



Project Week: ELK Stack

Cybersecurity
Project Week 1



12.1 - Project Week

Class Preparation

1. Check into BCS
2. Update your git repository with ``git pull``
3. Launch/login to your **PERSONAL** Azure Portal

Homeworks Due

- Unit 10 (Network Security): due last night
- Unit 11 (Cloud): due Sunday December 20
- Unit 12 (Project): due Sunday January 10

Upcoming Units

- Week 13: Cryptography (1/04 - 1/09)
- Weeks 14 & 15: Web Development, Vulnerabilities, and Hardening (1/11 - 1/23)

Schedule Notes

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

- Crypto delayed until after Winter Break

Holidays (No Class)

- Mon 1/18 (MLK Day)
- Mon 2/15 (Presidents' Day)



Welcome to Project Week!

This week, you will set up an ELK stack server to monitor your cloud network.

Project Week 1: ELK Stack

Placing an ELK monitoring stack within your virtual network will allow you to:

01

Easily collect logs from multiple machines into a single database.

02

Quickly execute complex searches, such as:

Find the 12 internal IP addresses that sent the most HTTP traffic to my gateway between 4 a.m. and 8 a.m. in April 2019.

03

Build graphs, charts, and other visualizations from network data.

Day 1: Configuring an ELK Stack

ELK Stack

- Deploying and configuring an ELK stack is a common task for network engineers.
- SOC analysts and other security professionals use it often.

Completing this project will provide convincing proof of your skills, which you can present to hiring managers.



ELK Stack

- The ELK stack is commonly used in network production.
- You'll likely work for organizations that use either ELK or Splunk, covered later in the course.
- Experience with both tools is a valuable addition to any job application.



ELK Stack

You can expand this network with additional machines on your own time to generate a lot of interesting log information.

This sort of independent research is useful for learning, and hiring managers love to see it.



Project Week 1: ELK Stack

You'll develop the following deliverables, which you can present in job interviews:

01

Network Diagram

An architecture diagram describing the topology of your network.

02

Technical Brief

Answers to a series of questions explaining the important features of the suite, completed after deploying the stack. This brief is often referred to as a README document.

03

GitHub Repository

When complete, you will save your work to a Git repository, along with an in-depth description. This makes it easy to redeploy your work in the future, and share it with others.

The ELK Stack

ELK

ELK is an acronym. Each letter stands for an open-source technology:



Elastic Stack

These tools are collectively known as **ELK stack**.



Search and analytics engine.

Server-side data processing pipeline that sends data Elasticsearch.

Tool for visualizing Elasticsearch data with charts and graphs.



- ELK started with Elasticsearch.
- It was initially designed to handle *any* kind of information. This means that logs and arbitrary file formats, such as PCAPs, can be easily stored and saved.



- After Elasticsearch became popular for logging, Logstash was added to make it easier to save logs from different machines into the Elasticsearch database.
- Logstash also processes logs before saving them, to ensure data from multiple sources has the same format before it is added to the database.



- Since Elasticsearch can store so much data, analysts often use visualizations to better understand the data at a glance.
- Kibana is designed to make it easy to visualize massive amounts of data in Elasticsearch.
- Kibana is known for its complex dashboards.

The Beats Family

Beats

The ELK stack works by storing log data in Elasticsearch with the help of Logstash.

- While functional, this approach is not ideal because it requires administrators to collect all data reported by tools like `syslog`, even if they only need a small portion of it.

For example: Administrators often need to monitor changes to specific files, such as `/etc/passwd`, or track specific information, such as a machine's uptime.

In cases like this, it is wasteful to collect all of the machine's log data in order to only inspect a fraction of it.

Beats

Recently, ELK addressed this issue by adding an additional tool to its data collection suite, called **Beats**.

- Beats are special-purpose data collection modules. Rather than collecting all a machine's log data, Beats allow you to collect only the very specific pieces you're interested in.
- ELK officially supports eight Beats. We will use two of them in this project:
 - **Filebeat** collects data about the file system.
 - **Metricbeat** collects machine metrics, such as uptime.



beats

Project Overview

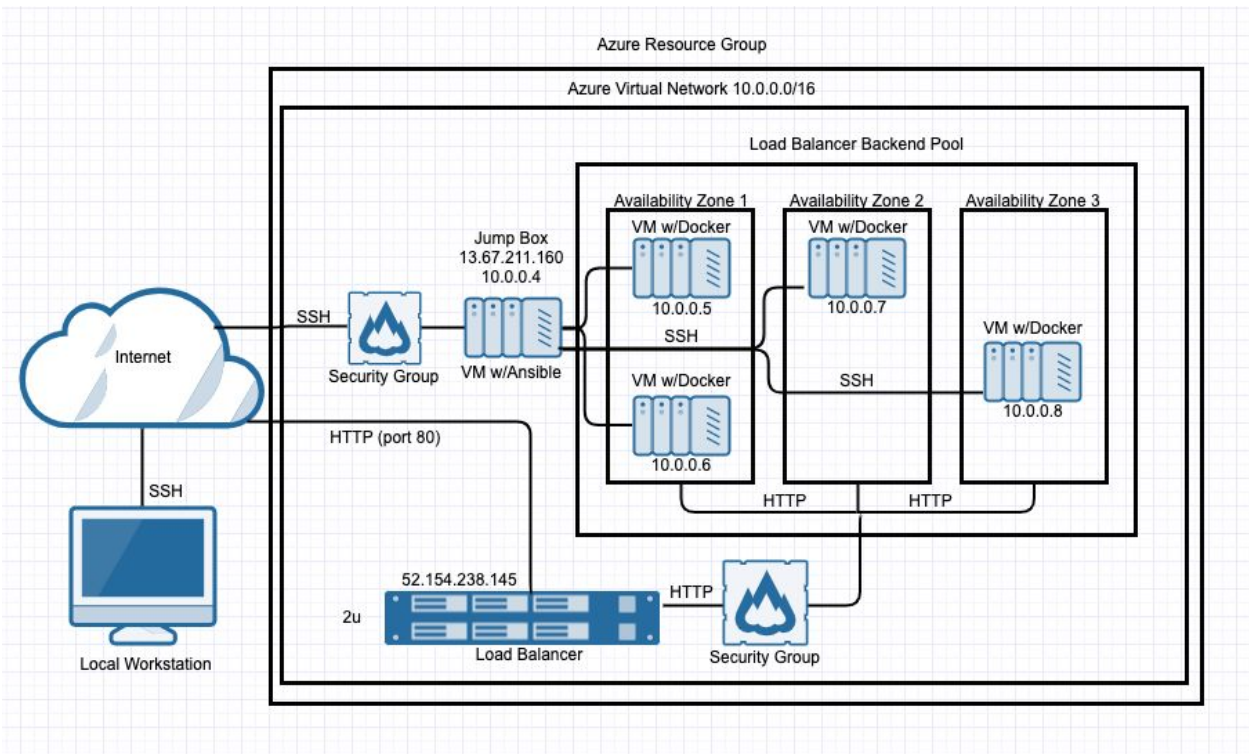


Now it's time to begin deploying.

Make sure you're logged into your **personal Azure account**, *not* your cyberxsecurity account.

Project Setup

We'll continue to build off the cloud week architecture.



This network has:

A gateway: the jump box configured during the cloud week.

Three additional VMs: one configuring the others, and two functioning as load-balanced web servers.



Project Milestones



Day 1: Configure the ELK server.



Day 2: Install Filebeat and Metricbeat.



Day 3: Finish leftover work, and create a network diagram and documentation.

Working Ahead



You are free to work ahead of the day's activity if you would like to



We will only be assisting students with issues relating to the current day's activities



So you are on your own if you'd like to work ahead (at least until next class)

Configure the ELK Server

The rest of today will consist of the following:

01

Create a VM. Deploy a new VM onto the network to host the ELK server.

02

Download and configure the container. Download and configure the elk-docker container on the new VM.

03

Launch and expose the container. Launch the elk-docker container to start the ELK server.

04

Implement identity and access management. Configure your preexisting security group so you can connect to ELK via HTTP and view it through the browser.

Hints/Suggestions

01

Read the instructions.

02

Slow down and read all the instructions.

03


Don't skip any steps that are in the instructions

04


Seriously - slow down and follow ALL the instructions, paying particular attention to notes about VM sizes, which network to use, etc.

Target Accomplishments


By the end of this class, you should have completed the following:

A teal-colored circle containing the text "Deployed a new VM on your virtual network." data-bbox="117 420 278 566">

Deployed a new
VM on your
virtual network.

A dark blue-colored circle containing the text "Created an Ansible play to install and configure an ELK instance." data-bbox="422 370 573 625">

Created an
Ansible play to
install and
configure an
ELK instance.

A dark purple-colored circle containing the text "Restricted access to the new server." data-bbox="727 424 870 569">

Restricted
access to the
new server.

Completing these steps required you to leverage your systems administration, virtualization, cloud, and automation skills. This is an impressive set of tools to have in your toolkit.



Day 1 Activity: ELK Installation

For the remainder of class, you will work on the ELK installation, configuration, launch.

Suggested Time:
Full Class Time

