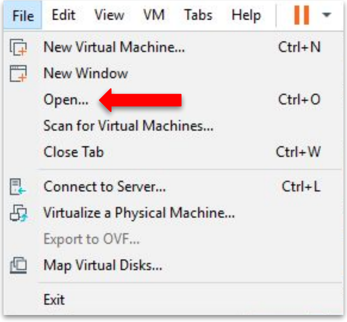
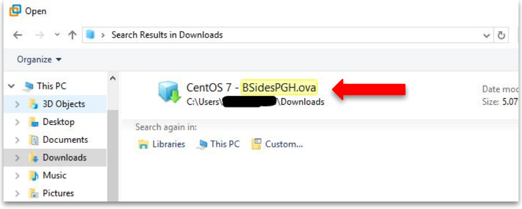
Import the Workshop OVA Files

1

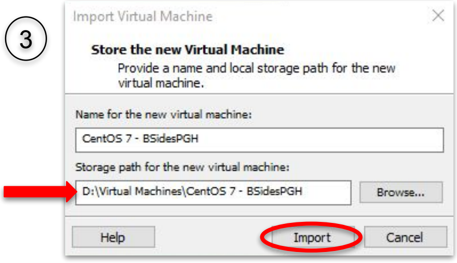

File
Edit
View
VM
Tabs
Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Scan for Virtual Machines...
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Virtualize a Physical Machine...
Export to OVF...
Map Virtual Disks...
Exit

2



CentOS 7 - BSidesPGH.ova
C:\Users\[redacted]\Downloads

3



Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: CentOS 7 - BSidesPGH

Storage path for the new virtual machine: D:\Virtual Machines\CentOS 7 - BSidesPGH

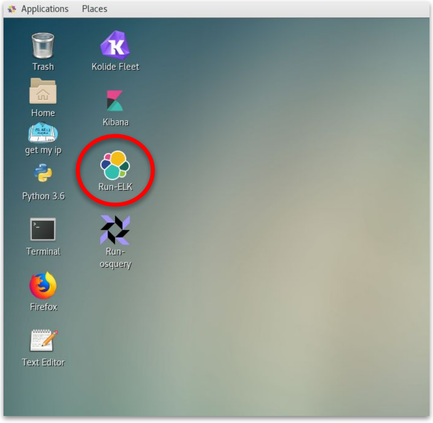
We'll use the provided virtual machines throughout the day. You should have already installed a copy of VMWare Workstation, but if you haven't, there is a trial copy available on the workshop USB drive.

Please copy the files on the USB to your hard drive and follow the steps below:

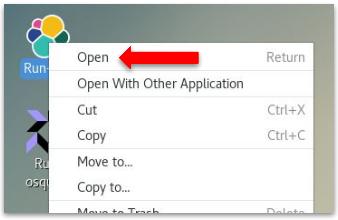
1) In VMWare, click the **File** menu, then select **Open…**
2) Select the **CentOS 7 - BSidesPGH.ova** and click **Open**
3) Choose a path on your host to store the virtual machine and click **Import**. **DO NOT** attempt to run these from a USB drive - make sure they're saved to your hard drive.
4) Repeat these steps with the **Windows Server 2016.ova**

Start-up and Configure the Workshop Environment

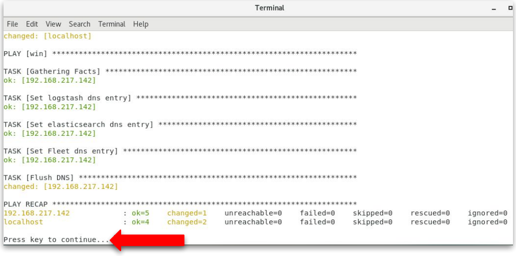
1



2



3



```
changed: [localhost]

PLAY [win] *********************************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.217.142]

TASK [Set logstash dns entry] **************************************************
ok: [192.168.217.142]

TASK [Set elasticsearch dns entry] *********************************************
ok: [192.168.217.142]

TASK [Set Fleet dns entry] *****************************************************
ok: [192.168.217.142]

TASK [Flush DNS] ***************************************************************
changed: [192.168.217.142]

PLAY RECAP *********************************************************************
192.168.217.142            : ok=5    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
localhost                  : ok=4    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

Press key to continue...
```

The set-up and configuration of the ELK environment for both the CentOS and Windows hosts are automated using Ansible playbooks. You're welcome to view all the playbooks used to build the environment by navigating to **/opt/playbooks**.

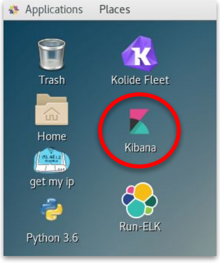
Instead of running through all the playbooks, configuring DNS and multiple other requirements, we've created a desktop shortcut to run the playbooks and simplify the process by automating it. **DO NOT** start the following until both OVA files have been imported and are running on your host (please ask if you have problems with this step).

For reference, the account credentials for the **CentOS** vm are: **analyst/bsides**. For the **Windows** box, they're **admin/admin**.

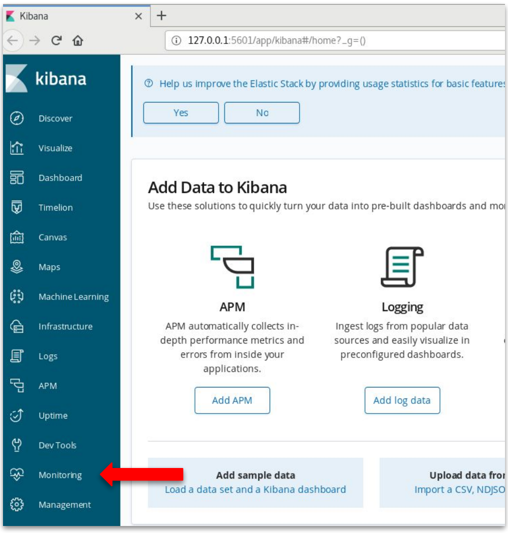
1) On the desktop of the CentOS host, right-click the **Run-ELK** shortcut and select **Open**
2) A terminal window will pop-up and begin running Ansible playbooks to set-up both the ELK environment and the Windows Server to send logs to it. This will take a while.
3) The terminal should complete without error. The playbooks are finished running if you see **Press key to continue...** If you see bright-red text instead, please notify one of us.
4) Repeat the steps above with the **Run-osquery** shortcut that's also located on the desktop.

Check ELK is Running

1



3



Help us improve the Elastic Stack by providing usage statistics for basic features

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and mo

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add sample data

Load a data set and a Kibana dashboard

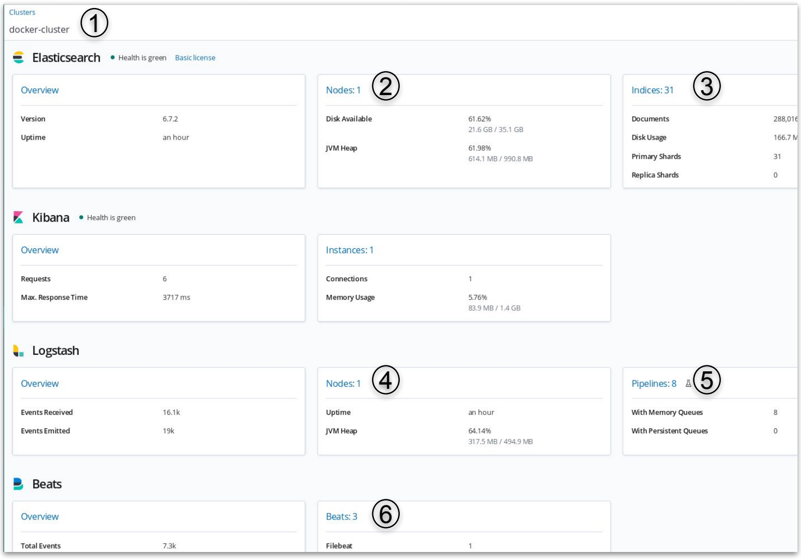
Upload data fro

Import a CSV, NDJSO

We need to check that everything is working. To do so, we're going to use Kibana's monitoring feature to see what's talking to Elasticsearch.

1) On the desktop of the CentOS host, right-click the **Kibana** shortcut and select **Open**
2) This should open Kibana in Firefox. You can also login from a browser on your host OS by navigating to **http://<ip_of_centos_vm>:5601**. You can easily determine the IP by using the shortcut on the CentOS Desktop called **get my ip**.
3) Once Kibana opens, click the **Monitoring** link in the left toolbar.

Check ELK is Running



Clusters

docker-cluster

Elasticsearch • Health is green Basic license

Overview

Version 6.7.2

Uptime an hour

Nodes: 1

Disk Available 61.62%
21.6 GB / 35.1 GB

JVM Heap 61.98%
614.1 MB / 990.8 MB

Indices: 31

Documents 288,016

Disk Usage 166.7 M

Primary Shards 31

Replica Shards 0

Kibana • Health is green

Overview

Requests 6

Max. Response Time 3717 ms

Instances: 1

Connections 1

Memory Usage 5.76%
83.9 MB / 1.4 GB

Logstash

Overview

Events Received 16.1k

Events Emitted 19k

Nodes: 1

Uptime an hour

JVM Heap 64.14%
317.5 MB / 494.9 MB

Pipelines: 8

With Memory Queues 8

With Persistent Queues 0

Beats

Overview

Total Events 7.3k

Beats: 3

Filebeat 1

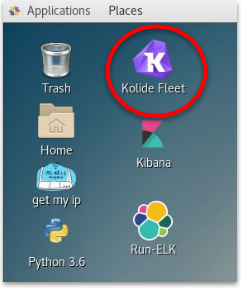
We can see the status of all the different components in ELK from the monitoring view in Kibana. We'll walk through a few here just to check that everything is configured as expected and able to talk to ELK.

These terms and how these pieces all fit together may not make sense yet, and that's okay. We'll talk about what each of these does shortly. For now, we just want to make sure everything is in its expected state.

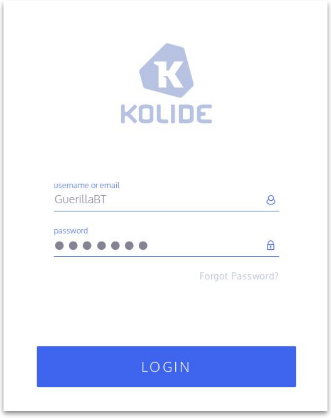
1) The Elasticsearch cluster name should be **docker-cluster**.
2) There should be one node under the **Elasticsearch** section. If you see zero or more than one node, something went wrong (please tell us).
3) You should see at least 30 indices under the **Elasticsearch** section. If you have more than that, that is expected. If you have fewer, please let us know.
4) In the **Logstash** section you should see one node.
5) There should also be eight pipelines in the **Logstash** section.
6) Under the **Beats** section, there should be three Beats, one of each of the following: **Filebeat, Packetbeat, and Winlogbeat**.

Check Kolide Fleet is Running

1



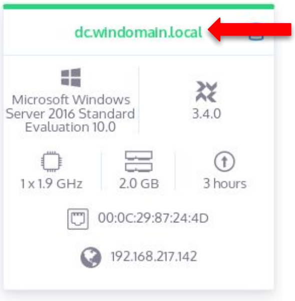
4



username or email: GuerillaBT

password: ●●●●●●●

5



dc.windomain.local

Microsoft Windows Server 2016 Standard Evaluation 10.0

3.4.0

1 x 1.9 GHz

2.0 GB

3 hours

00:0C:29:87:24:4D

192.168.217.142

We need to check that everything is working. To do so, we're going to use Kibana's monitoring feature to see what's talking to Elasticsearch.

1) On the desktop of the CentOS host, right-click the **Kolide Fleet** shortcut and select **Open**
2) This should open the Kolide Fleet login page in Firefox.
3) You'll be presented with a warning that **Your connection is not secure** because we're using a self-signed certificate. Click **Advanced** > **Add Exception…** > **Confirm Security Exception**.
4) The Kolide Fleet login page should load. Login using the following credentials:

   Username: **GuerillaBT**
   Password: **bsid3s!**

5) Once you login, you should see the host **dc.windomain.local** in the center of the browser window.
6) That's it! If you've got this far, everything should be working and properly configured.