

# Building a Pipeline for Secure VMs in AWS

Shaun McCullough  
@thecybergooof



# The Pipeline for Building Virtual Machines



# The Pipeline for Building Virtual Machines



Redeploy Everywhere Daily

# The Pipeline for Building Virtual Machines



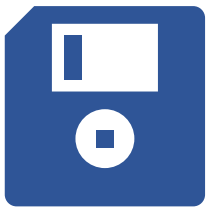
Solid Baseline



# Start with a Solid VM Baseline

- Cloud Service Provided
- Marketplace
- Shared by Stranger
- On Prem





AWS Linux 2

Patch Prepare

Configure App

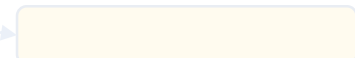
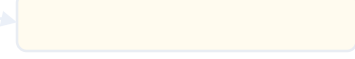
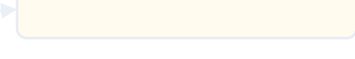
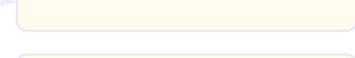
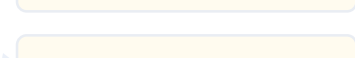
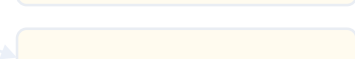
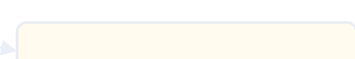
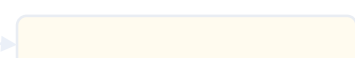
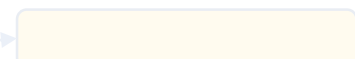
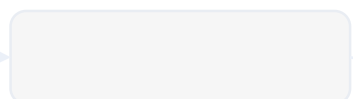
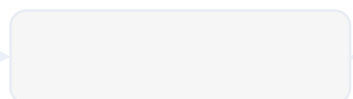
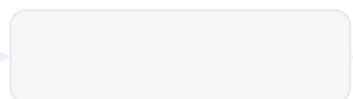
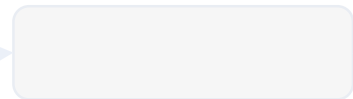
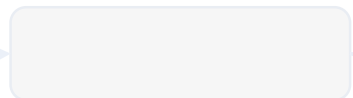
Windows

Centos 7.x

Centos 8.x

Ubuntu  
16.04

Marketplace  
Image



# The Pipeline for Building Virtual Machines



Solid Baseline



Patch and Prepare

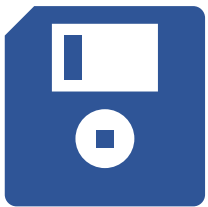




# Patch and Prepare

- Prepare image for security and operational requirements
- CIS Benchmarks are a great place to start
- Enforce security policies through code
- Dev teams build off these images





AWS Linux 2

Patch Prepare

Configure App

Windows

Centos 7.x

Centos 8.x

Ubuntu  
16.04

Marketplace  
Image



# The Pipeline for Building Virtual Machines



Solid Baseline



Patch and Prepare



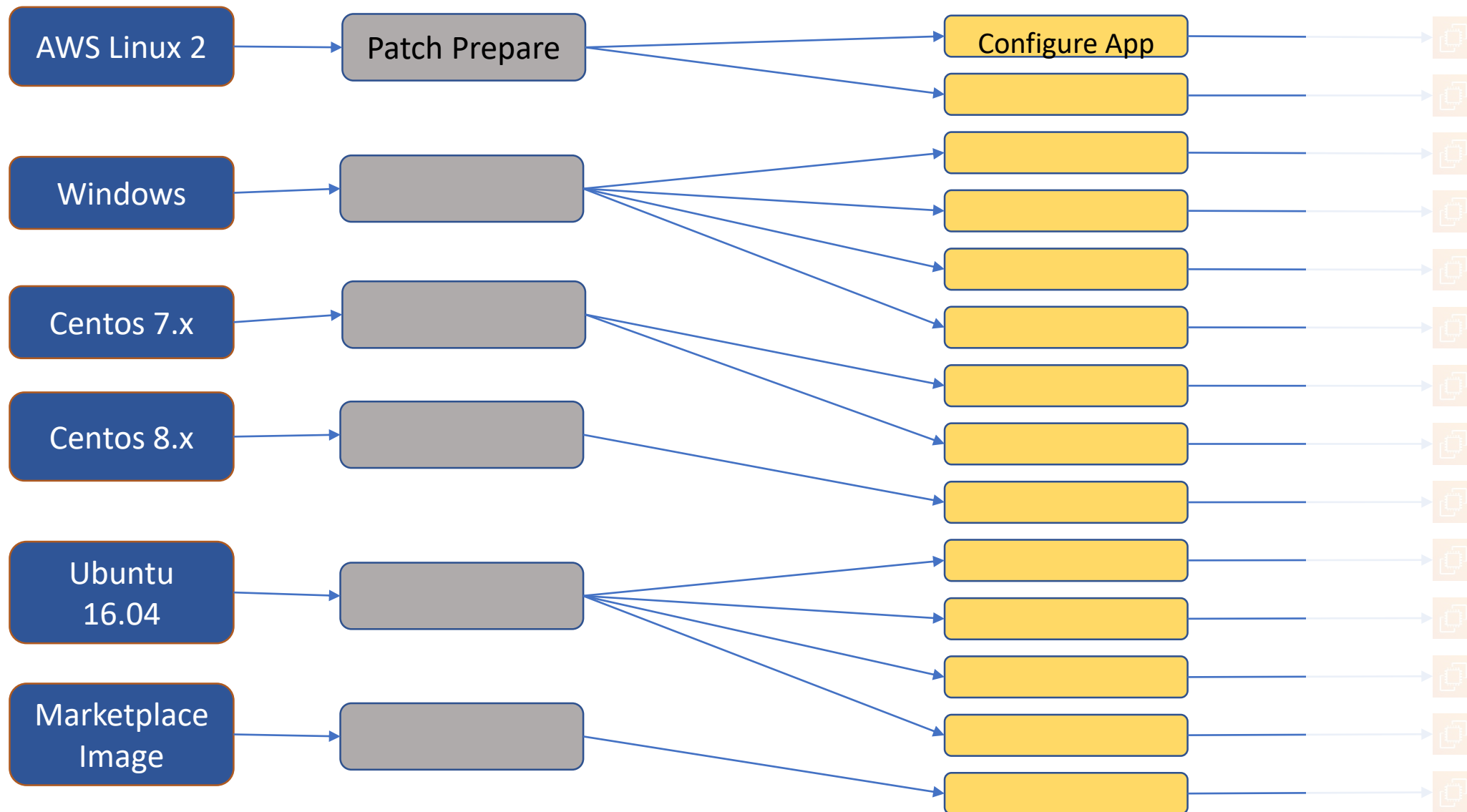
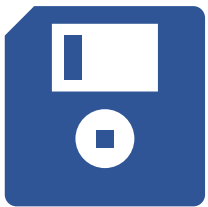
Deployable Image



# Deployable Image

- Install required libraries and configs
- Deploy app right from source control
- Test now, before deployments
- Save Image, deploy when needed





# The Pipeline for Building Virtual Machines



Solid Baseline



Patch and Prepare



Deployable Image

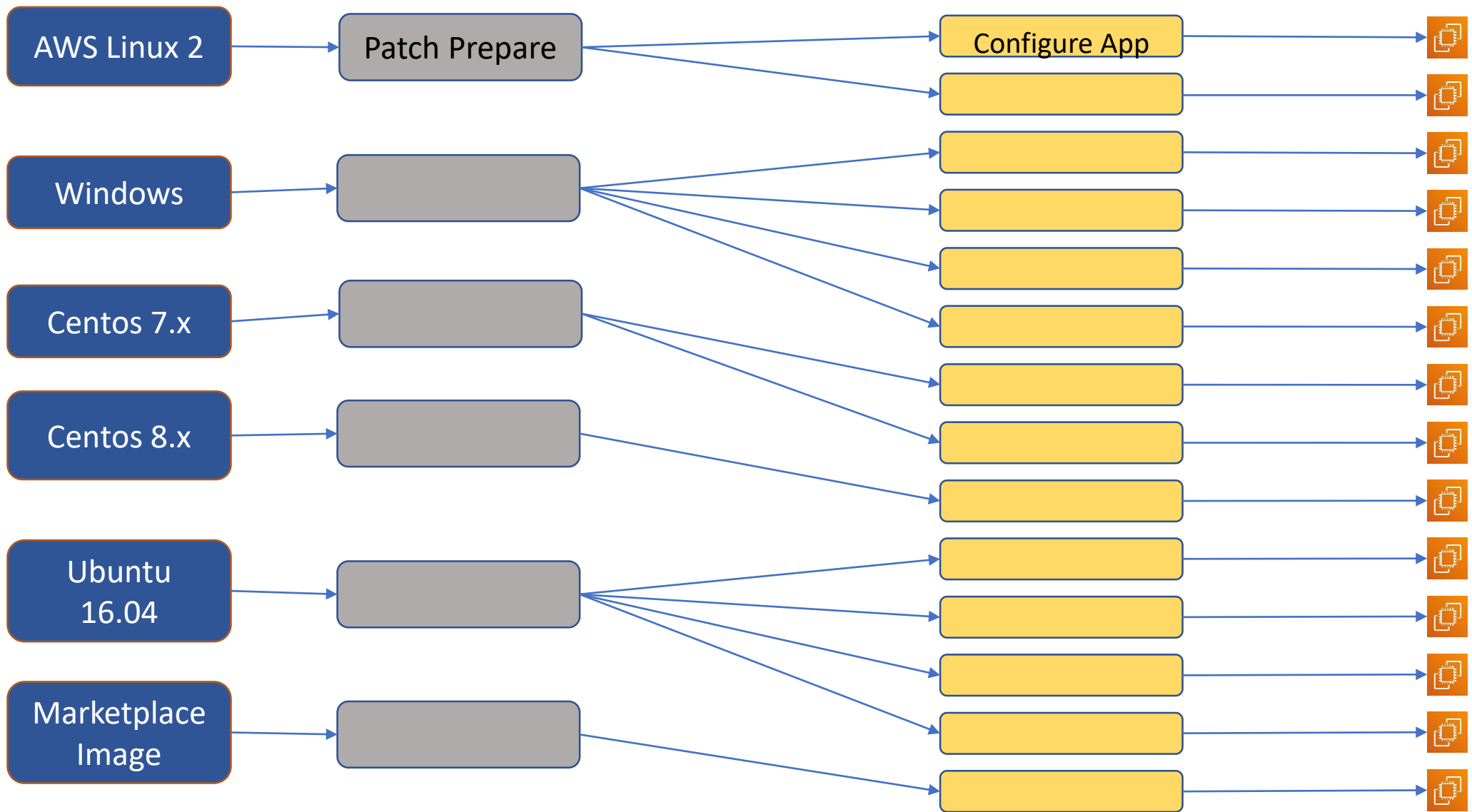
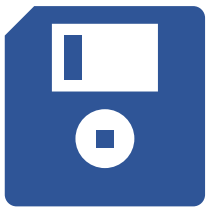


Redeploy Everywhere Daily



# Redeploy Everywhere Daily (or weekly) (or whenever)

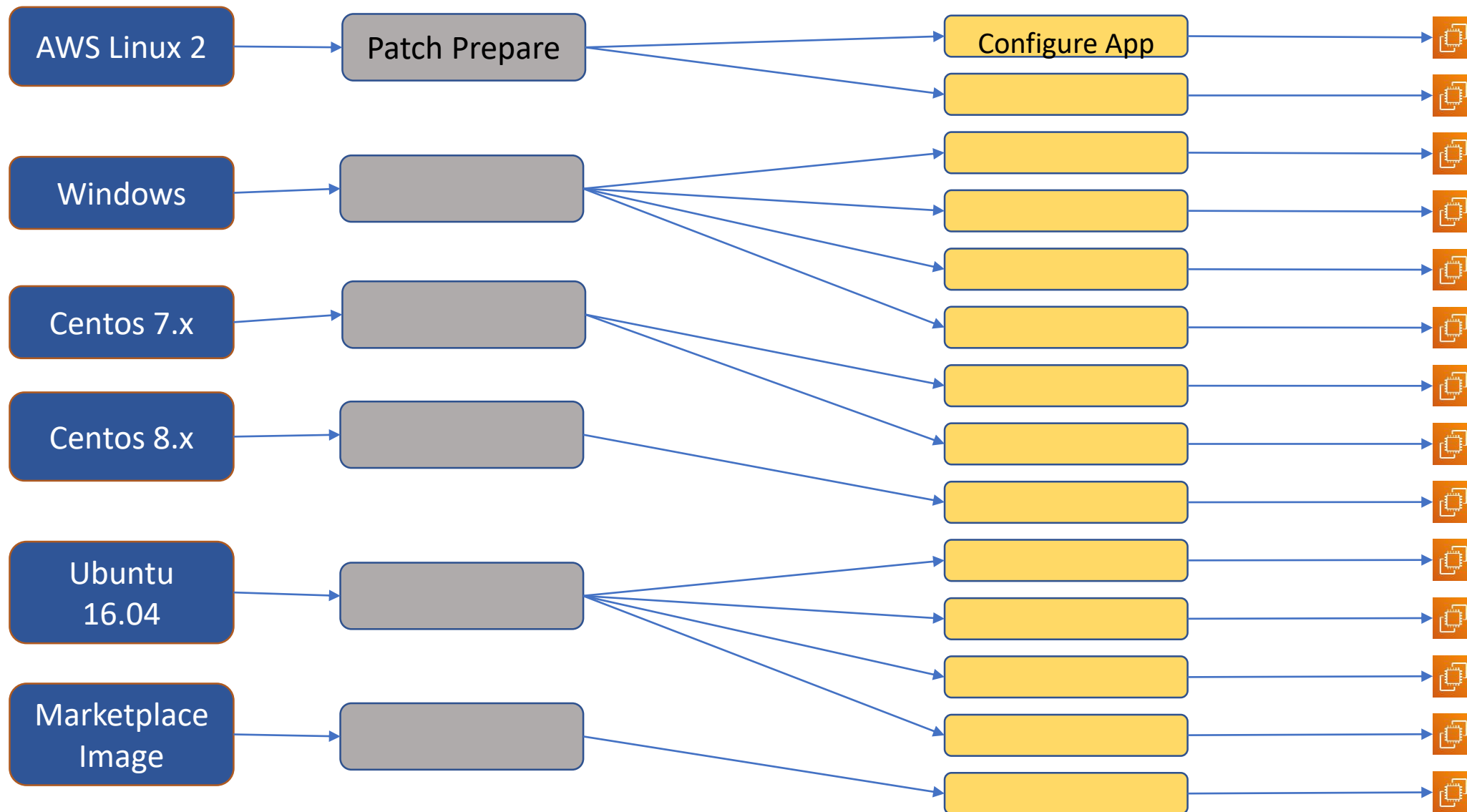
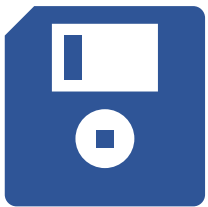
- Never Patch a live system
- Deploy new images with Cloud service provider's Elasticity tools.
- Destroy and Redeploy on schedule
- Do you need to scan?

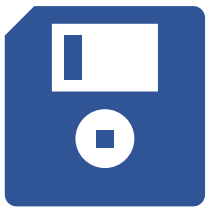




# Making the Pipeline Smoother

- Simplify where possible
- Build in Monitoring and Response
- Offload to the CSP where you can
- Fail Fast and Learn





AWS Linux 2

Patch Prepare

Configure App

Centos 8.x

Marketplace Image



# Making the Pipeline Smoother

- Simplify where possible
- Build in Monitoring and Response
- Offload to the CSP where you can
- Fail Fast and Learn

## Definition document [Info](#)

This defines the actions for Image Builder to perform on your image. It uses the YAML format to list customizations steps on to be executed.

☒ **Define document content**  
Specify content in YAML.

☐ **Use build component example**  
Content can be edited inline.

☐ **Use test example**  
Content can be edited inline.

### Content

```
1 name: HelloWorldTestingDocument
2 description: This is hello world testing document.
3 schemaVersion: 1.0
4
5 phases:
6   - name: test
7     steps:
8       - name: HelloWorldStep
9         action: ExecuteBash
10        inputs:
11          commands:
12            - echo "Hello World! Test."
13
```

Define a  
component  
that builds  
or tests

## Build components [Info](#)

Build components contain software, settings, and configurations to be installed or applied. Build components are included in the recipe and are run during the process of building custom images.

Create build component 


Browse to select build components

*Enter component ARN or browse to select compo*

Browse build components

## Tests [Info](#)

You can select from AWS-provided test or create custom tests to validate your images. Tests are run after a custom image is built to validate functionality, security, performance, etc.

Create test 

Browse to select tests

*Enter component ARN or browse to select compo*

Browse tests

Cancel

Next

Grab  
components  
for building,  
and testing

## Image pipelines

S

n Image Builder defines all aspects of the process to  
: consists of the image recipe, infrastructure configuration,  
t settings.

[View details](#)[Actions ▼](#)[Cr](#)

by name. Press enter to search all results.

Any status ▼

Image name	Date created	Version	Status	Date of last run	ARN
	2020-01-20   17:24:26.929 Z	1.0.0	✔ Enabled	-	arn:aws:imagebuilder:us-east-1:191 pipeline/nginx-test
	2020-01-20   19:47:11.870 Z	1.0.0	✔ Enabled	-	arn:aws:imagebuilder:us-east-1:191 pipeline/nginx2

Each pipeline outputs a new AMI on a schedule

# Making the Pipeline Smoother

- Simplify where possible
- Build in Monitoring and Response
- Offload to the CSP where you can
- Fail Fast and Learn



# Thanks for Attending

Shaun McCullough  
@thecybergooof

