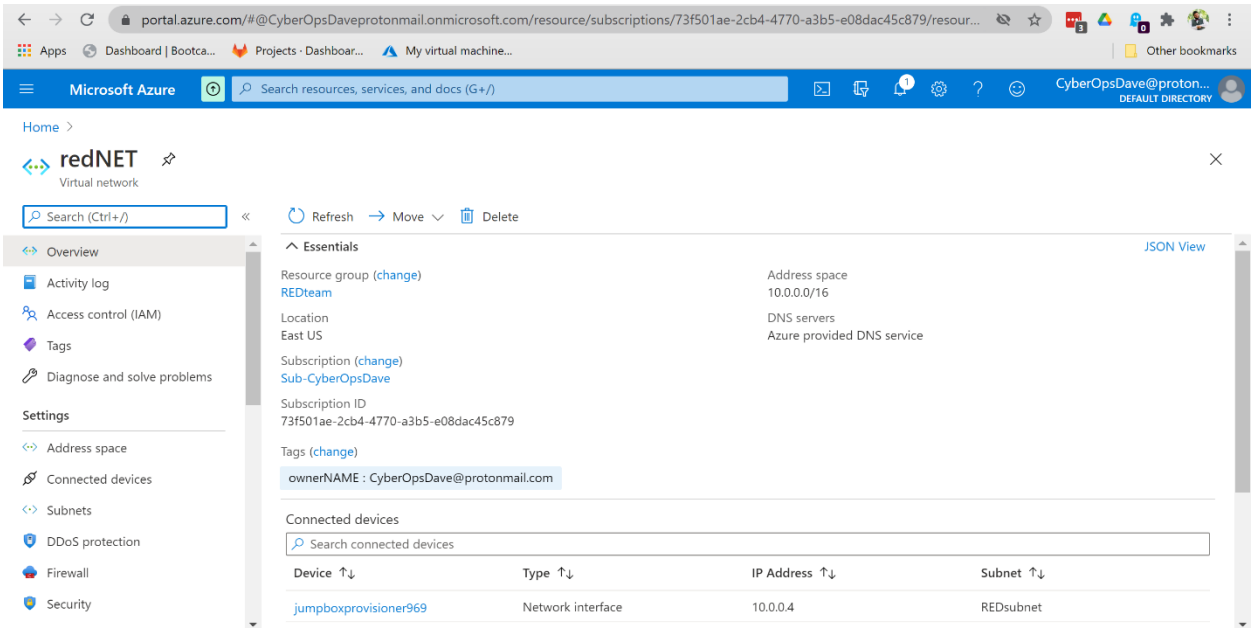
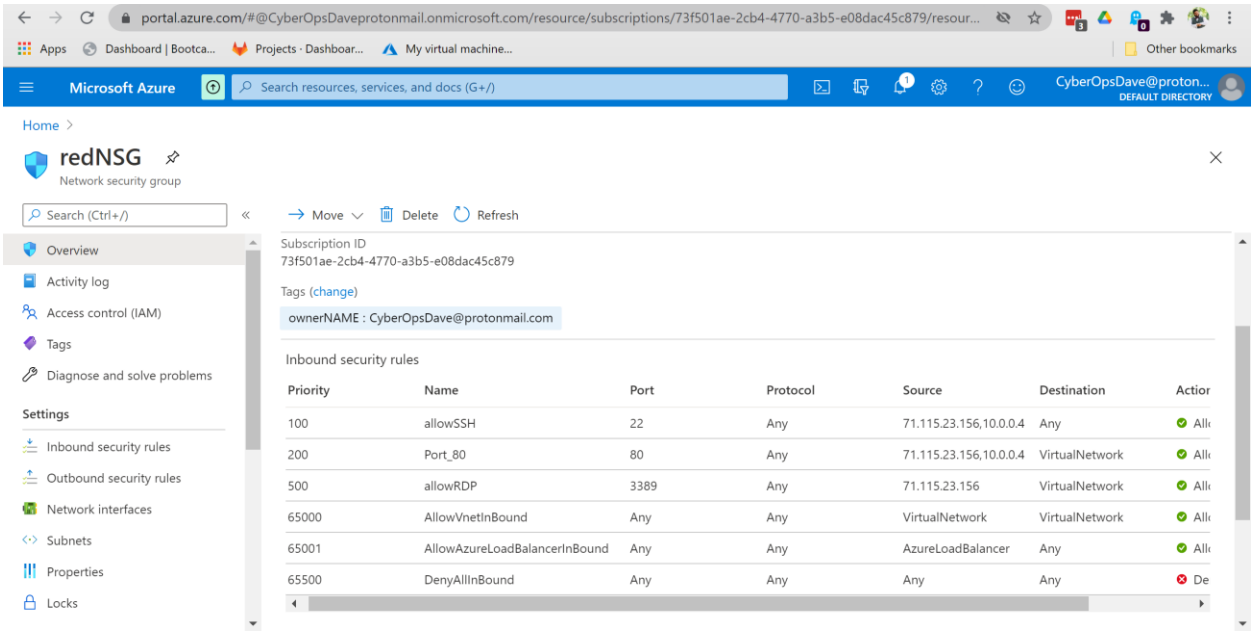

Subscription 'Sub-CyberOpsDave'
Azure Portal
HTTPS
HTTPS
World Wide Web
HTTP
My Workstation
Region (US) East US
Availability Zone 2
webTWO 10.0.0.10
Availability Set 'webSET'
dvwaVM3 10.0.0.8
webONE 10.0.0.9
SSH
SSH
SSH
Load Balancer 'REDteamLB' 20.62.210.194 (LB-redteam-IP)
My Website @20.62.210.194
HTTP
Availability Option: No Infrastructure Redundancy Required
Ansible Container goofy_buck
SSH (PuTTY)
JUMPBOXprovisioner 10.0.0.4 Public IP:Dynamic
Virtual Network 'redNET' 10.0.0.0/16 Subnet 'REDsubnet' 10.0.0.4 - 10.0.0.10
Virtual Network 'elkNET' 10.1.0.0/16 Subnet 'ELKsubnet' 10.1.0.4
Availability Zone 1
SSH
Elastic Stack
Log Traffic
Stack
Container
kibana
@
20.57.177.110:5601/app/kibana
HTTP
elkVM 10.1.0.4 Public IP: 20.57.177.110
Region (US) West US 2
Azure Resource Group 'REDteam'

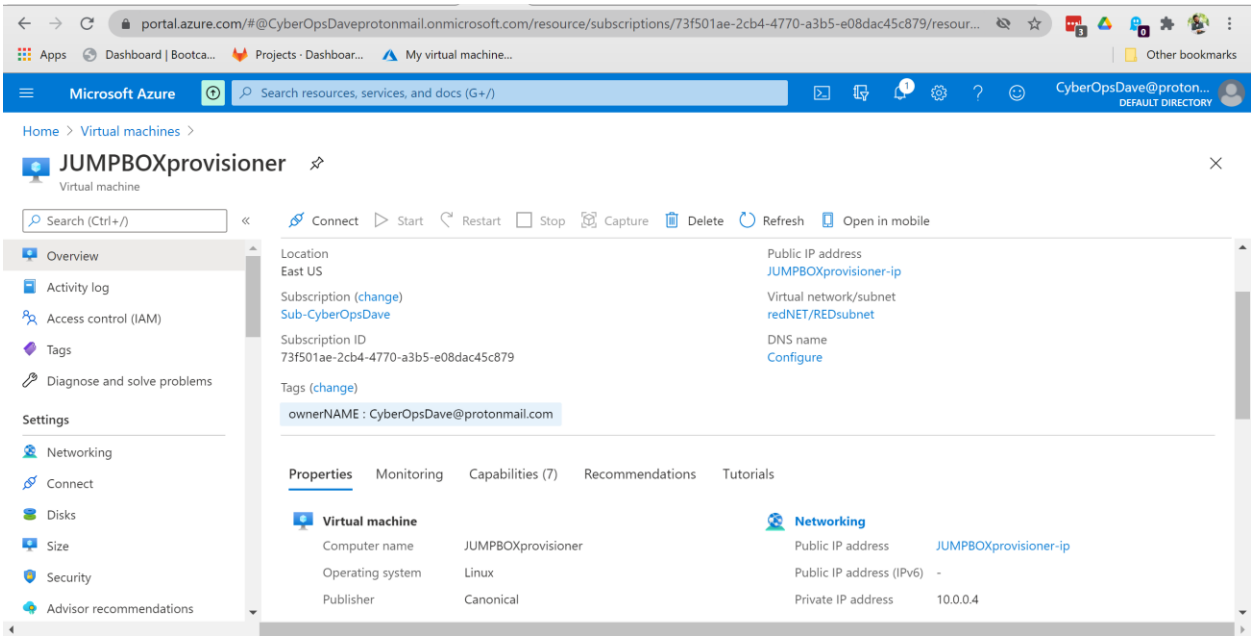

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
elkNET
Virtual network
Search (Ctrl+/)
Refresh
Move
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
Resource group (change)
REDteam
Location
West US 2
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Tags (change)
ownerNAME :
Address space
10.1.0.0/16
DNS servers
Azure provided DNS service
Connected devices
Search connected devices
Device
Type
IP Address
Subnet
elkvm976
Network interface
10.1.0.4
ELKsubnet

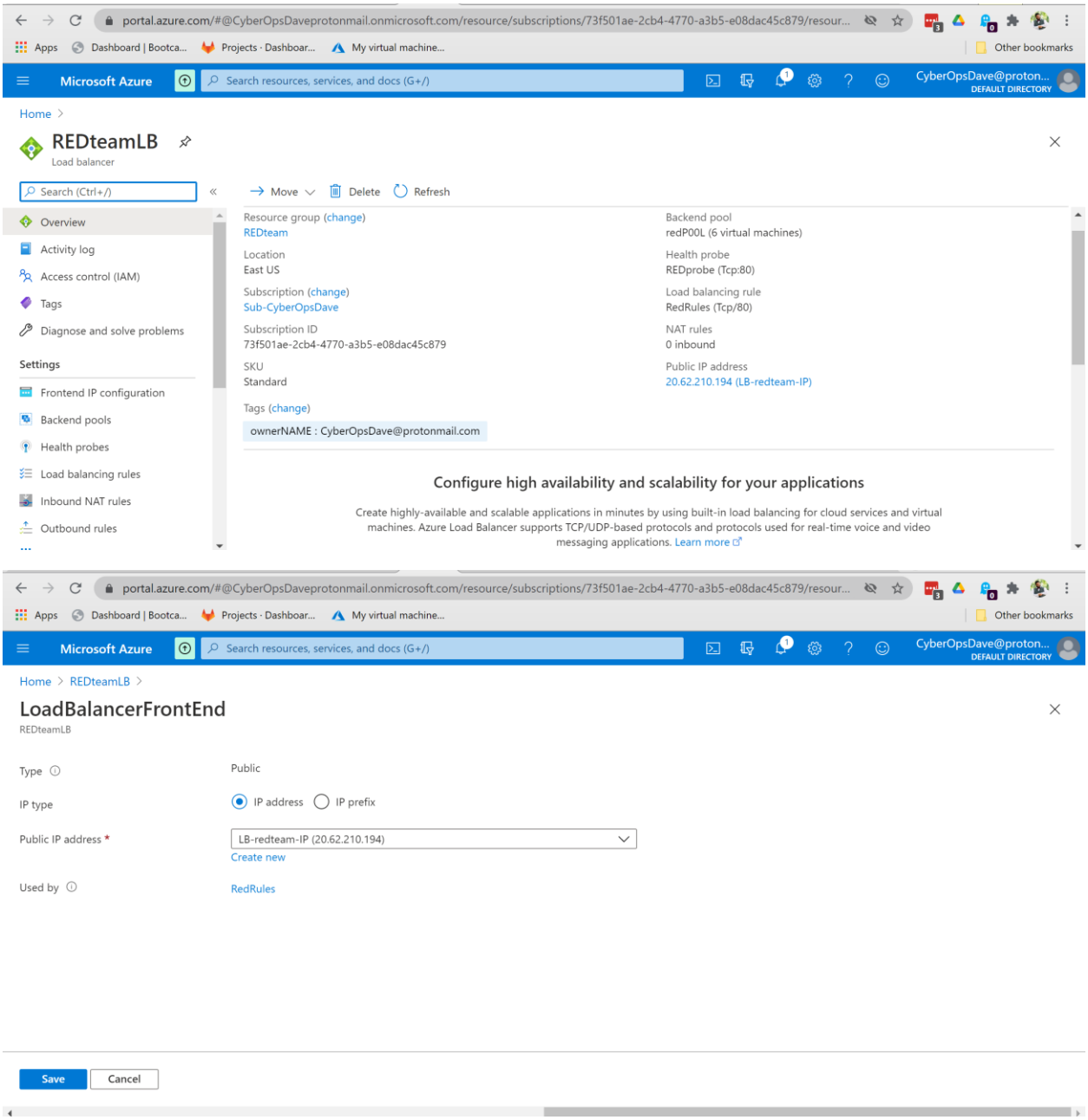

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
Virtual machines
elkVM
Virtual machine
Search (Ctrl+/)
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
West US 2 (Zone 1)
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Availability zone
1
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
20.57.177.110
Virtual network/subnet
elkNET/ELKsubnet
DNS name
Configure
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name
elkVM
Operating system
Linux
Publisher
Canonical
Networking
Public IP address
20.57.177.110
Public IP address (IPv6)
-
Private IP address
10.1.0.4


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
elkVM-nsg
Network security group
Search (Ctrl+/)
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Inbound security rules
Priority Name Port Protocol Source Destination Actior
100 SSH 22 Any 71.115.23.156,10.0.0.4 Any All
101 Port_5601 5601 Any 71.115.23.156,10.0.0.4 Any All
300 HTTPS 443 TCP Any Any All
320 HTTP 80 TCP Any Any All
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork All
65001 AllowAzureLoadBalancerInBound Any Any AzureLoadBalancer Any All
65500 DenyAllInBound Any Any Any Any De

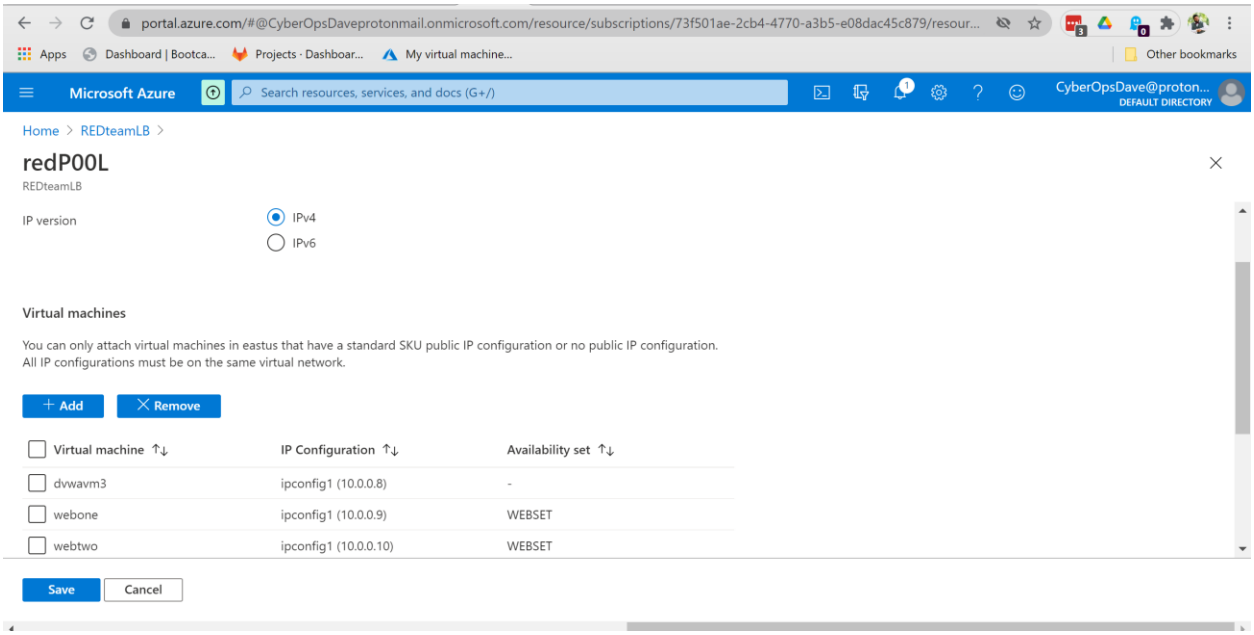

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
redNET
Virtual network
Search (Ctrl+/)
Refresh
Move
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
Essentials
JSON View
Resource group (change)
REDteam
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Address space
10.0.0.0/16
DNS servers
Azure provided DNS service
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Connected devices
Search connected devices
Device Type IP Address Subnet
jumpboxprovisioner969 Network interface 10.0.0.4 REDsubnet

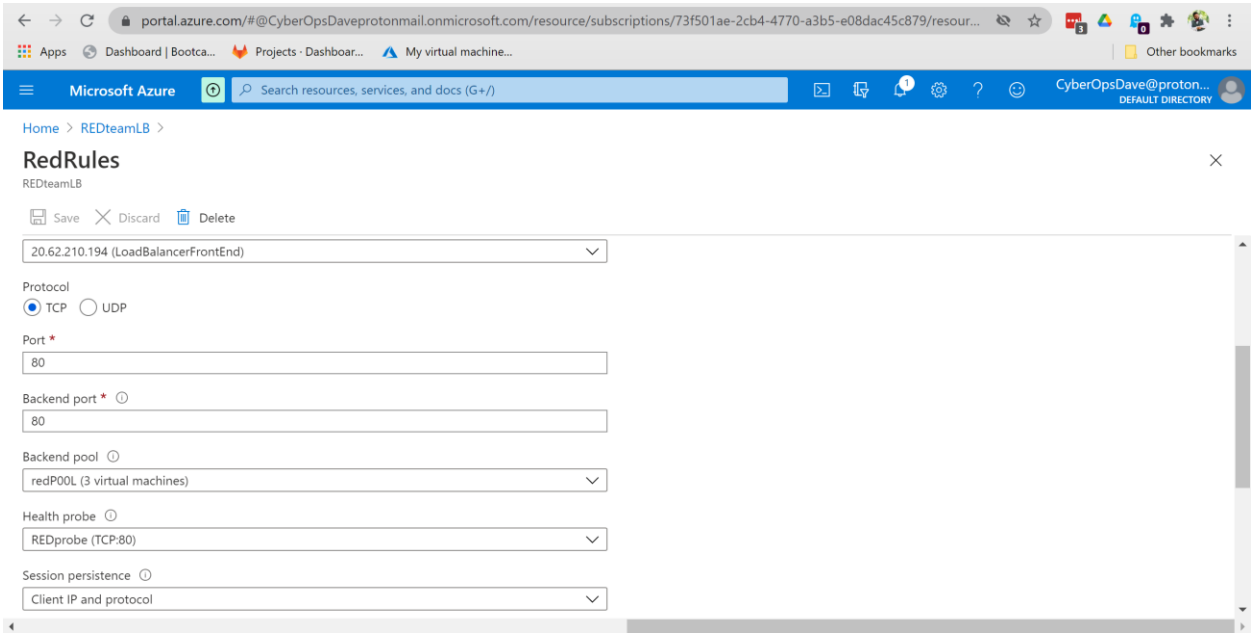

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
redNSG
Network security group
Search (Ctrl+/)
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Inbound security rules
Priority
Name
Port
Protocol
Source
Destination
Actior
100
allowSSH
22
Any
71.115.23.156,10.0.0.4
Any
200
Port_80
80
Any
71.115.23.156,10.0.0.4
VirtualNetwork
500
allowRDP
3389
Any
71.115.23.156
VirtualNetwork
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
Any
65500
DenyAllInBound
Any
Any
Any
Any

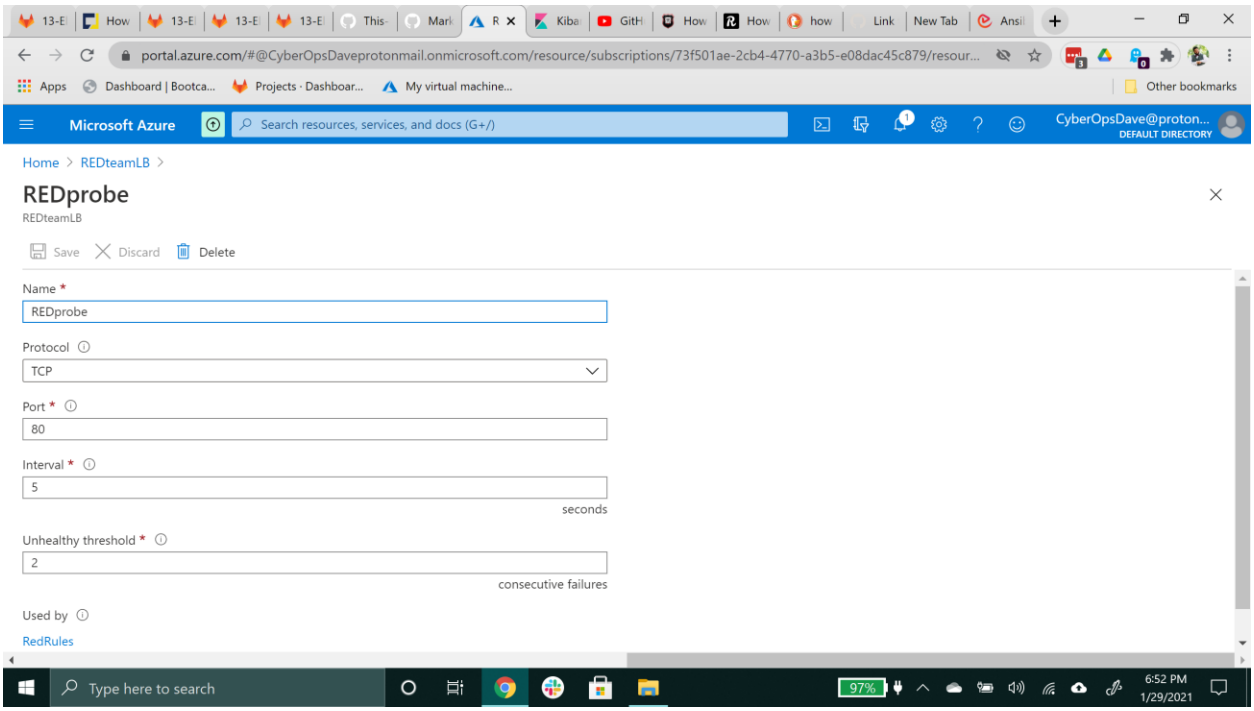

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
Virtual machines
JUMPBOXprovisioner
Virtual machine
Search (Ctrl+/)
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Public IP address
JUMPBOXprovisioner-ip
Virtual network/subnet
redNET/REDsubnet
DNS name
Configure
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name
JUMPBOXprovisioner
Operating system
Linux
Publisher
Canonical
Networking
Public IP address
JUMPBOXprovisioner-ip
Public IP address (IPv6)
-
Private IP address
10.0.0.4

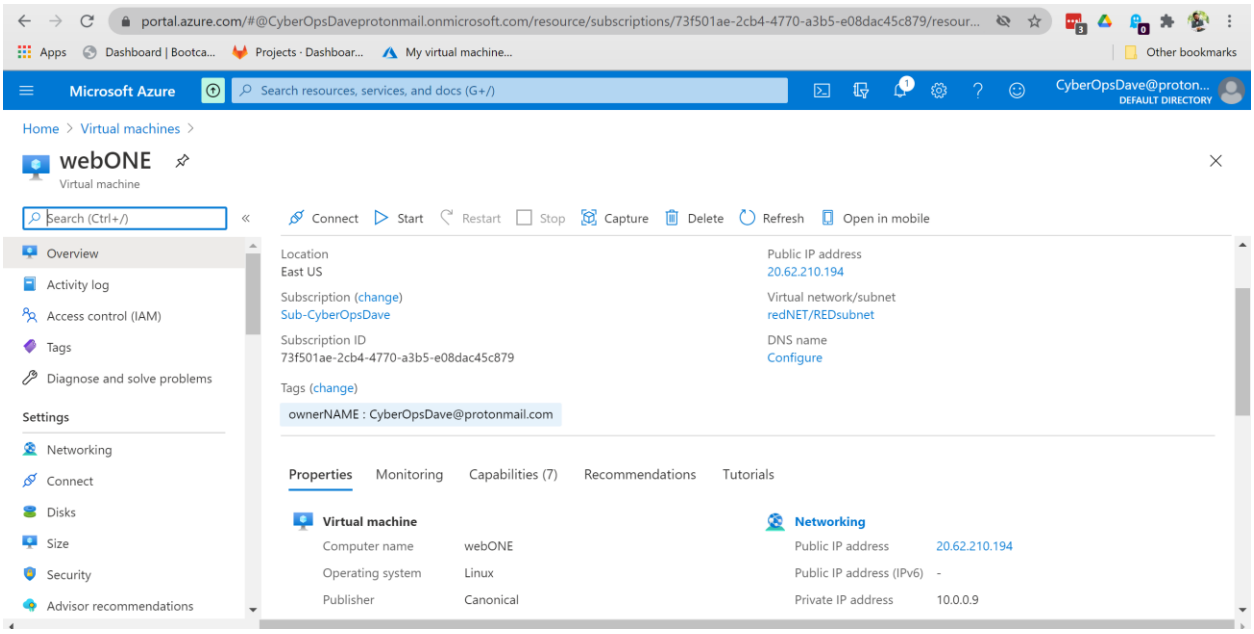

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
REDteamLB
Load balancer
Search (Ctrl+/)
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Frontend IP configuration
Backend pools
Health probes
Load balancing rules
Inbound NAT rules
Outbound rules
Resource group (change)
REDteam
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
SKU
Standard
Backend pool
redP00L (6 virtual machines)
Health probe
REDprobe (Tcp:80)
Load balancing rule
RedRules (Tcp/80)
NAT rules
0 inbound
Public IP address
20.62.210.194 (LB-redteam-IP)
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Configure high availability and scalability for your applications
Create highly-available and scalable applications in minutes by using built-in load balancing for cloud services and virtual machines. Azure Load Balancer supports TCP/UDP-based protocols and protocols used for real-time voice and video messaging applications. Learn more

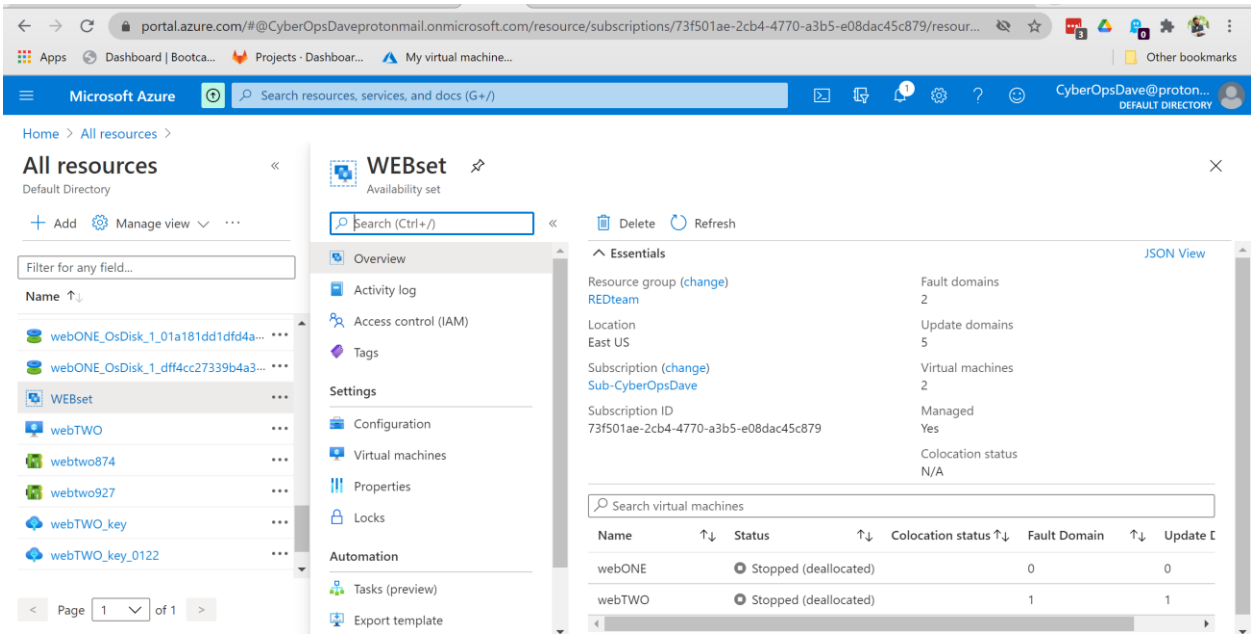
portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home
REDteamLB
LoadBalancerFrontEnd
REDteamLB
Type
Public
IP type
IP address
IP prefix
Public IP address *
LB-redteam-IP (20.62.210.194)
Create new
Used by
RedRules
Save
Cancel

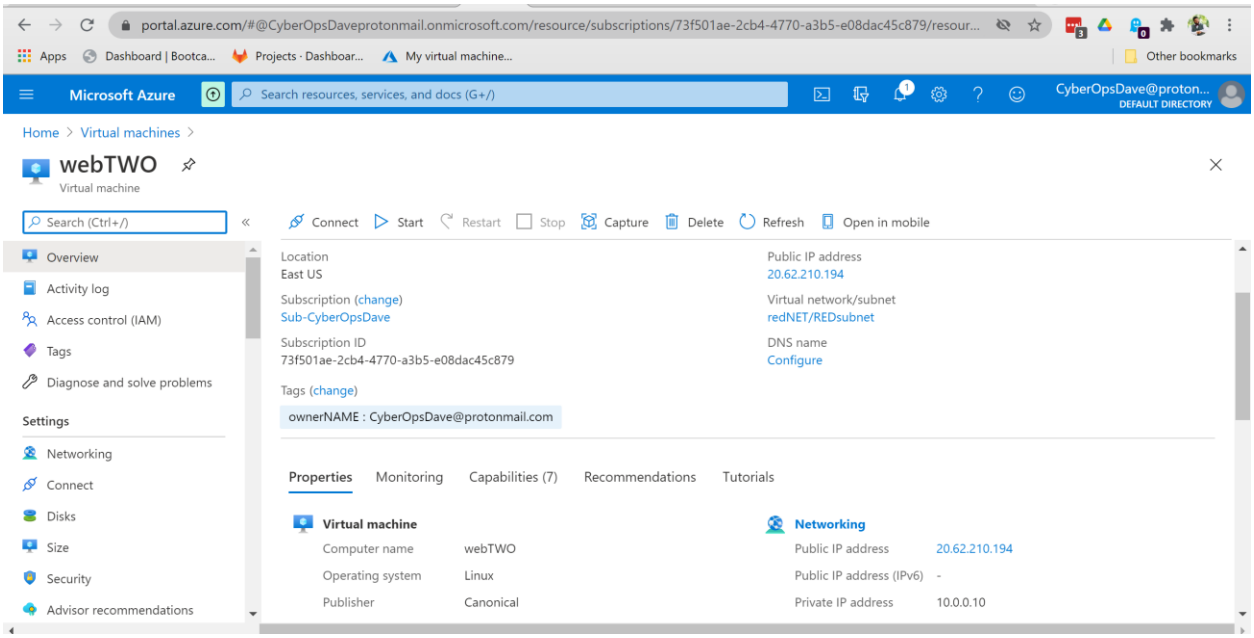

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > REDteamLB >
redP00L
REDteamLB
IP version
IPv4
IPv6
Virtual machines
You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration.
All IP configurations must be on the same virtual network.
+ Add
Remove
Virtual machine
IP Configuration
Availability set
dvwavm3
ipconfig1 (10.0.0.8)
-
webone
ipconfig1 (10.0.0.9)
WEBSET
webtwo
ipconfig1 (10.0.0.10)
WEBSET
Save
Cancel

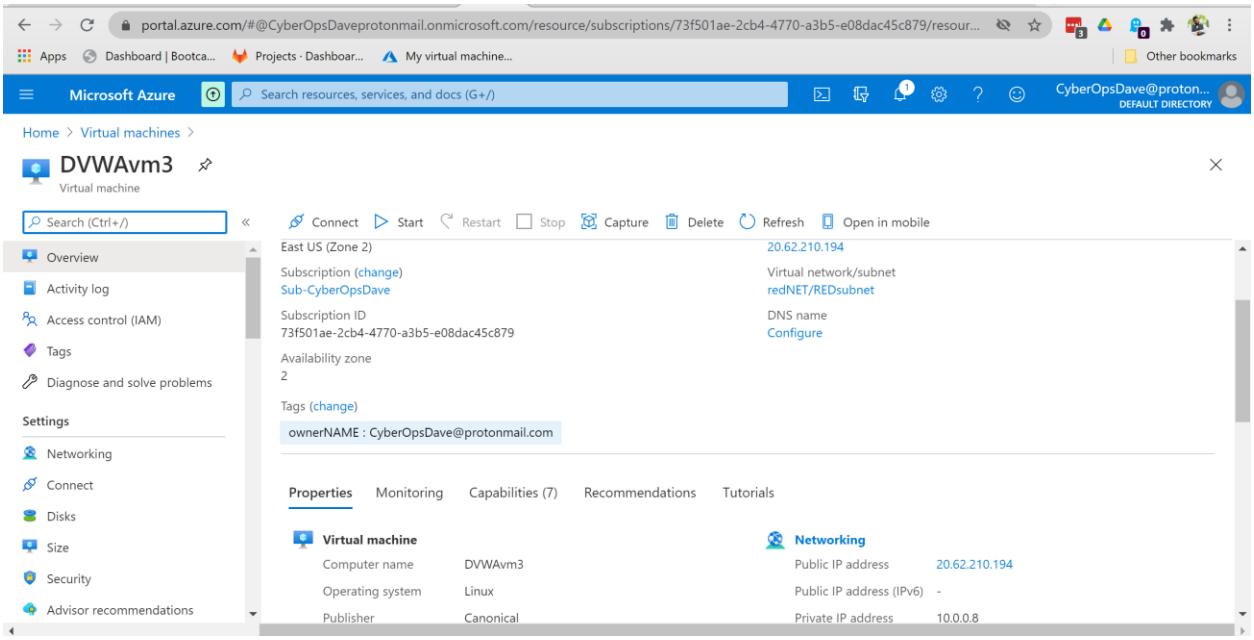

portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > REDteamLB >
RedRules
REDteamLB
Save
Discard
Delete
20.62.210.194 (LoadBalancerFrontEnd)
Protocol
TCP
UDP
Port *
80
Backend port *
80
Backend pool
redP00L (3 virtual machines)
Health probe
REDprobe (TCP:80)
Session persistence
Client IP and protocol


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > REDteamLB >
REDprobe
REDteamLB
Save
Discard
Delete
Name *
REDprobe
Protocol
TCP
Port *
80
Interval *
5
seconds
Unhealthy threshold *
2
consecutive failures
Used by
RedRules
Type here to search
97%
6:52 PM
1/29/2021


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > Virtual machines >
webONE
Virtual machine
Search (Ctrl+/)
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Public IP address
20.62.210.194
Virtual network/subnet
redNET/REDsubnet
DNS name
Configure
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name
webONE
Operating system
Linux
Publisher
Canonical
Networking
Public IP address
20.62.210.194
Public IP address (IPv6)
-
Private IP address
10.0.0.9


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > All resources >
All resources
Default Directory
Add
Manage view
Filter for any field...
Name
webONE_OsDisk_1_01a181dd1dfd4a...
webONE_OsDisk_1_dff4cc27339b4a3...
WEBset
webTWO
webtwo874
webtwo927
webTWO_key
webTWO_key_0122
Page 1 of 1
WEBset
Availability set
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Virtual machines
Properties
Locks
Automation
Tasks (preview)
Export template
Delete
Refresh
Essentials
JSON View
Resource group (change)
REDteam
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Fault domains
2
Update domains
5
Virtual machines
2
Managed
Yes
Colocation status
N/A
Search virtual machines
Name
Status
Colocation status
Fault Domain
Update D
webONE
Stopped (deallocated)
0
0
webTWO
Stopped (deallocated)
1
1


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > Virtual machines >
webTWO
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Location
East US
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
Public IP address
20.62.210.194
Virtual network/subnet
redNET/REDsubnet
DNS name
Configure
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name
webTWO
Operating system
Linux
Publisher
Canonical
Networking
Public IP address
20.62.210.194
Public IP address (IPv6)
-
Private IP address
10.0.0.10


portal.azure.com/#@CyberOpsDaveprotonmail.onmicrosoft.com/resource/subscriptions/73f501ae-2cb4-4770-a3b5-e08dac45c879/resour...
Apps
Dashboard | Bootca...
Projects · Dashboar...
My virtual machine...
Other bookmarks
Microsoft Azure
Search resources, services, and docs (G+/)
CyberOpsDave@proton...
DEFAULT DIRECTORY
Home > Virtual machines >
DVWAvm3
Virtual machine
Search (Ctrl+/)
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
East US (Zone 2)
Subscription (change)
Sub-CyberOpsDave
Subscription ID
73f501ae-2cb4-4770-a3b5-e08dac45c879
Availability zone
2
Tags (change)
ownerNAME : CyberOpsDave@protonmail.com
20.62.210.194
Virtual network/subnet
redNET/REDsubnet
DNS name
Configure
Properties
Monitoring
Capabilities (7)
Recommendations
Tutorials
Virtual machine
Computer name
DVWAvm3
Operating system
Linux
Publisher
Canonical
Networking
Public IP address
20.62.210.194
Public IP address (IPv6)
-
Private IP address
10.0.0.8