KPLABS Course

Splunk 2021 - Beginner to Architect

Domain 1

ISSUED BY

Zeal

REPRESENTATIVE

instructors@kplabs.in

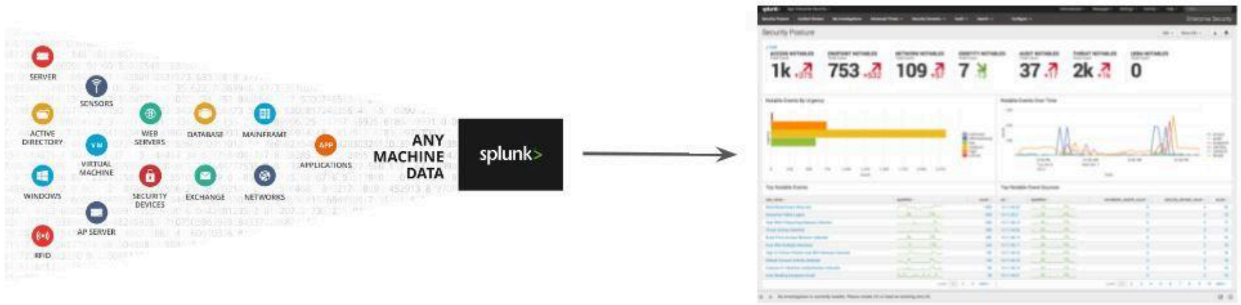
Domain 1 - Introduction to Splunk & Setting Up Labs

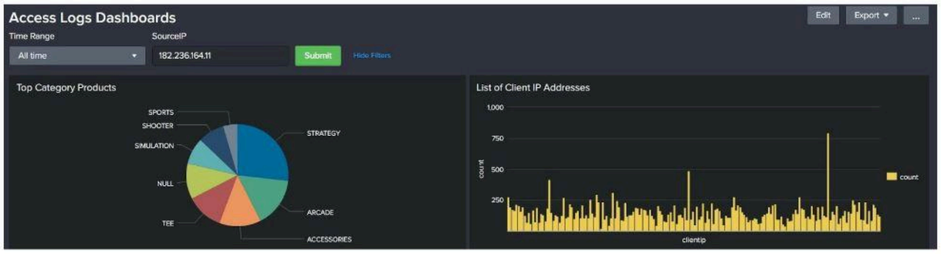
Module 1: Introduction to Splunk

1.1 Overview of Splunk

Splunk is one of the most popular log analyzing and monitoring tools.

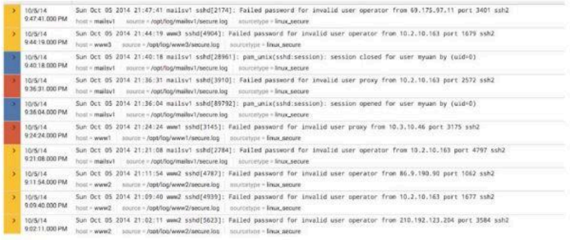
Splunk is a software platform to search, analyze and visualize the machine-generated data gathered from a wide variety of devices.




Access Logs Dashboards

Time Range: All time

SourceIP: 182.236.164.11

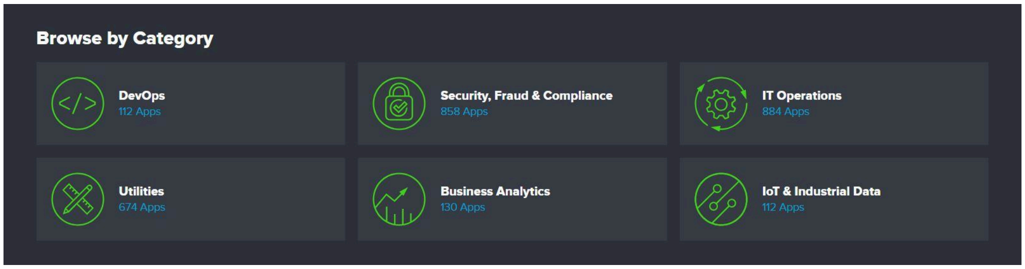


```
10/5/14      Sun Oct 05 2014 21:47:41 mailsv1 sshd[2174]: Failed password for invalid user operator from 69.175.97.11 port 3401 ssh2
9:47:41.000 PM  host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:44:19 www3 sshd[4904]: Failed password for invalid user operator from 10.2.10.163 port 1679 ssh2
9:44:19.000 PM  host = www3   source = /opt/log/www3/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:40:18 mailsv1 sshd[28961]: pam_unix(sshd:session): session closed for user myuan by (uid=0)
9:40:18.000 PM  host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:36:31 mailsv1 sshd[3910]: Failed password for invalid user proxy from 10.2.10.163 port 2572 ssh2
9:36:31.000 PM  host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:36:04 mailsv1 sshd[89792]: pam_unix(sshd:session): session opened for user myuan by (uid=0)
9:36:04.000 PM  host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:24:24 www1 sshd[3145]: Failed password for invalid user proxy from 10.3.10.46 port 3175 ssh2
9:24:24.000 PM  host = www1   source = /opt/log/www1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:21:08 mailsv1 sshd[2784]: Failed password for invalid user operator from 10.2.10.163 port 4797 ssh2
9:21:08.000 PM  host = mailsv1   source = /opt/log/mailsv1/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:11:54 www2 sshd[4787]: Failed password for invalid user operator from 86.9.190.90 port 1062 ssh2
9:11:54.000 PM  host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:09:40 www2 sshd[4939]: Failed password for invalid user operator from 10.2.10.163 port 1677 ssh2
9:09:40.000 PM  host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
10/5/14      Sun Oct 05 2014 21:02:11 www2 sshd[5623]: Failed password for invalid user operator from 210.192.123.204 port 3584 ssh2
9:02:11.000 PM  host = www2   source = /opt/log/www2/secure.log   sourcetype = linux_secure
```

1.2 Powerful Marketplace

Splunk has its own marketplace referred to as splunkbase where people can submit their apps and add-ons.

This allows customers to use out-of-box solutions for a wide variety of use-cases.



Browse by Category

DevOps
112 Apps

Security, Fraud & Compliance
858 Apps

IT Operations
884 Apps

Utilities
674 Apps

Business Analytics
130 Apps

IoT & Industrial Data
112 Apps

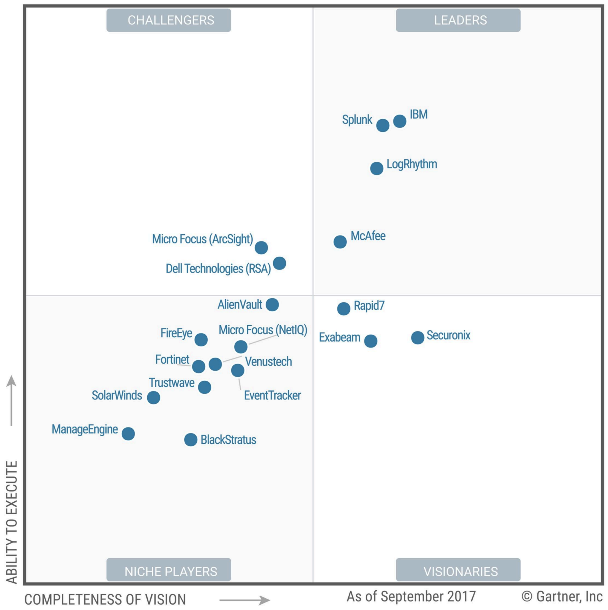
1.3 Splunk is More than Log Monitoring Solution

When a software platform is powerful in searching, analyzing, and visualizing, it can be used for much wider areas.

Splunk has been promoting new apps in various niche-specific areas like:

- Security information and event management (SIEM)
- Splunk IT Service Intelligence
- Splunk User Behavior Analytics

Figure 1. Magic Quadrant for Security Information and Event Management



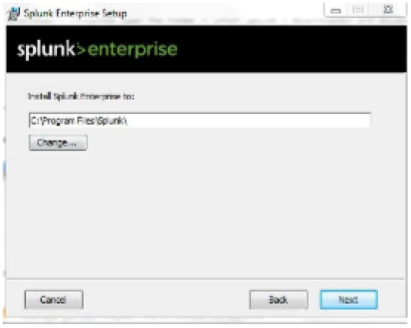
Source: Gartner (December 2017)

Module 2: Installation Methods for Splunk

2.1 Installation Options

There are two primary ways for installing Splunk:

- Download and install a Splunk Enterprise installation package
- Download the Splunk Enterprise Docker image

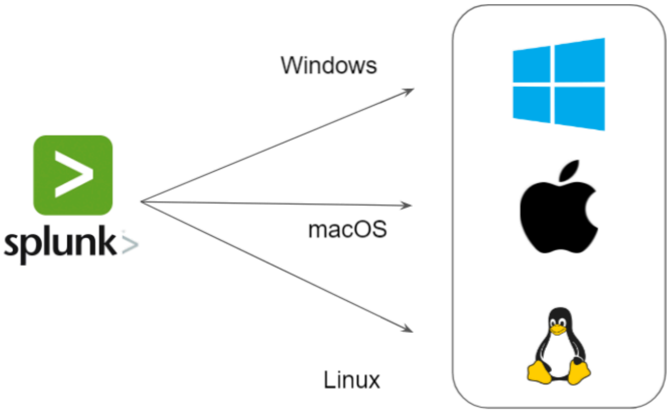


Install Splunk Enterprise to:

C:\Program Files\Splunk\

2.2 Installing Splunk via Installation Package

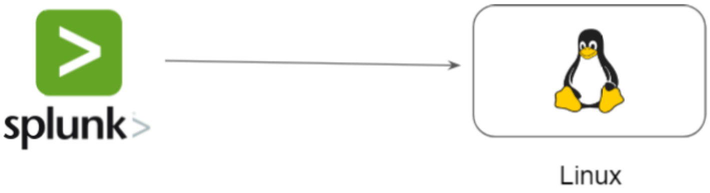
Splunk can be installed in a wide variety of operating systems.



Not All versions*

2.3 Preferred Choice for Splunk Installation Method

The preferred OS for Splunk installation would be Linux.



2.4 Revising the Choices

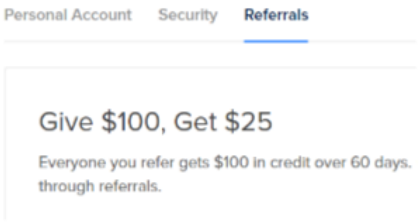
Following diagram illustrates the architecture that we will be following in this course:

Criteria	Choices
Operating System	Ubuntu
Cloud Provider	Digital Ocean

2.5 Why Digital Ocean?

Digital Ocean allows developers to quickly deploy, manage and scale cloud infrastructure without much complexity at an affordable cost.

They provide multiple coupon codes which gives great amount of credits ranging from $50-100 USD for new users.



Give $100, Get $25

Everyone you refer gets $100 in credit over 60 days. through referrals.

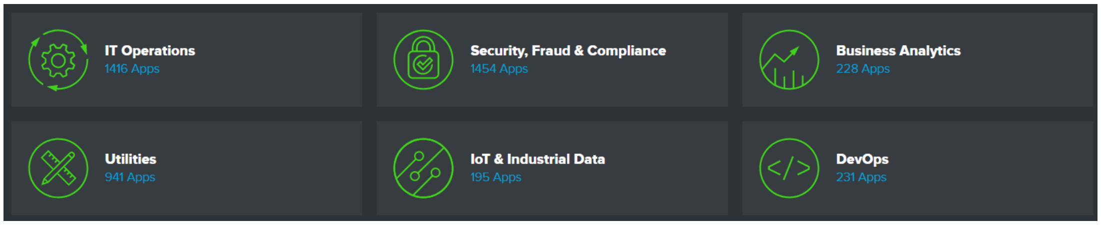
Module 3: Creating Splunk Account

3.1 Overview of Splunk Account

Creating a Splunk account is an important first step and it allows users to perform various operations.

Some of these include:

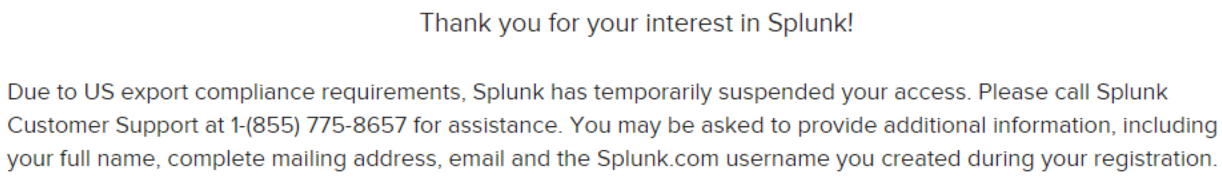
- Free Trials and Downloads
- Download Apps and Add-Ons from Splunk Marketplace.



3.2 Overview of Splunk Account

Sometimes, the Splunk signup process might fail due to restrictions based on name and countries part of a consolidated list.

The Consolidated List is a list of all persons and entities who are subject to targeted financial sanctions



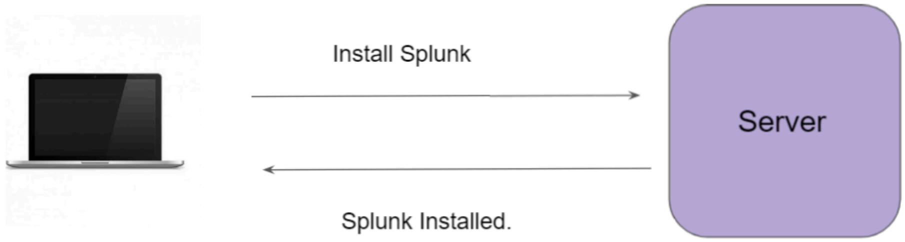
Thank you for your interest in Splunk!

Due to US export compliance requirements, Splunk has temporarily suspended your access. Please call Splunk Customer Support at 1-(855) 775-8657 for assistance. You may be asked to provide additional information, including your full name, complete mailing address, email and the Splunk.com username you created during your registration.

Module 4: Infrastructure for Splunk

4.1 Creating Infrastructure for Splunk

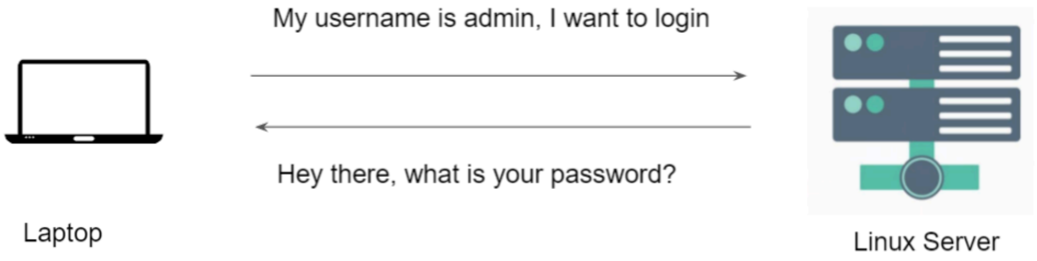
To begin with the Splunk installation process, we need one server hosting Ubuntu OS.

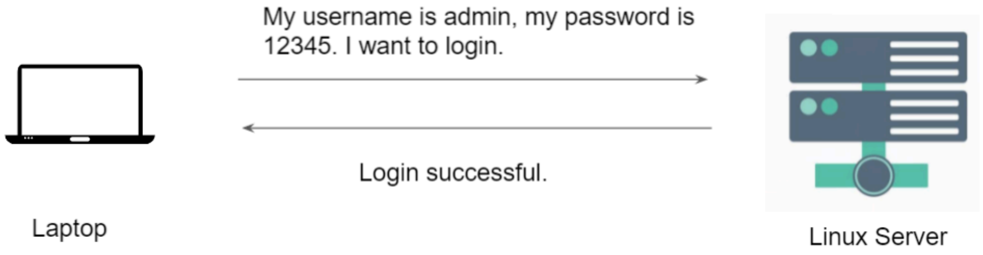


4.2 Creating Infrastructure for Splunk

There can be multiple methods for authentication against a system.

Password based authentication is the simplest form.


My username is admin, I want to login
Hey there, what is your password?
Laptop
Linux Server


My username is admin, my password is 12345. I want to login.
Login successful.
Laptop
Linux Server

4.3 Challenges with Password Based Authentication

Password based authentication is generally considered to be less-secure.

Many users write down the passwords in notepad files or as part of sticky notes.

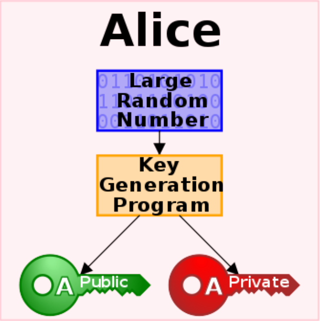
Most users would not create a complex password that is difficult to hack.

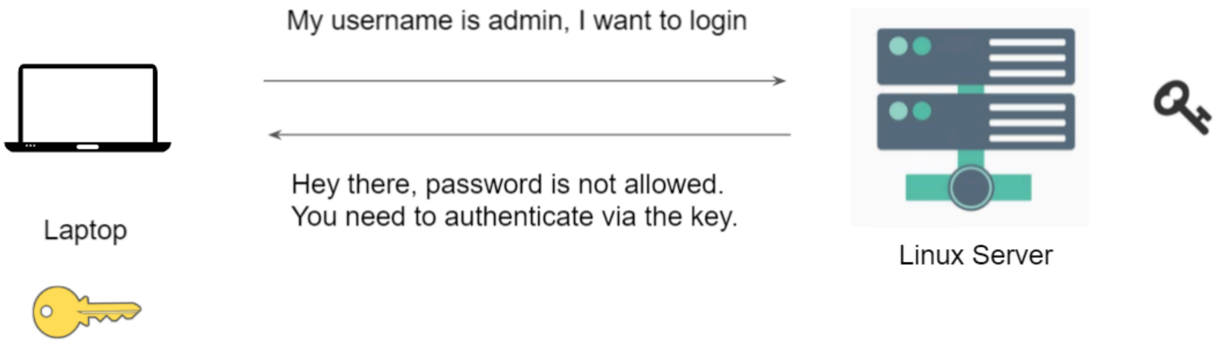
4.4 Key Based Authentication

In this type of authentication, there are two special keys that are generated.

One key is called a Public Key and the second key is called a Private key.

If the public key is stored in server and is used as authentication mechanism, only the corresponding private key can be used to successfully authenticate.

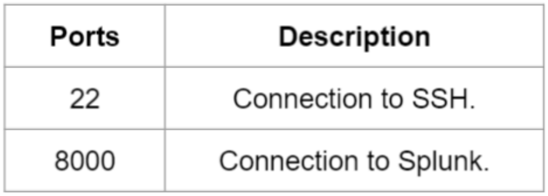



My username is admin, I want to login
Hey there, password is not allowed.
You need to authenticate via the key.
Laptop
Linux Server

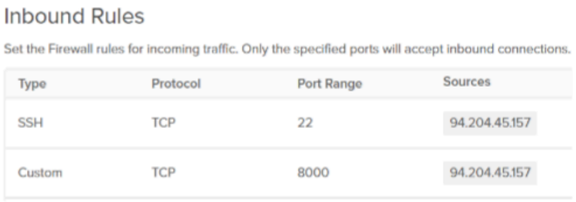
4.5 Firewall Rules

We do not want the entire internet to connect to our server.

With the help of Firewall, you can restrict the connection to your Splunk instance.



Ports	Description
22	Connection to SSH.
8000	Connection to Splunk.



Inbound Rules

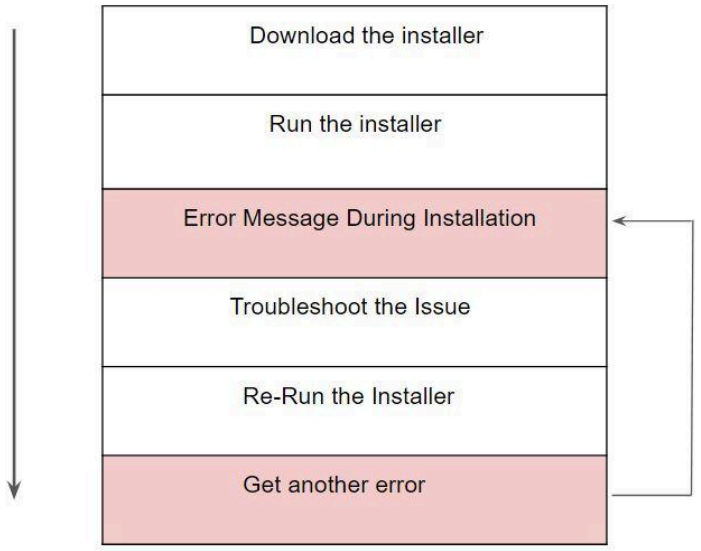
Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections.

Type	Protocol	Port Range	Sources
SSH	TCP	22	94.204.45.157
Custom	TCP	8000	94.204.45.157

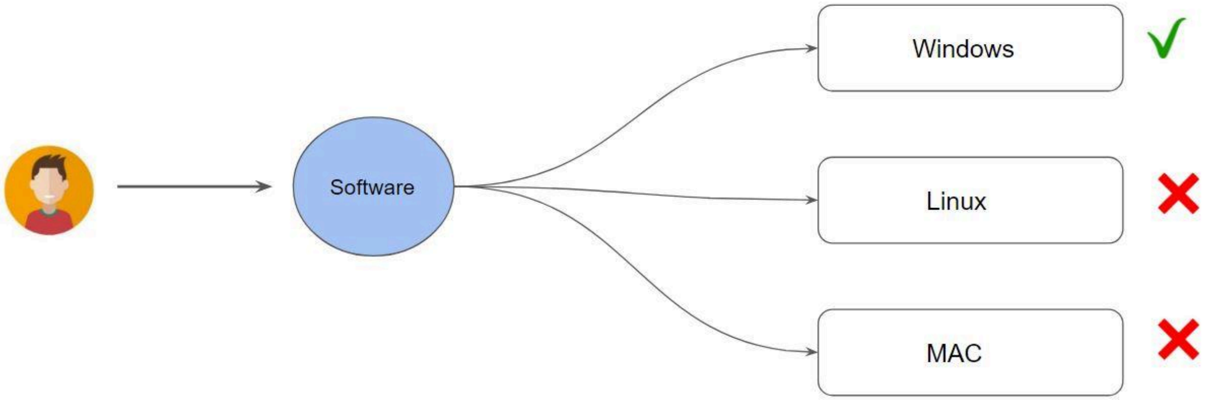
Module 5: Introduction to Docker

5.1 Understanding the Challenge

Every software has its own set of prerequisite dependencies which much be present before the installation. This leads to many sets of challenges depending on the operating system used.



Along with the above challenge, the second primary issue is related to OS compatibility. Software written for Windows might not work for Linux and MAC and so on.



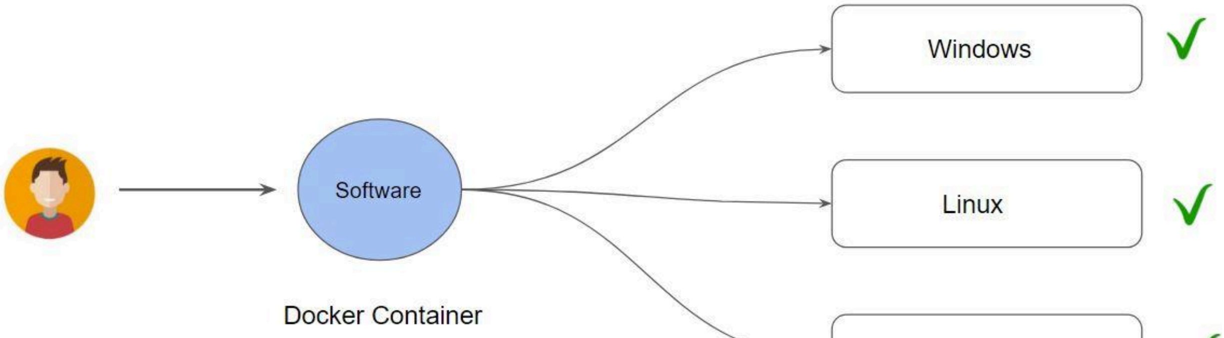
These are some of the primary challenges which Docker is trying to solve.

5.2 Introduction to Docker

Docker is a technology designed to make it easier to create, deploy, and run applications by using containers.

Docker is an open platform, once we build a docker container, we can run it anywhere, say it windows, Linux, mac whether on a laptop, data center, or in the cloud.

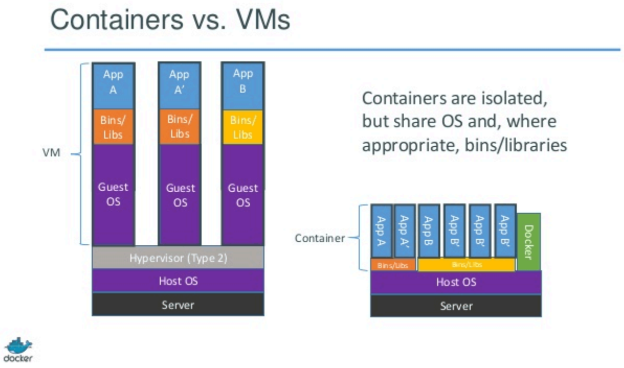
It follows the build once, run anywhere approach.



Docker Container

5.3 Docker Containers vs Virtual Machines

- Virtual Machine contains the entire Operating System.
- The container uses the resource of the host operating system

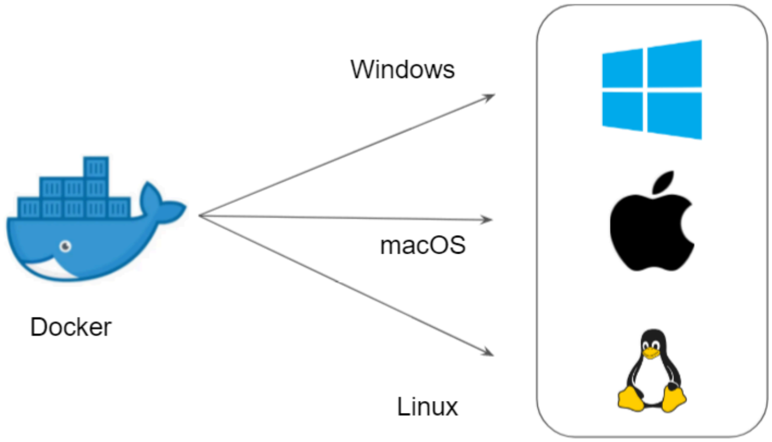

Containers vs. VMs

Containers are isolated, but share OS and, where appropriate, bins/libraries

Module 6: Installation Methods for Docker

6.1 Installing Docker

Docker can be installed in a wide variety of operating systems.



6.2 Revising the Preferred Choice

To begin with, you can install Docker Desktop directly within your laptop.

The preferred OS for Docker installation would be Linux.

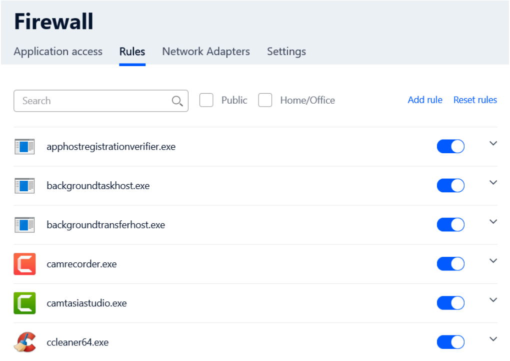
Docker
Linux

6.3 Why is Linux a Preferred Method?

Every user has a different version of the Operating System with a specific set of updates.

Many users have 3rd party firewalls or other security products on their workstation that can lead to issues.

As an Instructor, it is difficult to troubleshoot individual laptop configuration.



Firewall

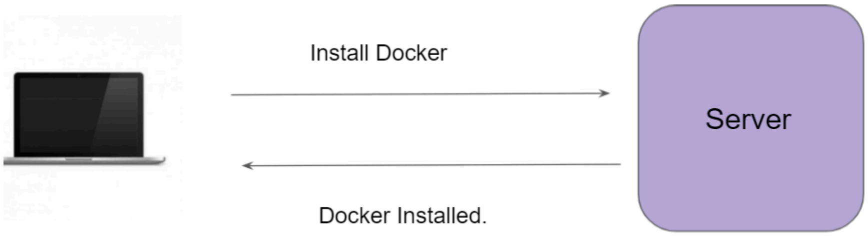
Application access | Rules | Network Adapters | Settings

Search | □ Public | □ Home/Office | Add rule | Reset rules

- apphostregistrationverifier.exe
- backgroundtaskhost.exe
- backgroundtransferhost.exe
- camrecorder.exe
- camtasiastudio.exe
- ccleaner64.exe

6.4 Creating Infrastructure for Docker

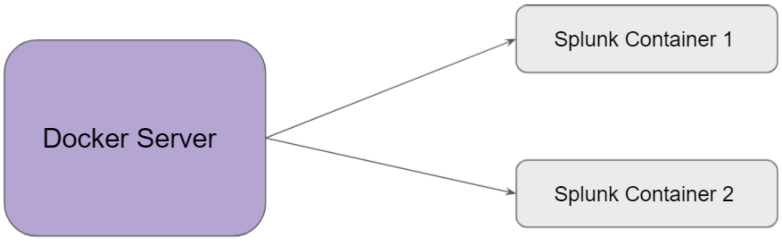
To begin with the Docker installation process, we need one server hosting Ubuntu OS.



Module 7: Deploying Splunk Docker Container

7.1 Splunk Infrastructure via Docker

Once we have Docker up and running, we can launch a Splunk Docker container to get started.



7.2 Basic Docker Commands

Let us explore the most important Docker commands that will often be used.

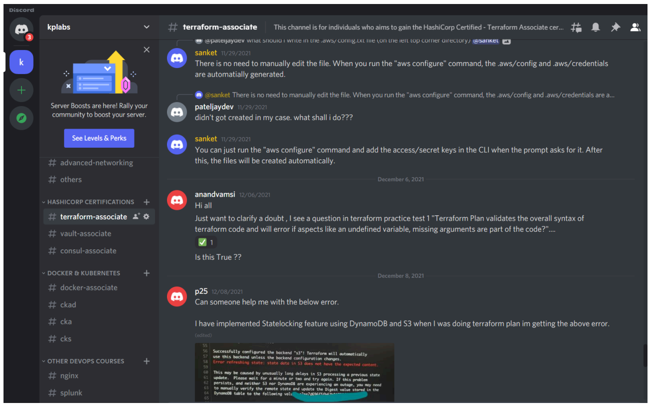
Basic Commands	Description
docker ps	Shows list of running containers.
docker ps -a	Show all containers
docker stop [container-name]	Stops Docker Container
docker start [container-name]	Starts Docker container
docker rm [container-name]	Remove Docker container

Join Our Discord Community

We invite you to join our Discord community, where you can interact with our support team for any course-based technical queries and connect with other students who are doing the same course.

Joining URL:

http://kplabs.in/chat



terraform-associate This channel is for individuals who aims to gain the HashiCorp Certified - Terraform Associate cer...

@pateljaydev what should i write in the .aws/config.txt file (on the left top corner directory) @sanket

sanket 11/29/2021
There is no need to manually edit the file. When you run the "aws configure" command, the .aws/config and .aws/credentials are automatially generated.

@sanket There is no need to manually edit the file. When you run the "aws configure" command, the .aws/config and .aws/credentials are a...

pateljaydev 11/29/2021
didn't got created in my case. what shall i do???

sanket 11/29/2021
You can just run the "aws configure" command and add the access/secret keys in the CLI when the prompt asks for it. After this, the files will be created automatically.

December 6, 2021

anandvamsi 12/06/2021
Hi all
Just want to clarify a doubt , I see a question in terraform practice test 1 "Terraform Plan validates the overall syntax of terraform code and will error if aspects like an undefined variable, missing arguments are part of the code?"....
✅ 1
Is this True ??

December 8, 2021

p25 12/08/2021
Can someone help me with the below error.

I have implemented Statelocking feature using DynamoDB and S3 when I was doing terraform plan im getting the above error.
(edited)

```
Successfully configured the backend "s3"! Terraform will automatically
use this backend unless the backend configuration changes.
Error refreshing state: state data in S3 does not have the expected content.

This may be caused by unusually long delays in S3 processing a previous state
update.  Please wait for a minute or two and try again. If this problem
persists, and neither S3 nor DynamoDB are experiencing an outage, you may need
to manually verify the remote state and update the Digest value stored in the
DynamoDB table to the following valu[redacted]
```