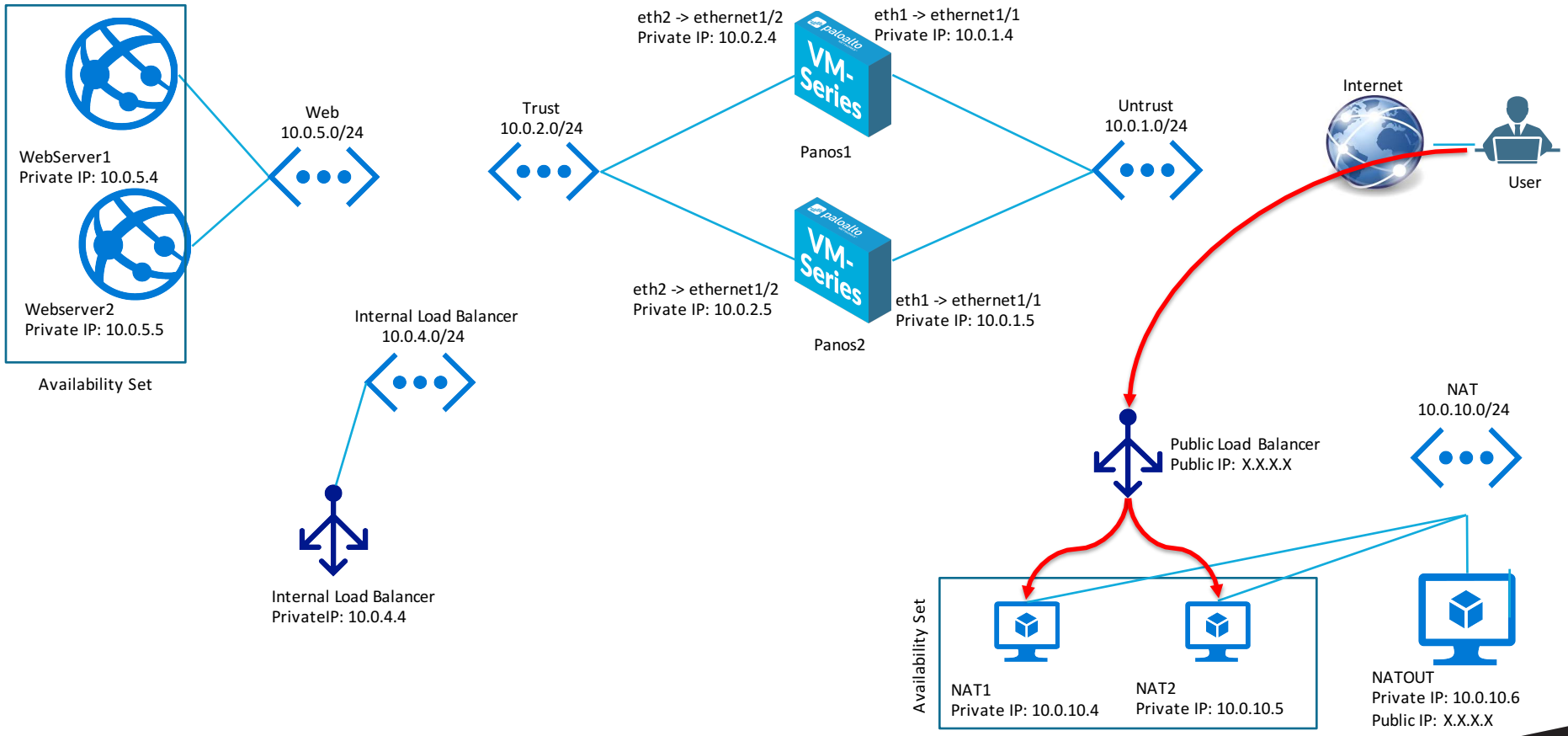
Microsoft Azure

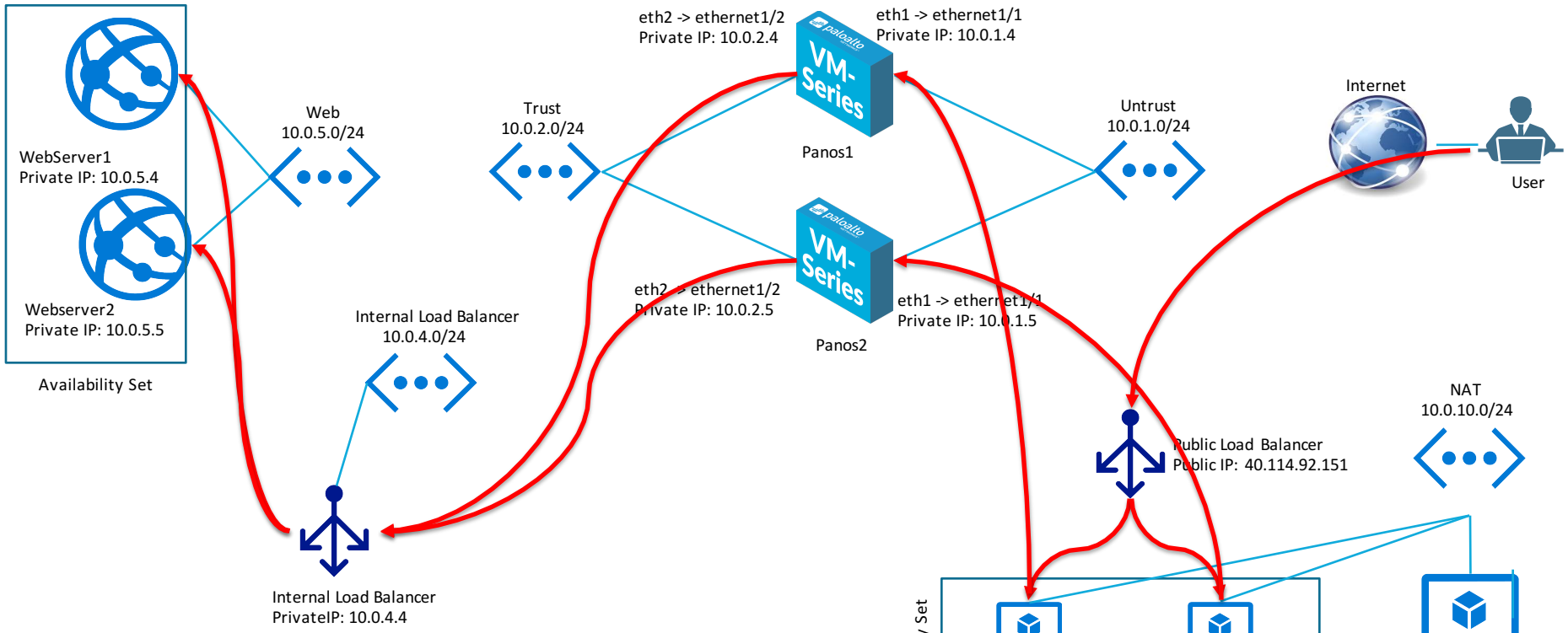
Load Balancer Sandwich
Template Overview

paloalto NETWORKS

Load Balancer “Sandwich” Template Logical Architecture



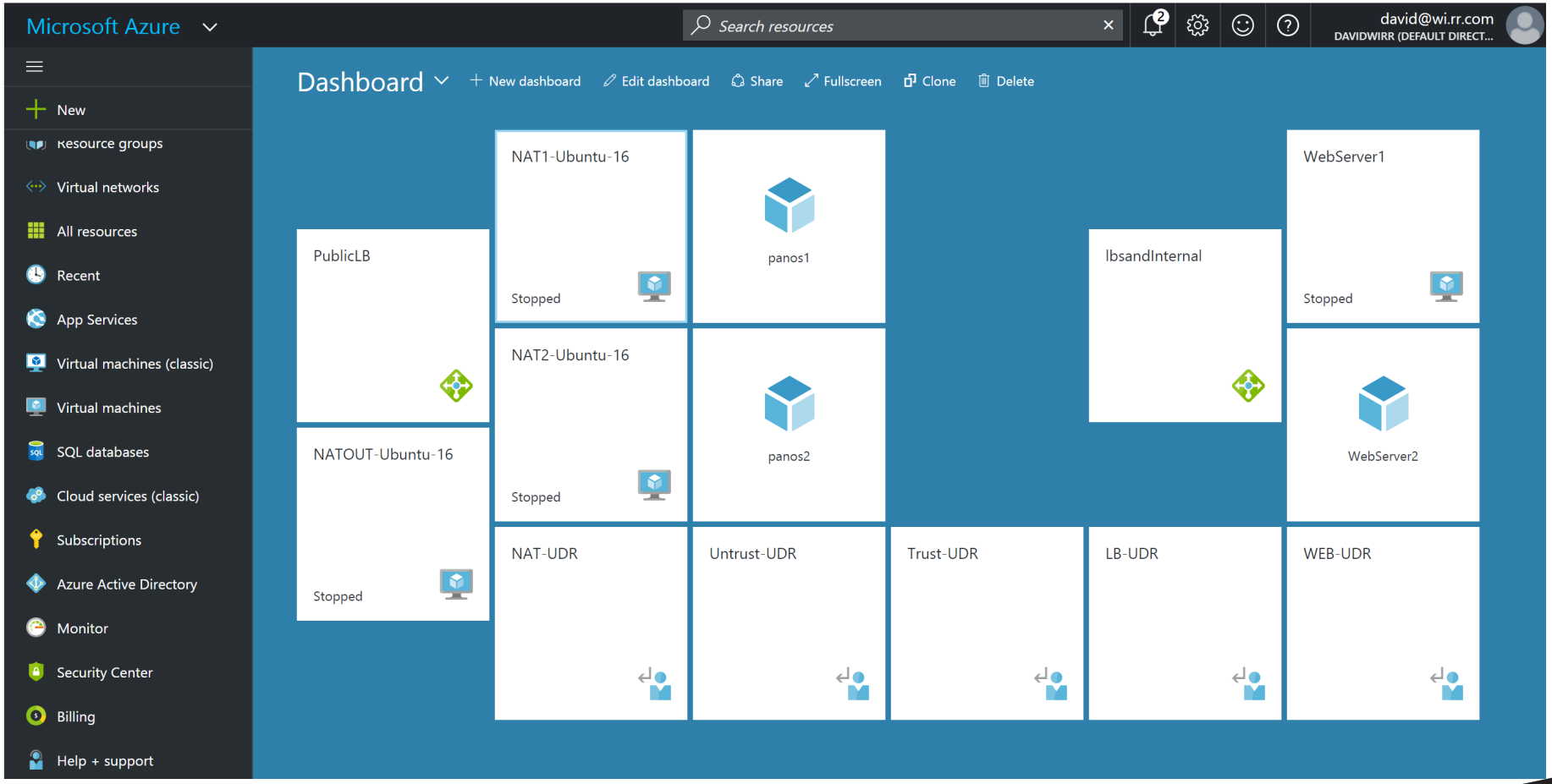
Load Balancer “Sandwich” Template Logical Architecture



NAT VM 1 source NATs traffic to 10.0.10.4 and destination NATs to 10.0.1.4
Panos 1 source NATs to 10.0.2.4 and destination NATs to 10.0.4.4

NAT VM 2 source NATs traffic to 10.0.10.5 and destination NATs to 10.0.1.5
Panos2 source NATs to 10.0.2.5 and destination NATs to 10.0.4.4

Overview of the deployment in the Azure Portal



Overview of the deployment

This template deploys:
- Two BYOL Palo Alto Networks firewalls- Panos1 and Panos2
- One internal Load Balancer
- One public Load Balancer
- Two Ubuntu NAT Servers for Inbound traffic– NAT1 and NAT2
- One Ubuntu NAT Server for Outbound traffic- NATOUT
- Two internal Web Servers with Apache – WebServer1 and WebServer2
- UDRs to direct traffic through the firewalls
- At this point the template deploys to the US Central Region

Post deployment tasks that need to be done to complete the setup:
- The firewalls need to be licensed and configured.

Microsoft Azure

To start the deployment

To start the deployment click on the Deploy to Azure from the README.md

README.md

2 VM-Series Firewalls in a load balancer sandwich along with two webservers

NOTE---DO NOT USE!!! THIS IS STILL UNDER CONSTRUCTION AND DOES NOT YET WORK AS INTENDED!

The intent of this ARM template is to deploy a firewall sandwich environment that includes:

- One Public Load Balancer
- Two Palo Alto Networks Firewalls
- One Internal Load Balancer
- Two Web Servers with apache webserver
- VNET 10.0.0.0/16
- Multiple Subnets and UDRs to support the traffic flow

This template creates all the infrastructure and appropriate UDRs. It does not currently license or configure the firewall. That will need to be done afterwards.

paloalto NETWORKS

Microsoft Azure

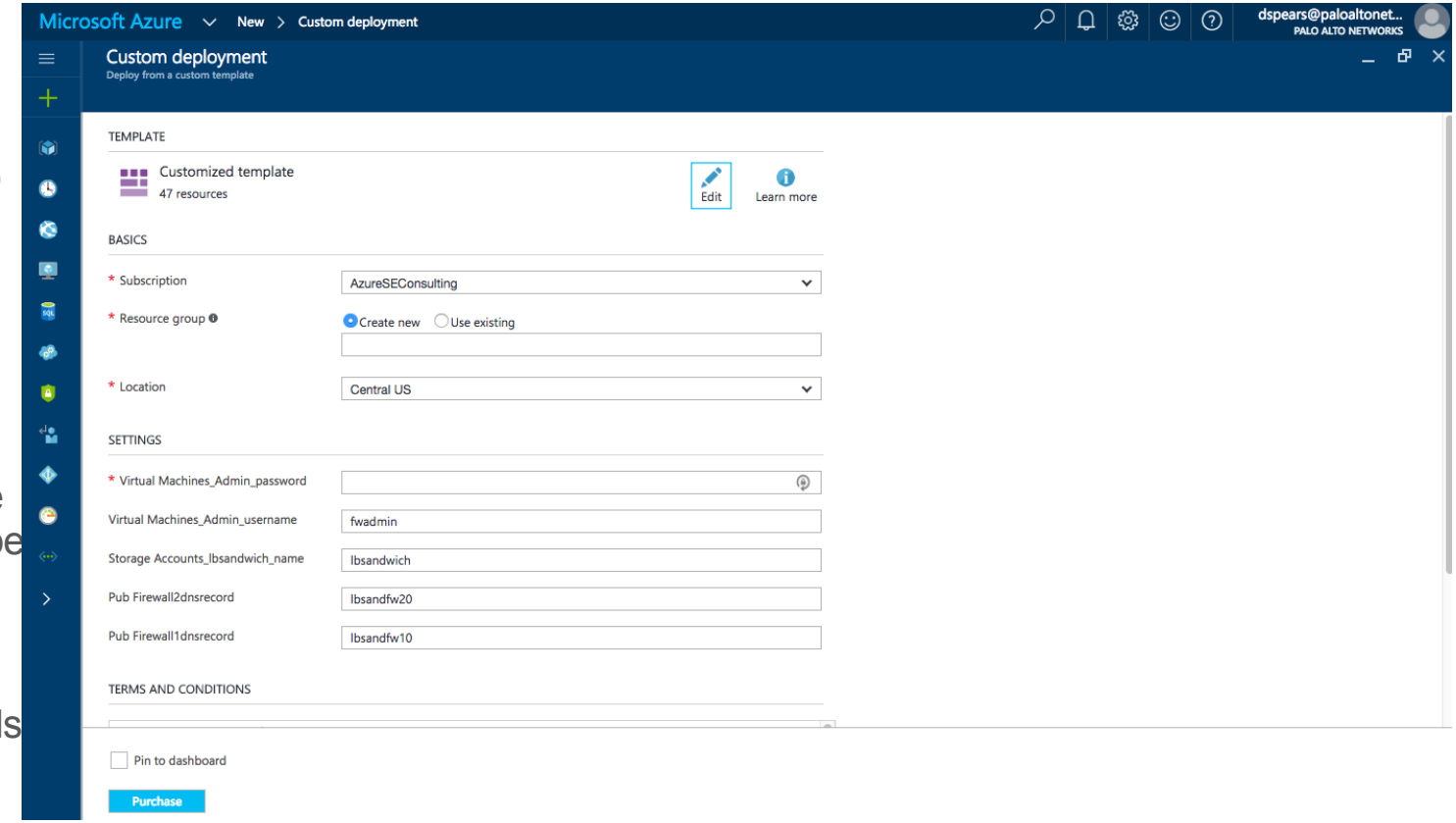
Fill out the template parameters

Everything will deploy into a single Resource Group. I usually create a new group to make it easier to delete later.

Select “Central US” as this is where all the individual resources will get deployed.

The Storage account must be globally unique so this must be changed or the deployment will fail.

The Pub Firewall DNS records are the DNS names for the firewall MGMT interfaces and must also be globally unique.

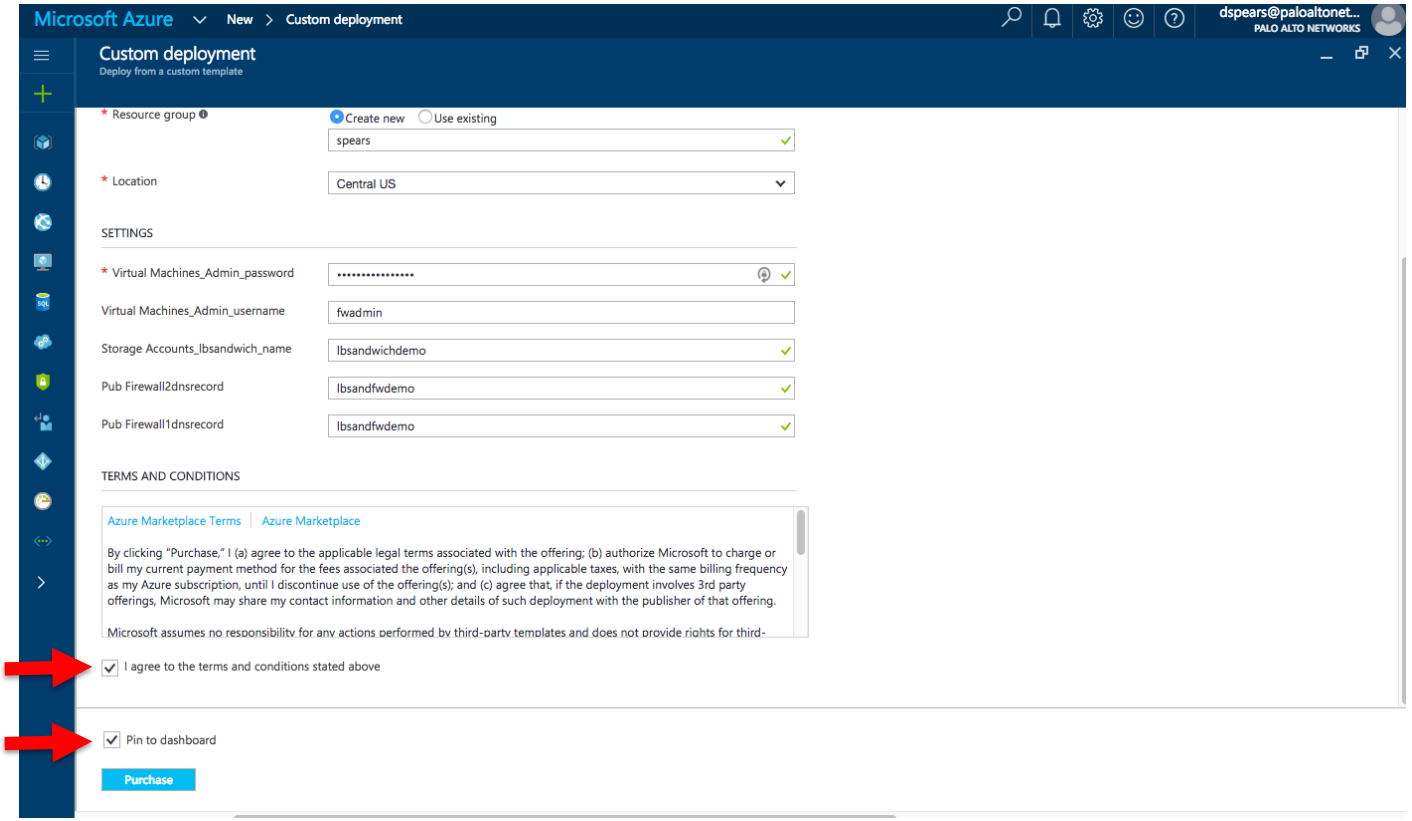


Microsoft Azure

Fill out the template parameters

Scroll down and check the agreement terms. I also check the Pin to dashboard.

Click on the Purchase button.



Microsoft Azure

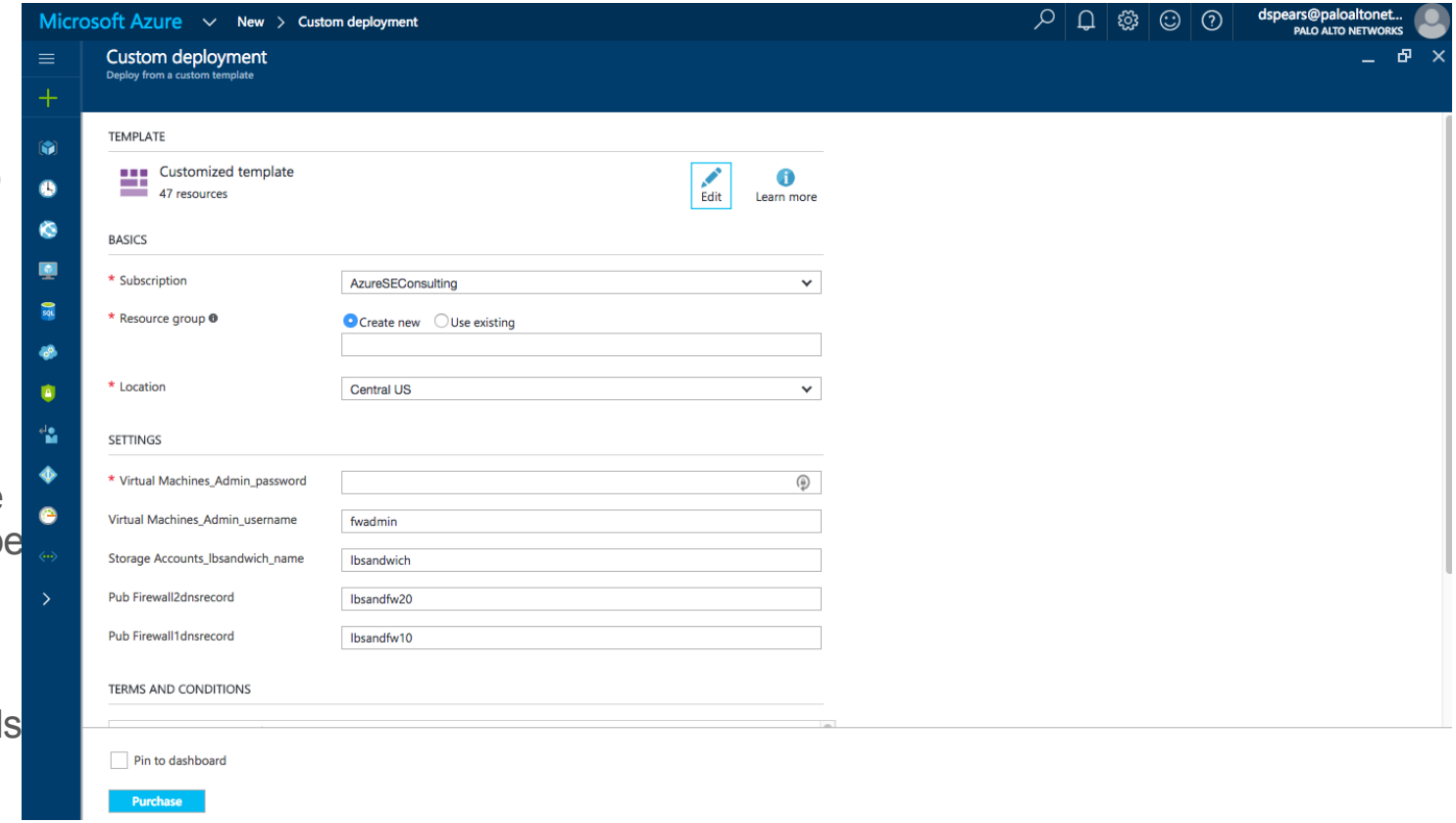
Fill out the template parameters

Everything will deploy into a single Resource Group. I usually create a new group to make it easier to delete later.

Select “Central US” as this is where all the individual resources will get deployed.

The Storage account must be globally unique so this must be changed or the deployment will fail.

The Pub Firewall DNS records are the DNS names for the firewall MGMT interfaces and must also be globally unique.

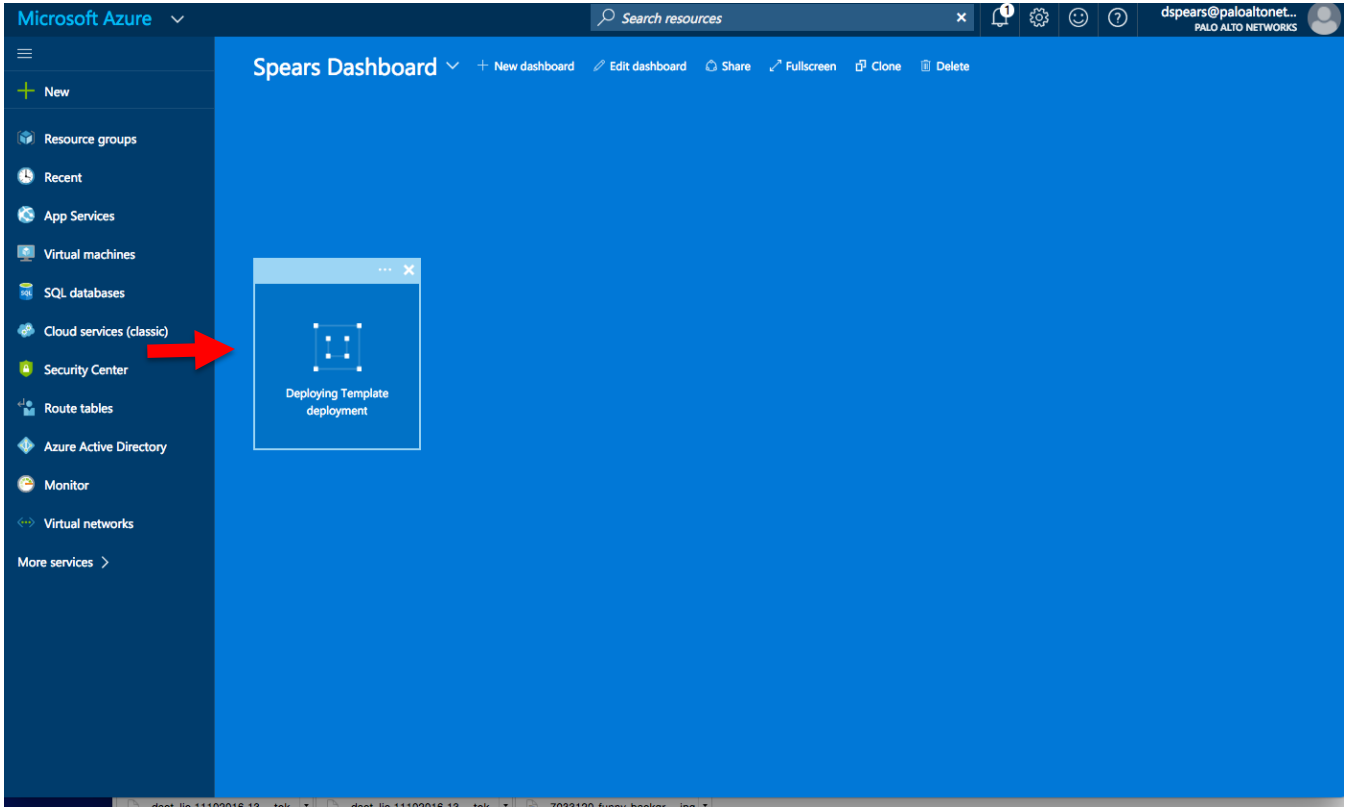


Microsoft Azure

Monitor the deployment

If the validation completes successfully you will be redirected to the dashboard.

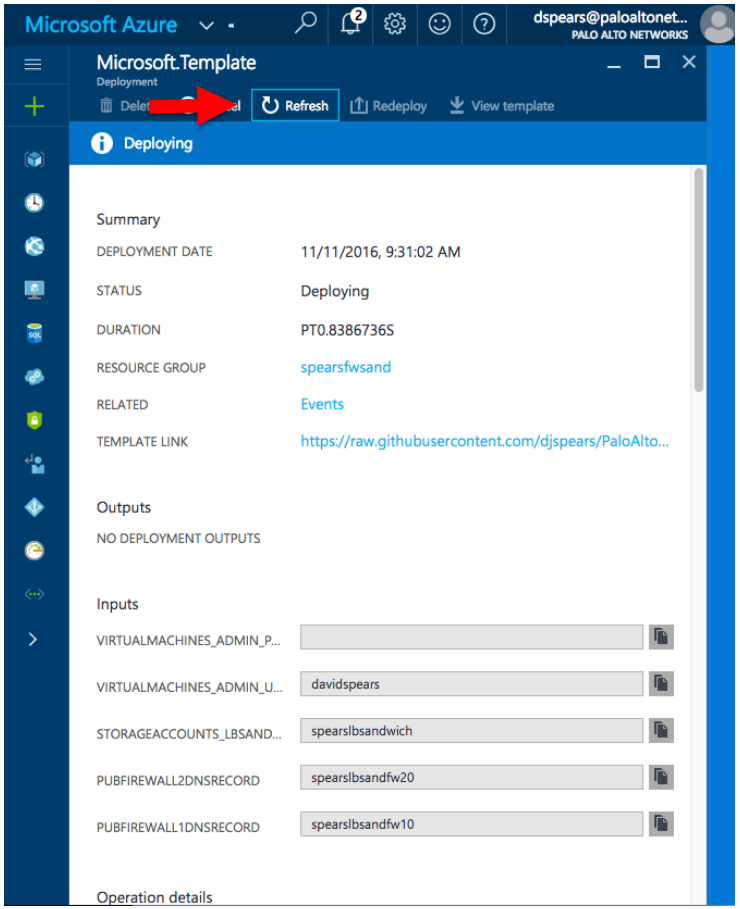
Click on the Deploying Template tile to monitor the deployment process.



Microsoft Azure

Monitor the deployment

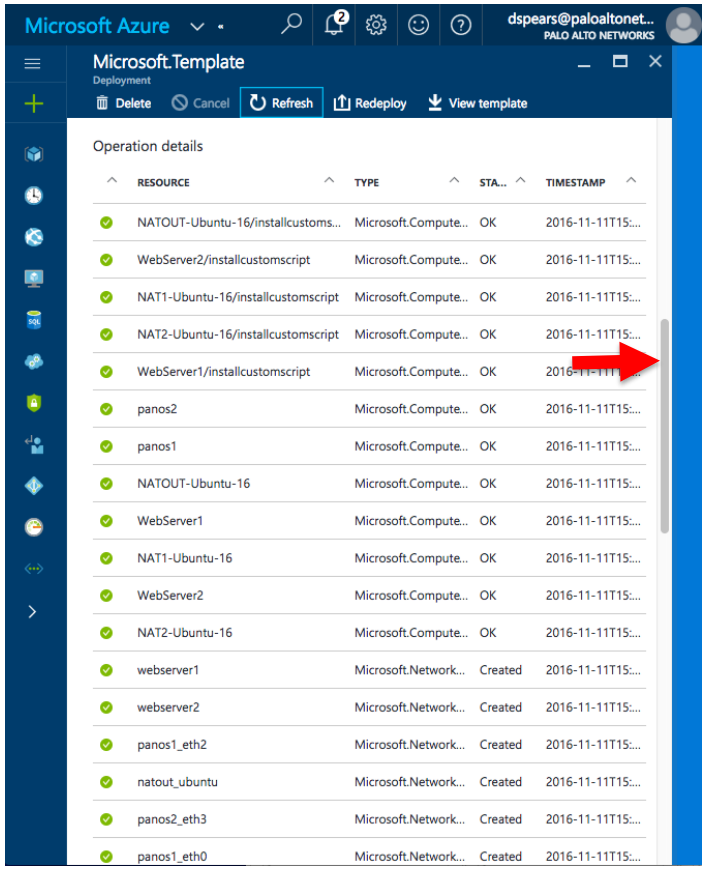
You can click on the Refresh button to get an update.



Microsoft Azure

Monitor the deployment

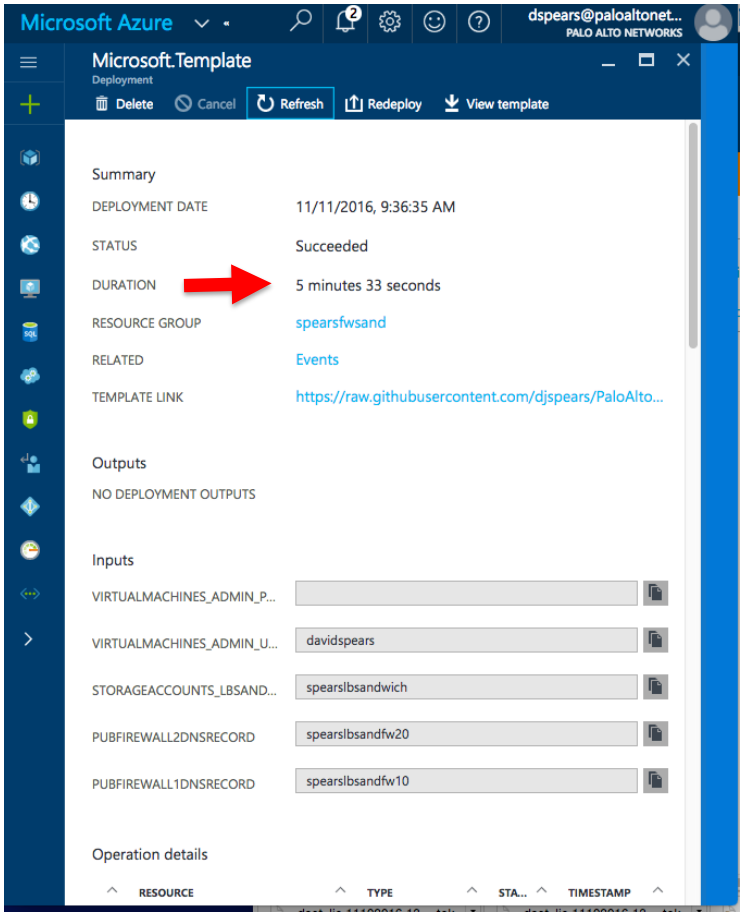
Scrolling down shows more specifics about what is being built.



Microsoft Azure

Monitor the deployment

Once the deployment is done the status will change to Succeeded. This one too 5min 33 seconds to deploy.



paloalto NETWORKS

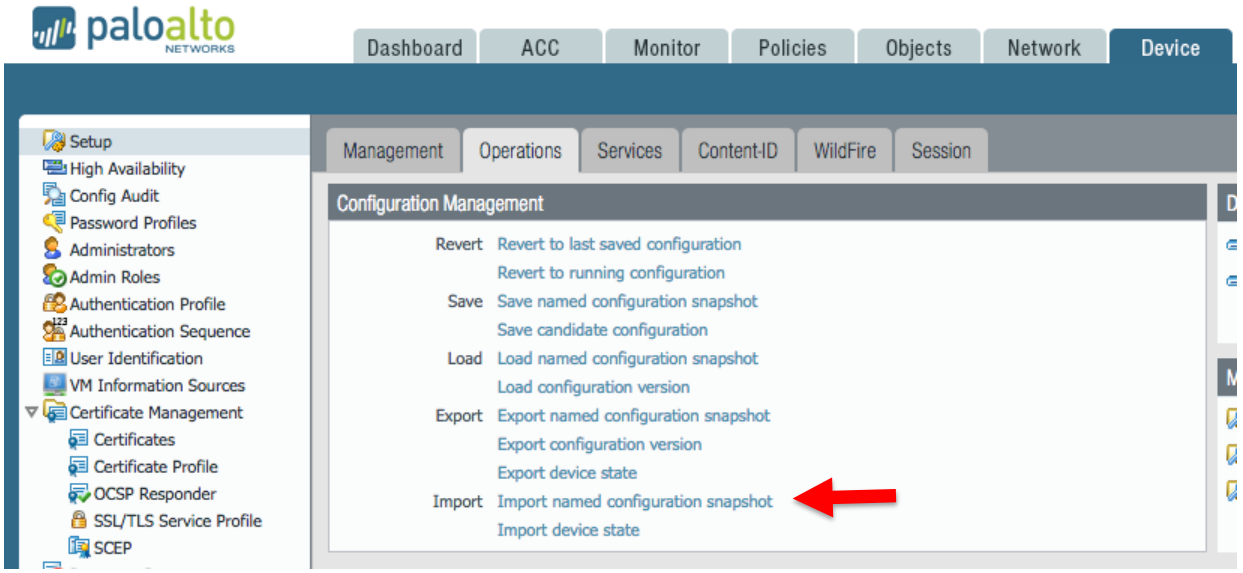
Microsoft Azure

License and configure the firewall

License the firewall through the support site. There are two basic config files in the github directory that can be used as a starting point.

Those files are called panos1-config.xml and panos2-config.xml.

Navigate to the Device/setup/operations tab to the partial config file. Select import and copy the appropriate file to the corresponding firewall.



paloalto NETWORKS

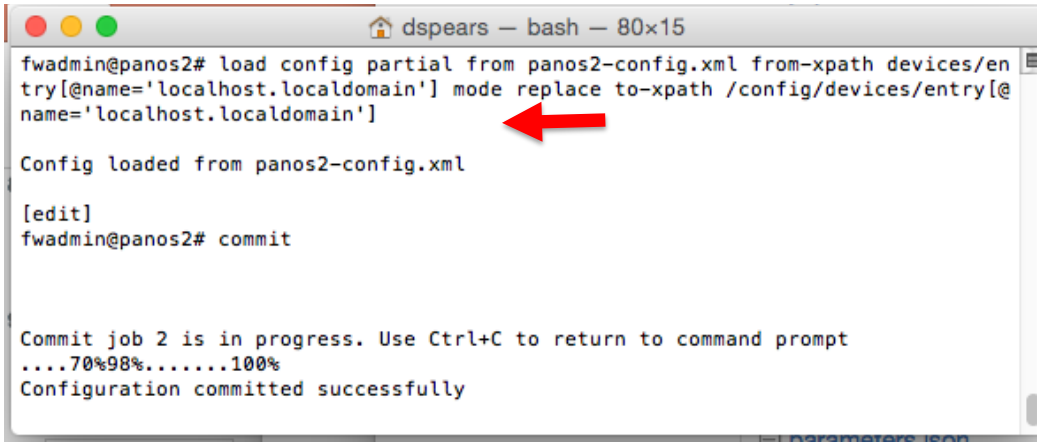
Load the configuration into the firewall

Ssh into the firewall and go into the configure mode.

To load the paritial configuration type:

load config partial from panos2-config.xml from-xpath devices/entry[@name='localhost.localdomain'] mode replace to-xpath /config/devices/entry[@name='localhost.localdomain']

Commit the configuration



Microsoft Azure

Test

Navigate to the public address of the public load balancer to identify the ip address that can be used to access the web servers through the two panos firewalls.

paloalto NETWORKS


paloalto
NETWORKS®