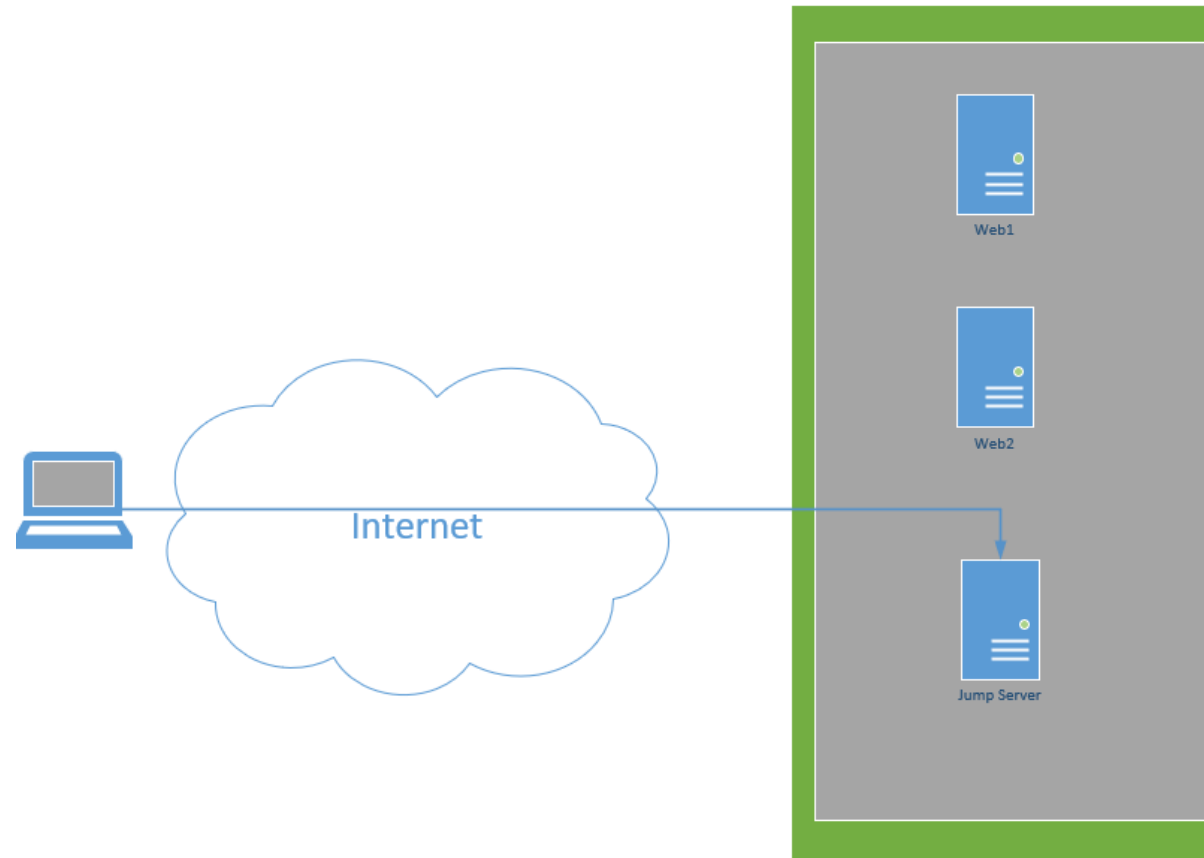


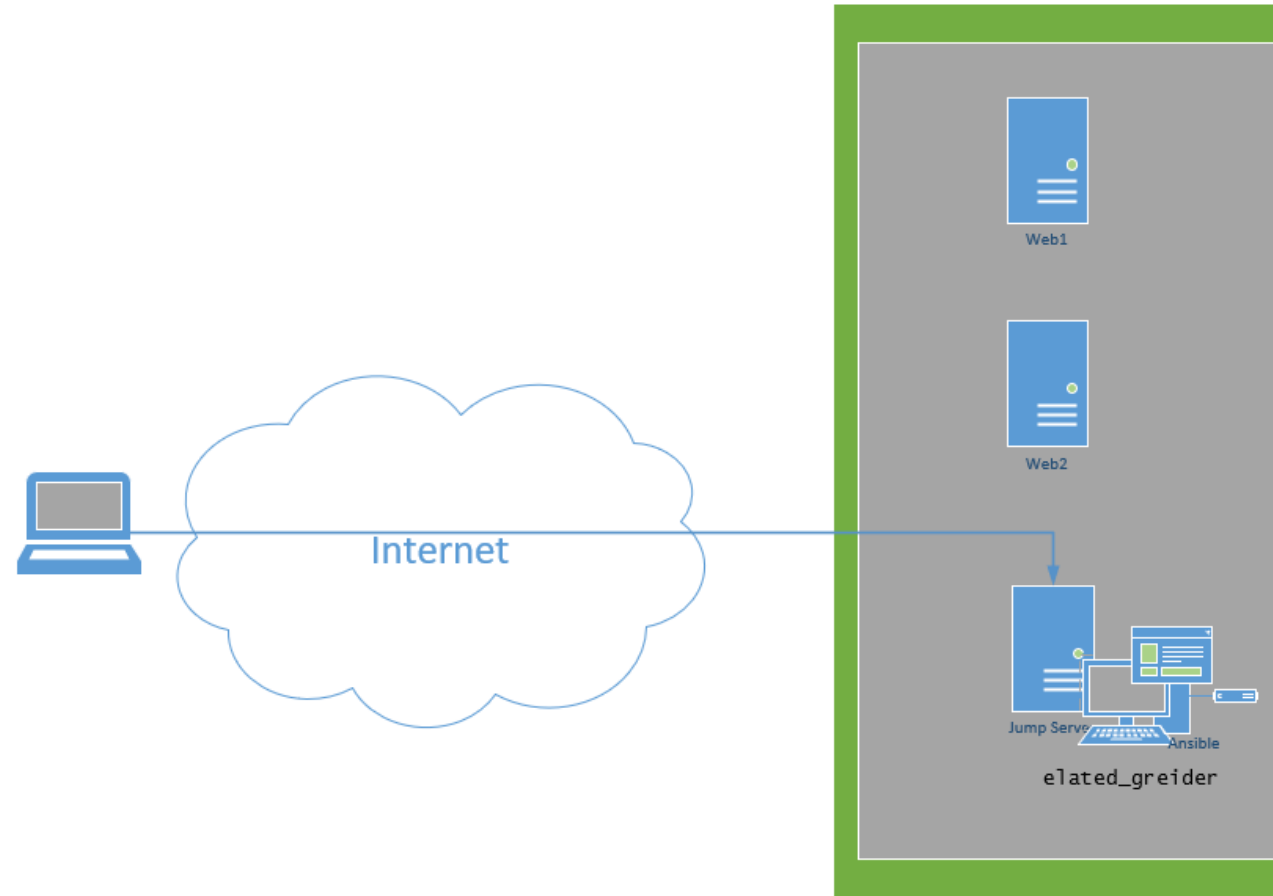
# ELK Project

# Last Class

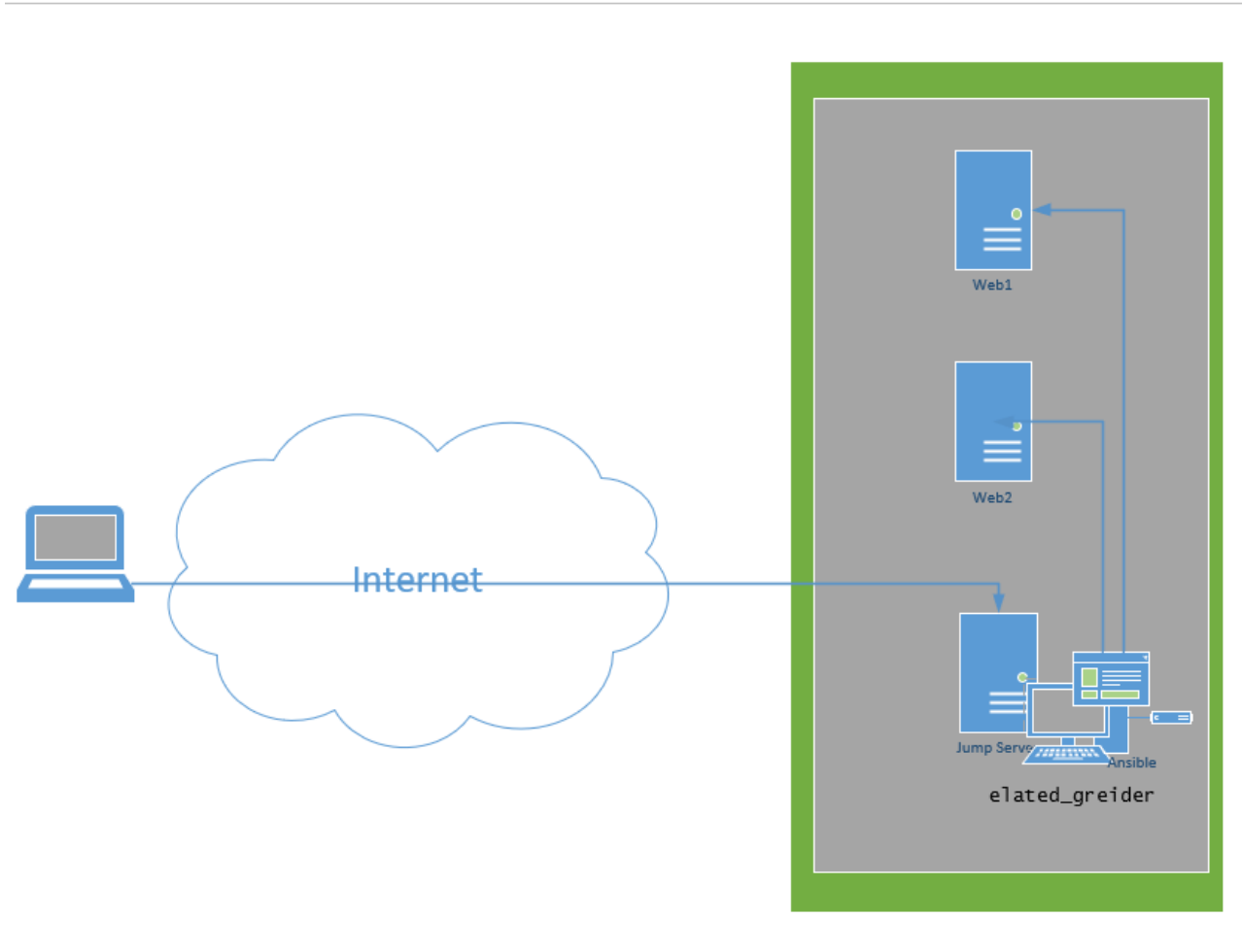
## Some of You Only Gained SSH Access



# A Few of You Set Up Ansible

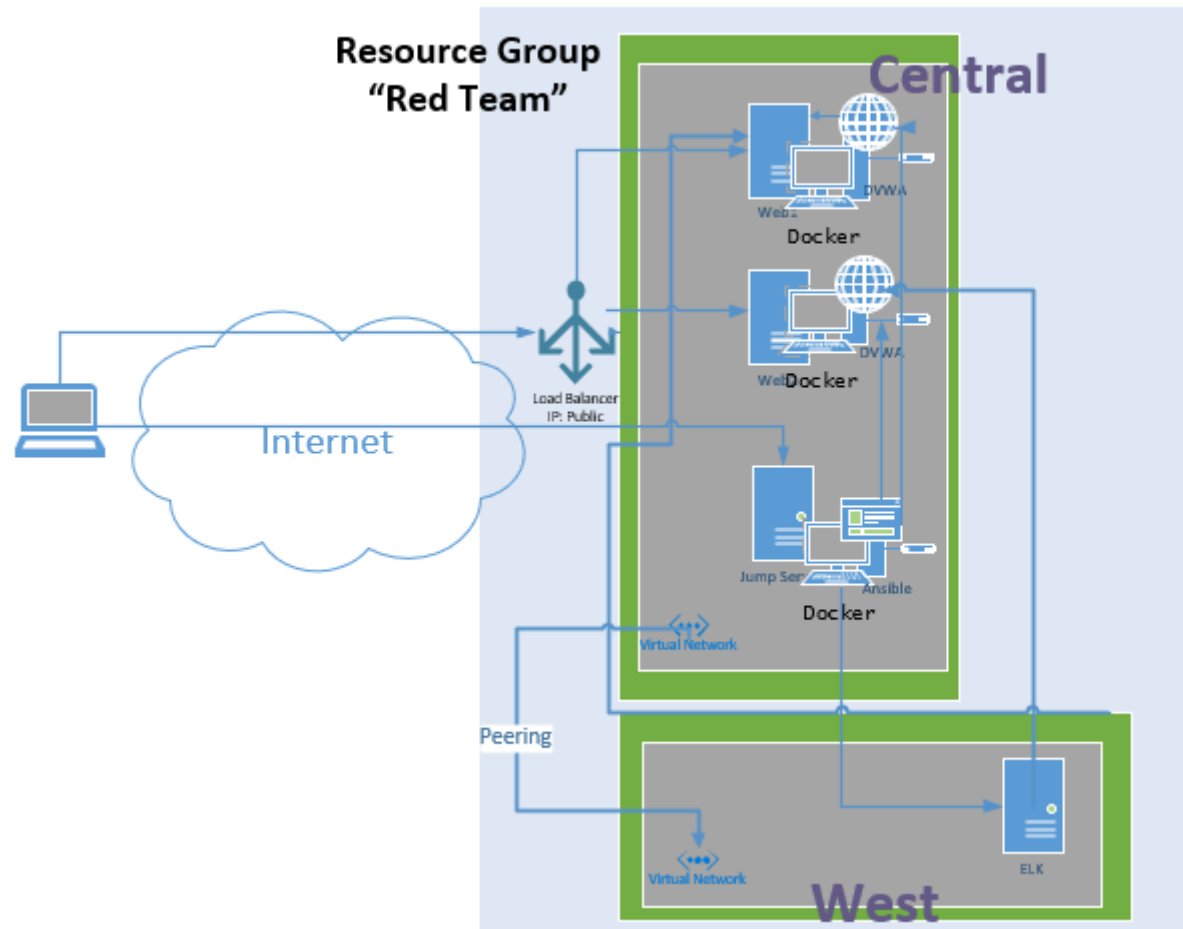


# And Three of Us Connected Ansible to the Web Servers

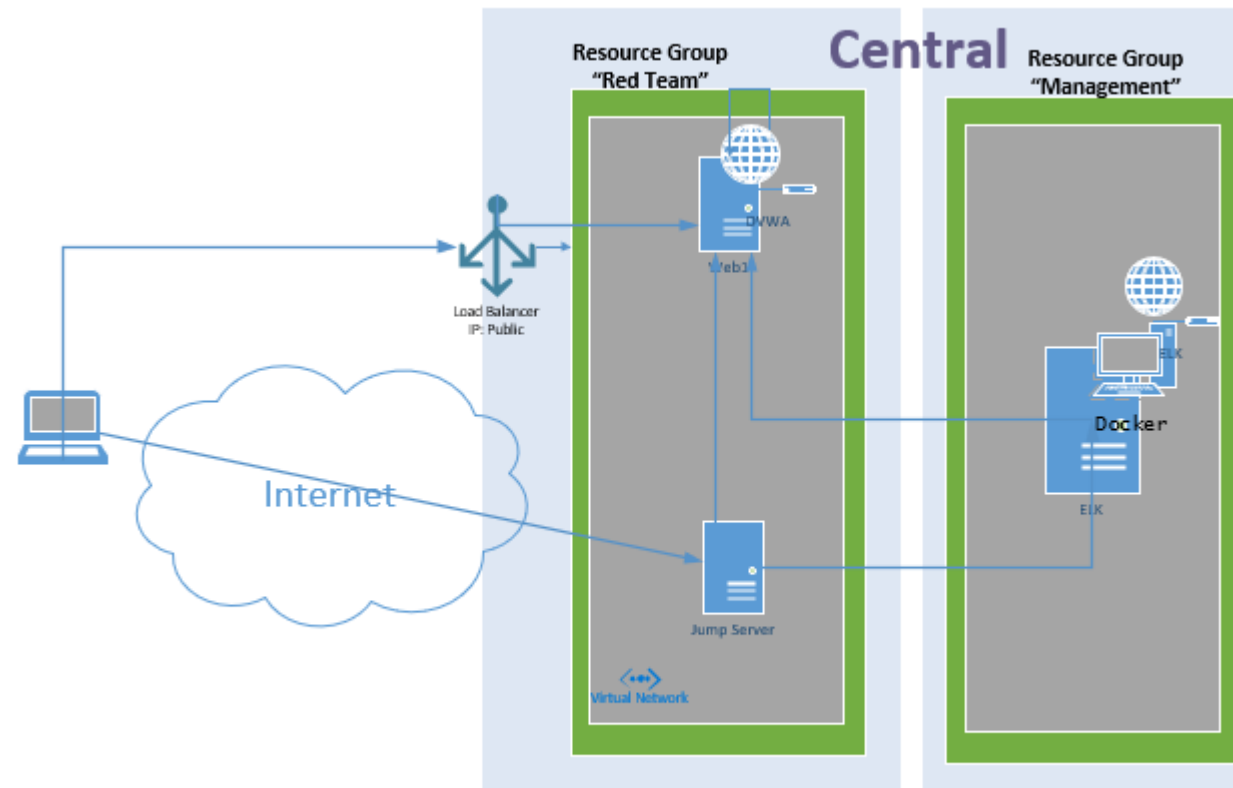


Day 1  
Start

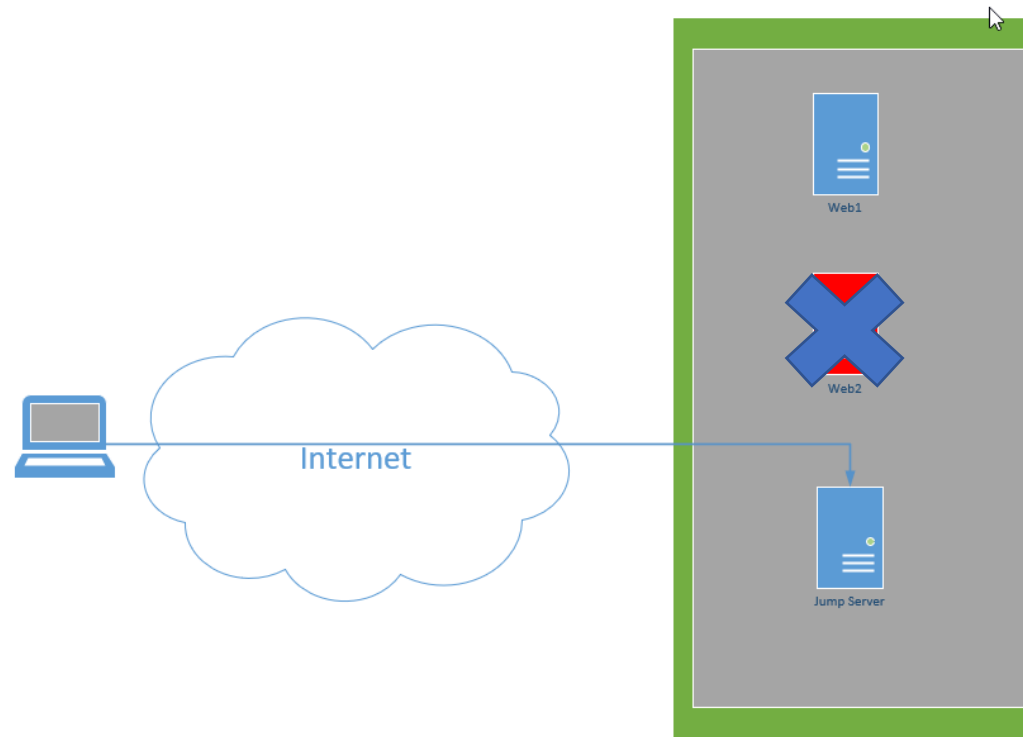
# Original Project



# New Project

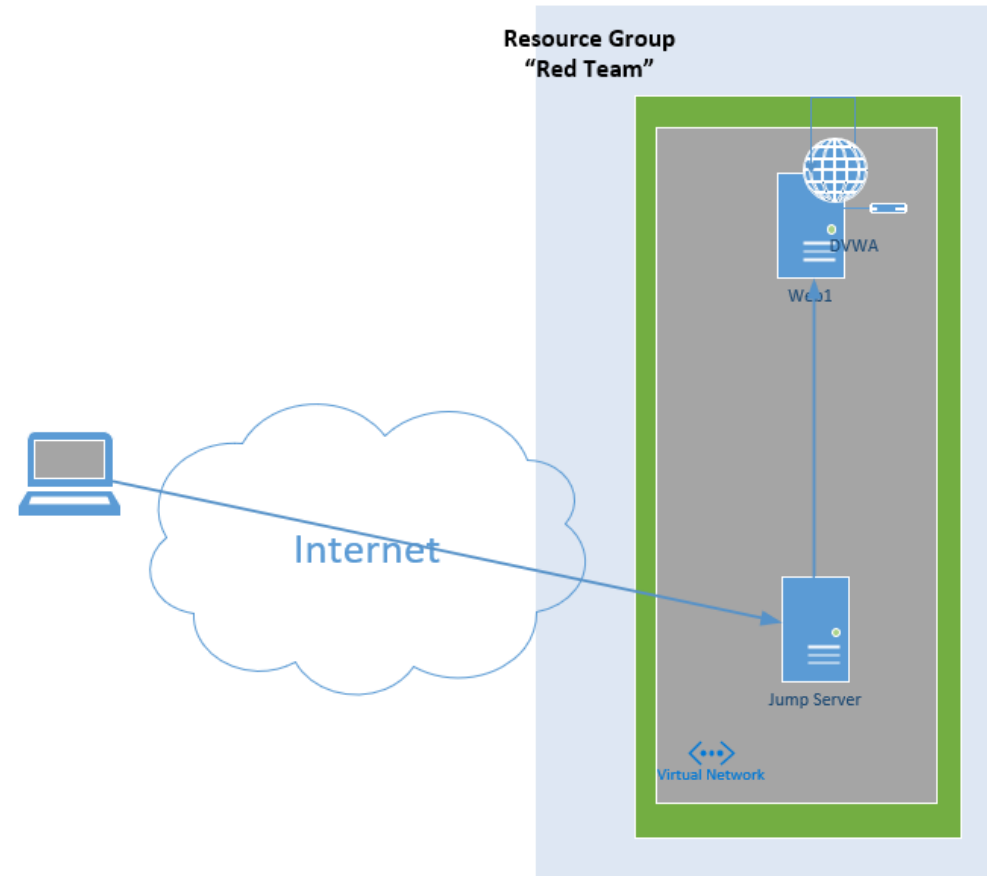


1. Forget About Ansible
2. Delete Any Containers on Web1
3. Delete VM Web 2
4. Create Usernames and Passwords for both VMs – Certs will not be used





# Setup DVWA



1. SSH into the Jump Server and use it to SSH into the Web1
2. Run the DVWA Script that Terrace and Steve Created and Thank Them

```
mv Filebeat /etc/filebeat/filebeat.yml

#!/bin/bash

if ! [ $(id -u) = 0 ]; then
    echo "The script need to be run as root." >&2
    exit 1
fi

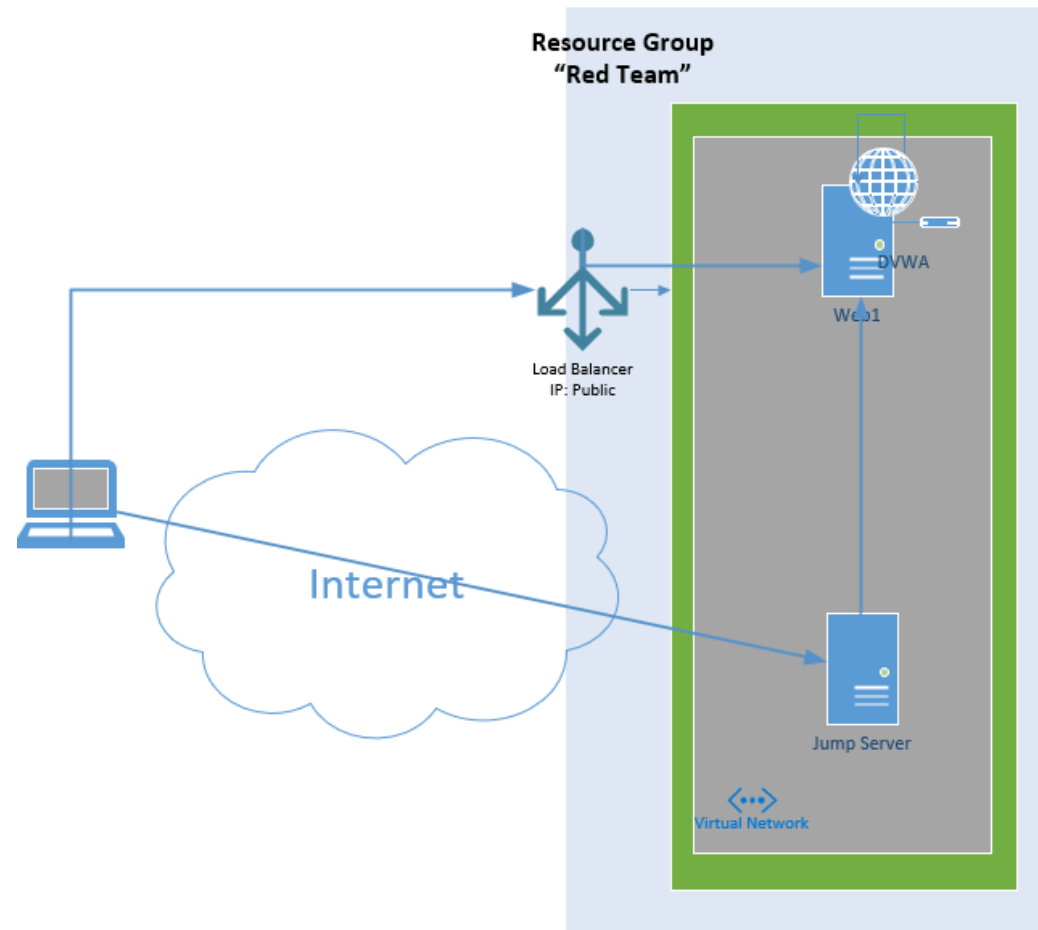
if [ $SUDO_USER ]; then
    real_user=$SUDO_USER
else
    real_user=$(whoami)
fi
#Check to see if user is Root
#
echo apt update && apt upgrade
#Update and upgrade Current VM
#
apt install docker.io
#installs docker to box
#
apt install python3-pip
#installs python
#
apt install docker
#installs docker python module
#
systemctl start docker
#starts docker
#
docker pull vulnerables/web-dvwa
#pulls docker Dvwa
#
docker run --rm -it -p 80:80 vulnerables/web-dvwa
#Create Image
#
```

# If It's Working.....

```
root@Jump-Box: /home/jack
[ ok ] Starting MariaDB database server: mysqld.
[+] Starting apache
[....] Starting Apache httpd web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message
. ok
==> /var/log/apache2/access.log <==
==> /var/log/apache2/error.log <==
[Sat Oct 10 04:04:21.645794 2020] [mpm_prefork:notice] [pid 302] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operations
[Sat Oct 10 04:04:21.645880 2020] [core:notice] [pid 302] AH00094: Command line: '/usr/sbin/apache2'
==> /var/log/apache2/other_vhosts_access.log <==
==> /var/log/apache2/access.log <==
99.2.0.163 - - [10/Oct/2020:04:05:11 +0000] "GET / HTTP/1.1" 302 479 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38"
99.2.0.163 - - [10/Oct/2020:04:05:11 +0000] "GET /login.php HTTP/1.1" 200 1049 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38"
99.2.0.163 - - [10/Oct/2020:04:05:11 +0000] "GET /dvwa/css/login.css HTTP/1.1" 200 741 "http://13.67.214.91/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38"
99.2.0.163 - - [10/Oct/2020:04:05:11 +0000] "GET /dvwa/images/login_logo.png HTTP/1.1" 200 9375 "http://13.67.214.91/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38"
99.2.0.163 - - [10/Oct/2020:04:05:11 +0000] "GET /favicon.ico HTTP/1.1" 200 1706 "http://13.67.214.91/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38"
```

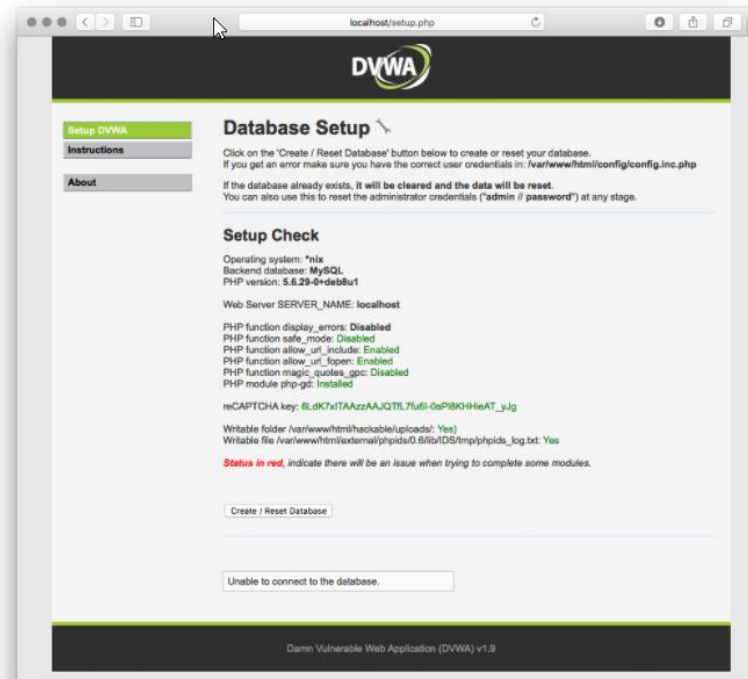
1. Create a Load Balancer and add Web01 into it
2. Open port 80 from your Load Balancer to your Web server (NSG)

<https://www.youtube.com/watch?v=-VMPzVoo5Nk>



1. Test Connecting to the DVWA Using the Public IP of the Load Balancer
2. Log in following the below Instructions – Start reading where the images start, ignore everything before it  
<https://hub.docker.com/r/vulnerables/web-dvwa>

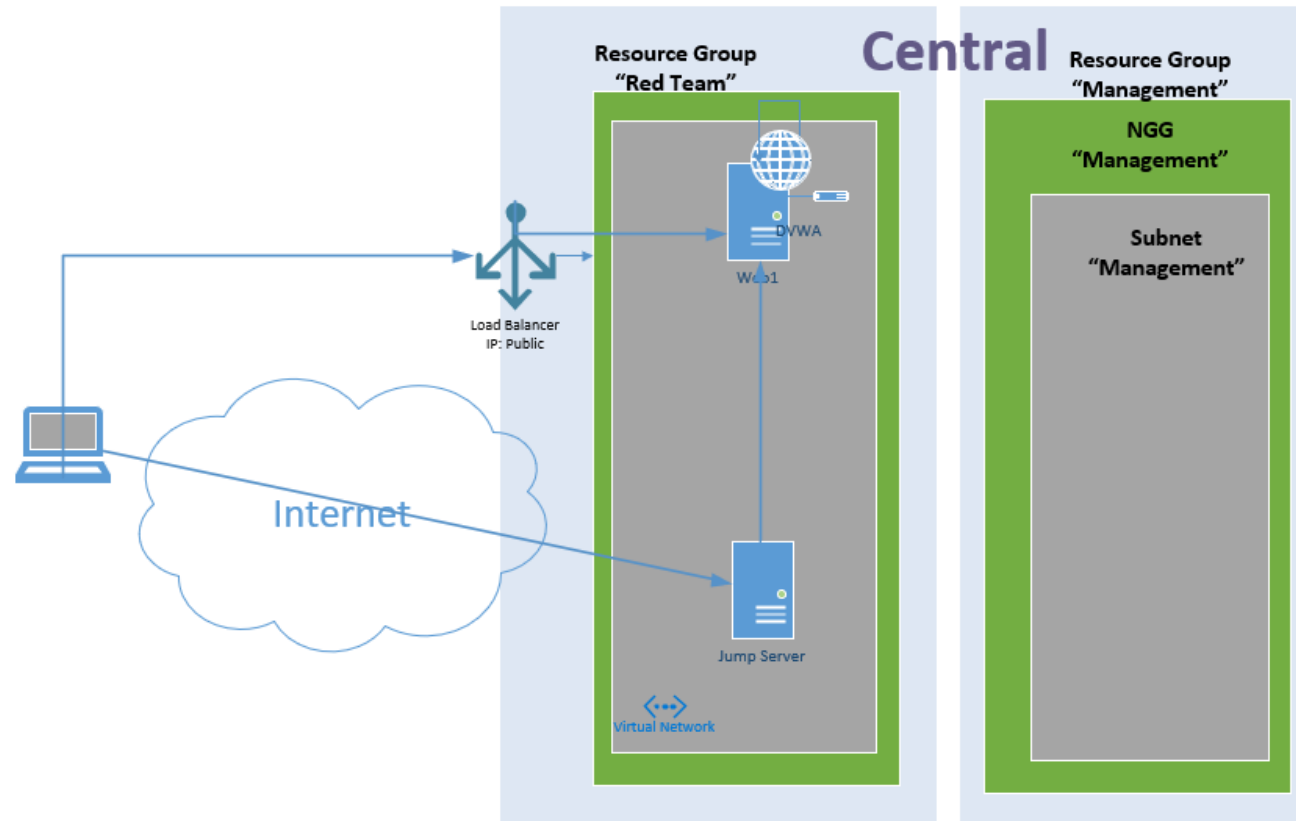
machine:



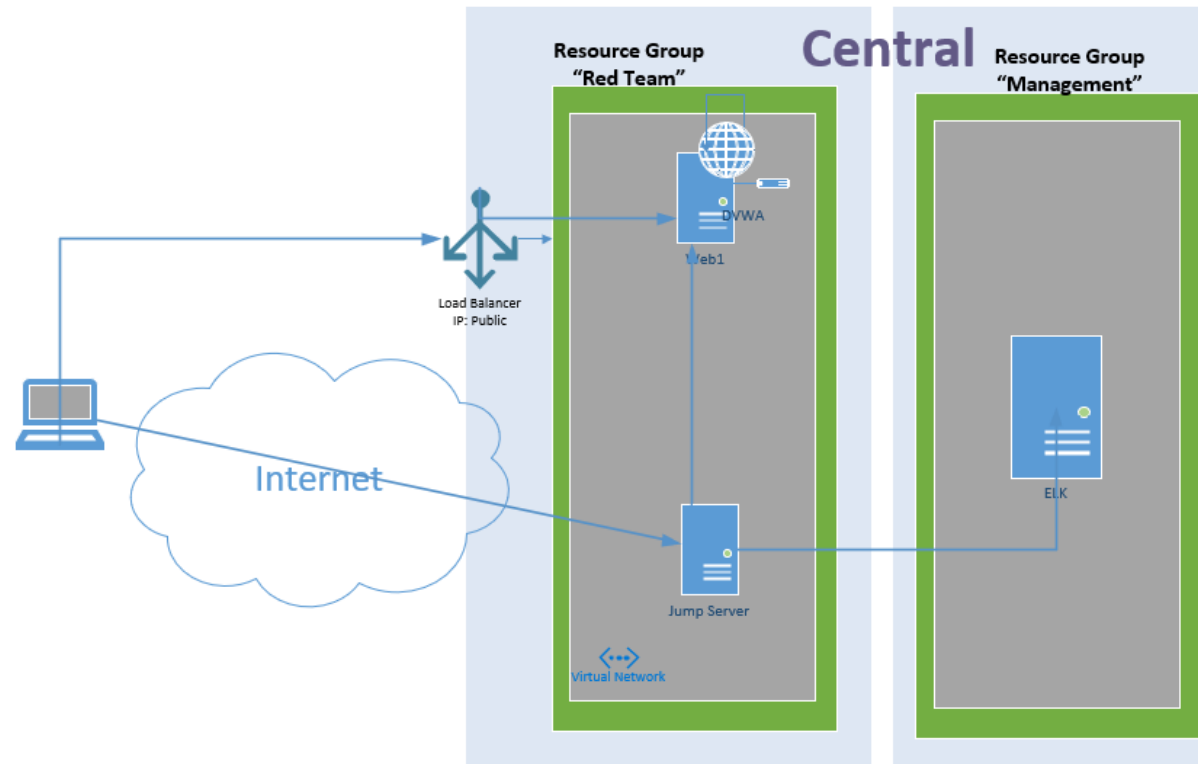
Just click on the `Create / Reset database` button and it will generate any additional configuration needed.

**Login with default credentials**

1. Create New Resource Group – “Management”
2. Create New Subnet in Existing Virtual Network
3. Create New NSG - “Management” in Management Resource Group
4. Associate NSG to “Management” Subnet
5. Move Existing VNET to New Resource Group



1. Create a Simple New VM, in Resource Group “Management”, Called “ELK”.  
Create a username and password and make sure the B series VM has 2 CPUs and 4gb of Memory  
Make Sure you Don’t Create a NEW NSG as part of the Setup  
Give it a Public IP
2. Verify you can SSH into it the new VM



# Install ELK

```
#!/bin/bash

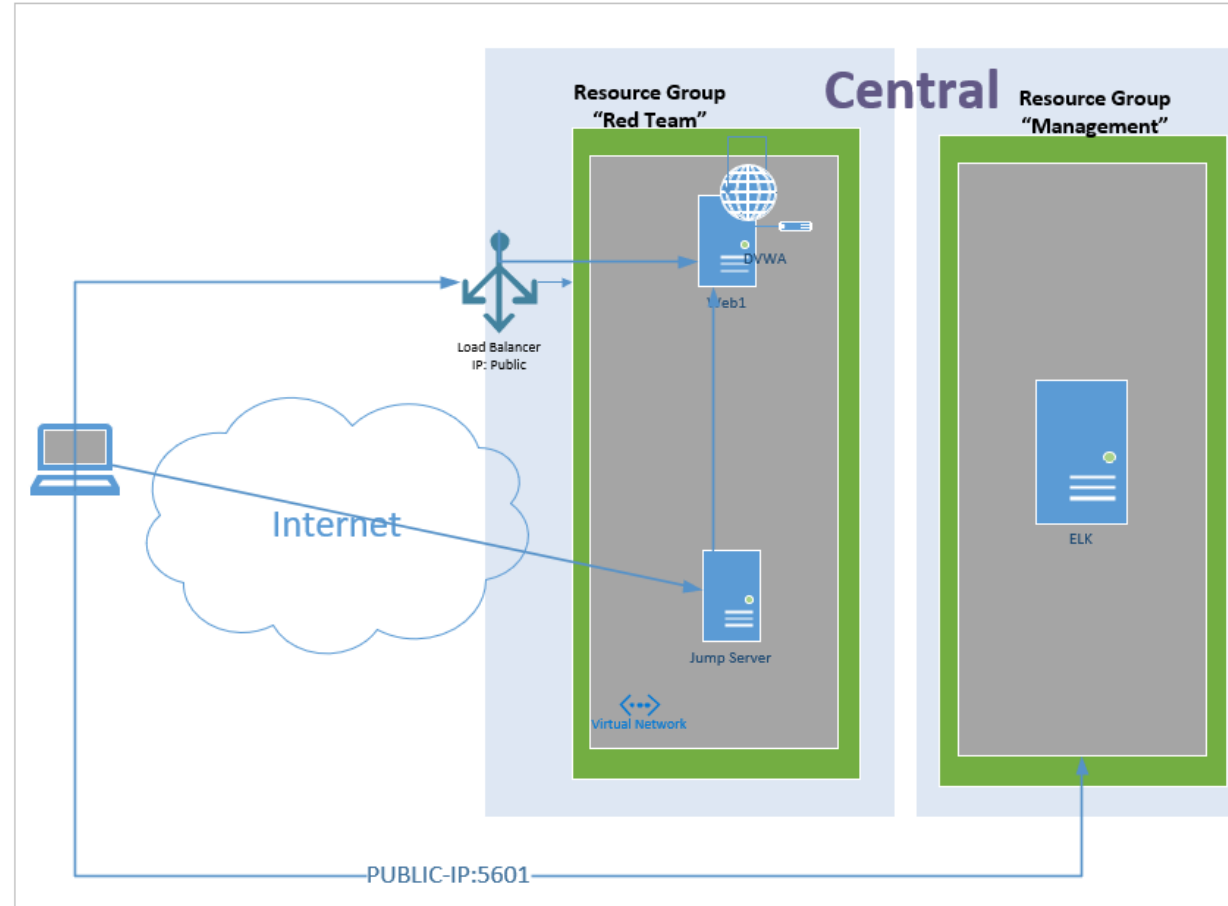
if ! [ $(id -u) = 0 ]; then
    echo "The script need to be run as root." >&2
    exit 1
fi

if [ $SUDO_USER ]; then
    real_user=$SUDO_USER
else
    real_user=$(whoami)
fi
#Check to see if user is Root
#
echo apt update && apt upgrade
#Update and upgrade Current VM
#
apt install docker.io
#installs docker to box
#
apt install python3-pip
#installs python
#
apt install docker
#installs docker python module
#
sysctl -w vm.max_map_count=262144
#increases virtual memory
#
systemctl start docker
#starts docker
#
docker pull sebp/elk
#pulls docker elk
#
docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it sebp/elk
#Create Image
#
```



# Connect to ELK and Login

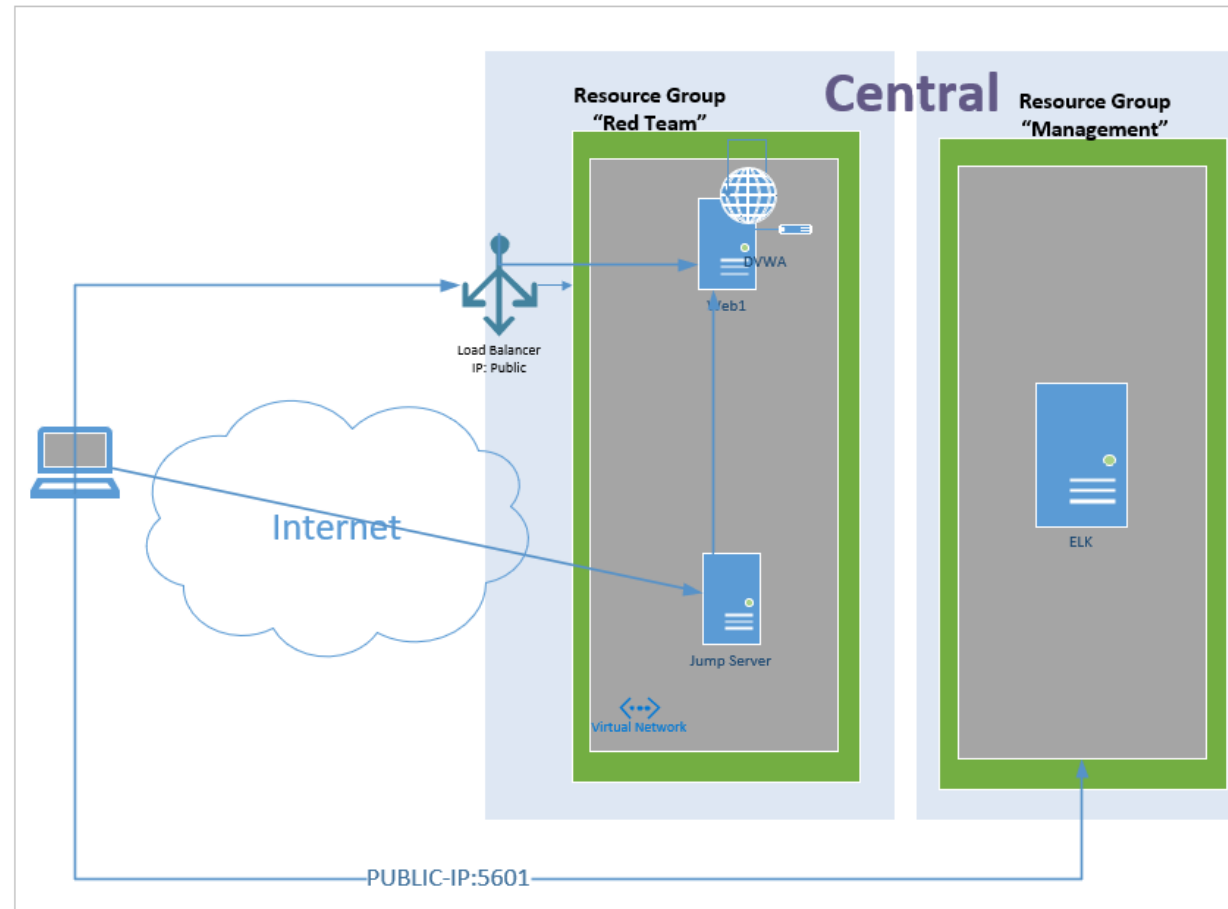
1. Modify the “management” NSG to Allow your Home IP to connect to the Elk Internal IP on port 5601
2. Browse to [http://Your\\_IP:5601/app/kibana](http://Your_IP:5601/app/kibana) and Login to change the default password



Day 1  
Complete

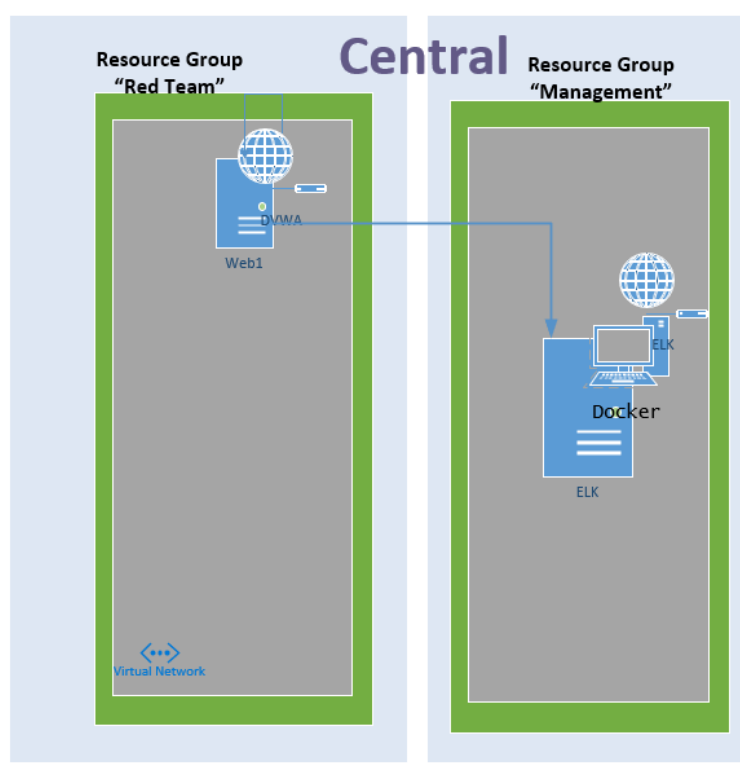
Day 2  
Start

# Where We Left Off

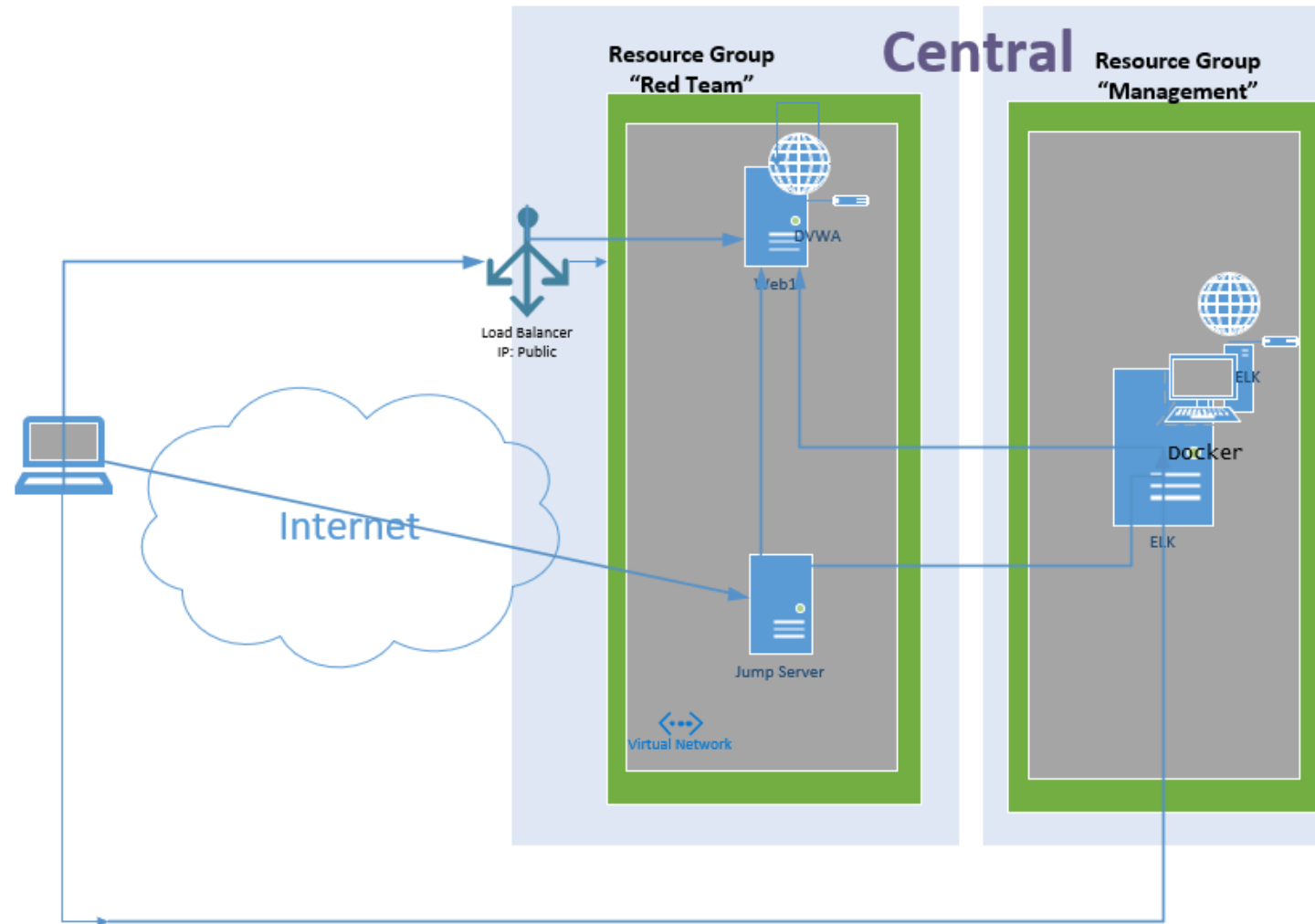


# Goal

## Push Logs from Web01 to ELK



# By the End of Today You Should Have



# Install File Beat on Web Server

1. SSH into the Web Server through the Jumpbox

```
#download filebeat
```

```
curl -L -O https://ln2.sync.com/dl/18aa05e60/zkc82r7a-adqnqwrk-9in3s62h-3yyj7kug
```

```
#rename file
```

```
mv zkc82r7a-adqnqwrk-9in3s62h-3yyj7kug filebeat-6.8.12-amd64.deb
```

```
#install filebeat
```

```
sudo dpkg -i filebeat-6.8.12-amd64.deb
```

ref: <https://www.elastic.co/guide/en/beats/filebeat/6.8/filebeat-installation.html>

# Download the Config File, Move it, and Add Dest Server

```
#download
curl -O -L https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat
#move
mv Filebeat /etc/filebeat/filebeat.yml
#open
Nano /etc/filebeat/filebeat.yml
#update Config to Point to ELK Server
```

Scroll to line #1106 and replace the IP address with the IP address of your ELK machine. And Update Password.

```
output.elasticsearch:
hosts: ["10.1.0.4:9200"]
username: "elastic"
password: "changeme"
```

Scroll to line #1806 and replace the IP address with the IP address of your ELK machine.

```
setup.kibana:
host: "10.1.0.4:5601"
```



# Open Port On Management NSG and Start Service

1. In Azure, navigate to the Management NSG and Open the needed port from Web Server to ELK = *9200*

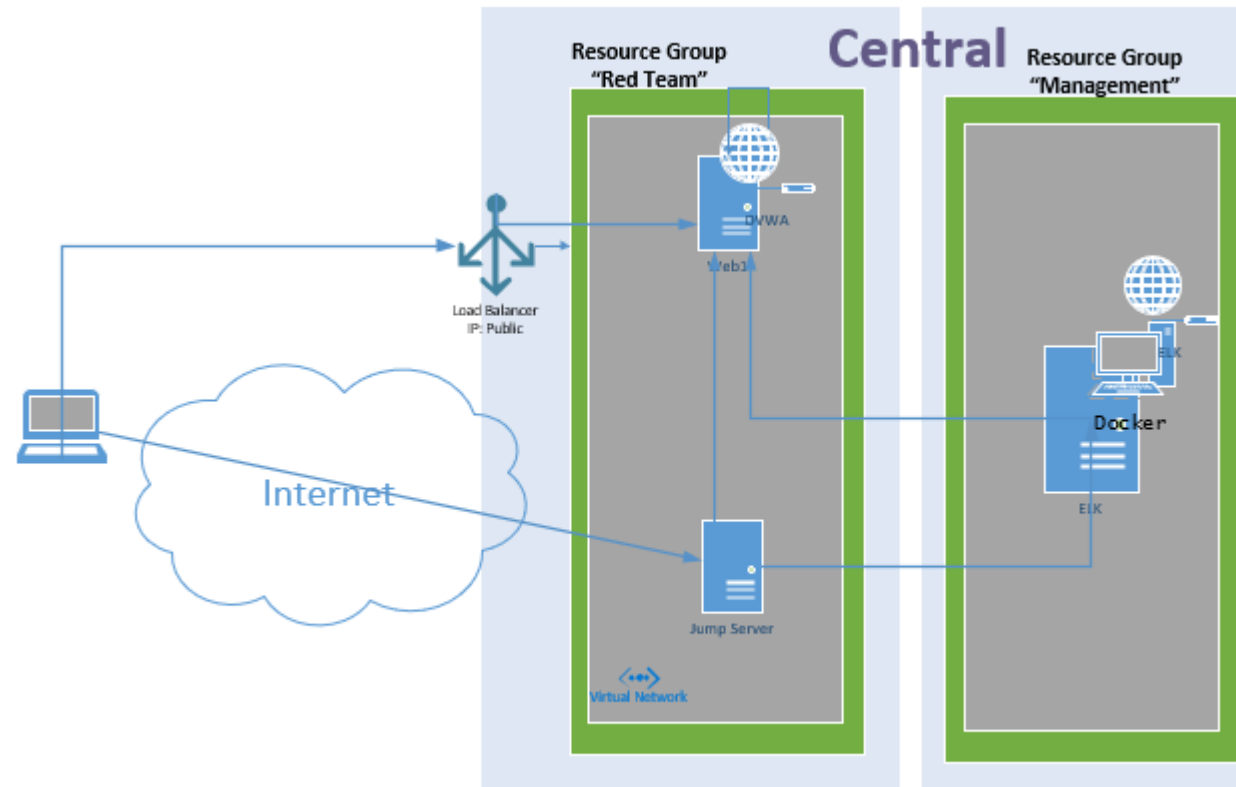
*2. After, Start the Filebeat on the Web Server*

```
filebeat modules enable system
```

```
filebeat setup
```

```
service filebeat start
```

# Final Elk Project



Day 2  
End

Day 3  
Start

# Home Work

- Create a Github Repository -  
[https://www.youtube.com/watch?v=XtCcoMd6U\\_4](https://www.youtube.com/watch?v=XtCcoMd6U_4)
- Create and Add a Network Diagram
- The Firewall Spreadsheet with access rules
- The “why”

Day 3  
End