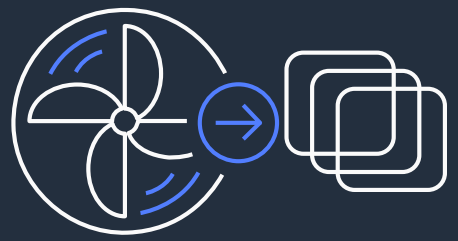
Building and Maintaining the Golden AMI with EC2 Image Builder

Dean Suzuki, Senior Solution Architect, AWS
Sirirat Kongdee, Senior Solution Architect, AWS
4/14/2020

Golden VM images



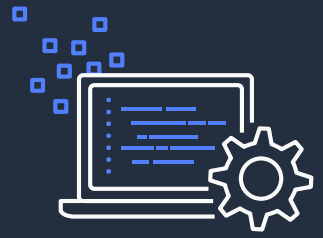
Template server image. Saves time & ensure consistency

Pre-installed & pre-configured with custom software & settings

Hardened to meet IT standards

How do customers build golden images today?

Manually build each golden images



Build and maintain custom automation

Build automation with opensource frameworks

Customers asked for a one-stop shop to build golden images

Customers have asked to be able to…

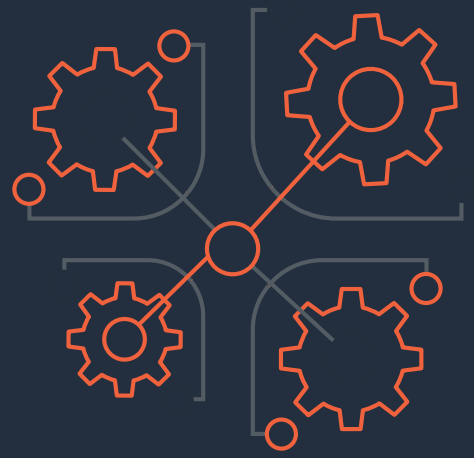
Quickly and easily build automation to create golden images without writing code

Easily **test** images with AWS-provided and custom tests before deploying to production

Secure images with AWS-provided & custom settings to meet internal/industry standards

Distribute and share images easily across accounts & regions with **centralized enforcement**

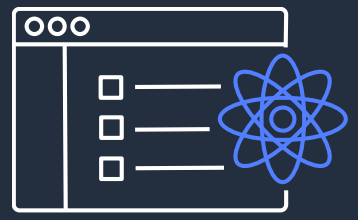
Build images for use on **AWS and on-premises**



EC2 Image Builder

EC2 Image Builder features

Quickly and easily automate the creation, management, and deployment of up-to-date and compliant “golden” VM images



Automated pipelines to keep images secure and up-to-date

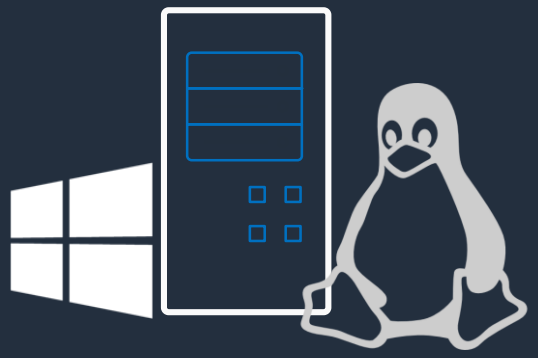
Minimize unnecessary exposure to security vulnerabilities

Validate and deploy high quality images into production

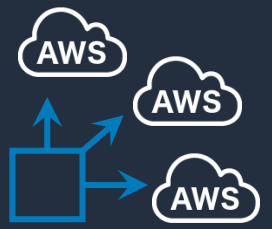
EC2 Image Builder features

Centralized Policy Enforcement

Enforce policies on VM image usage across AWS accounts



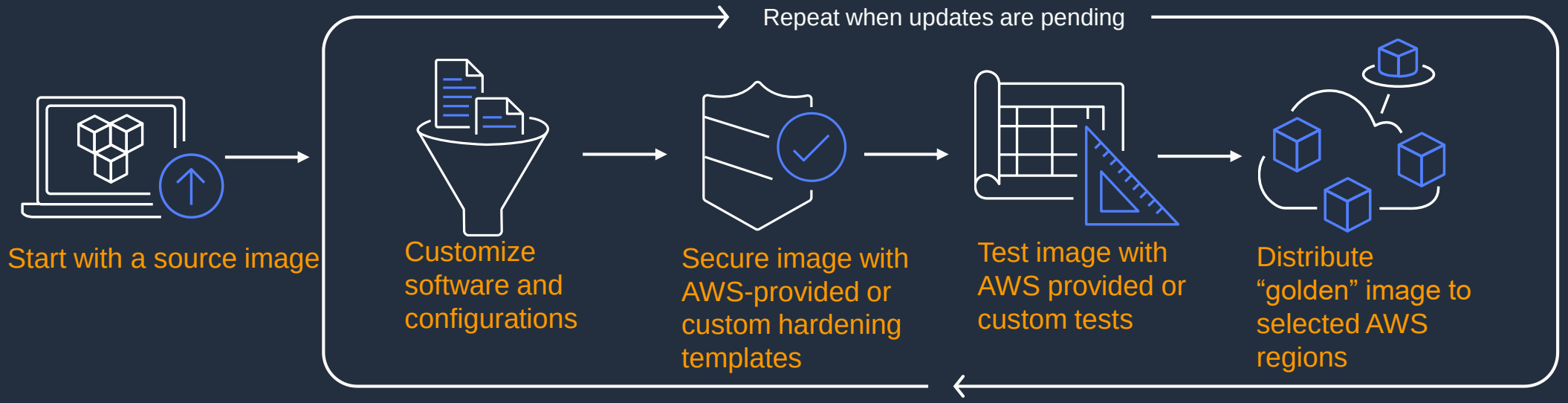
Support for both AWS and on-premises as well as Windows and Linux image creation



Simplified sharing of images across AWS accounts

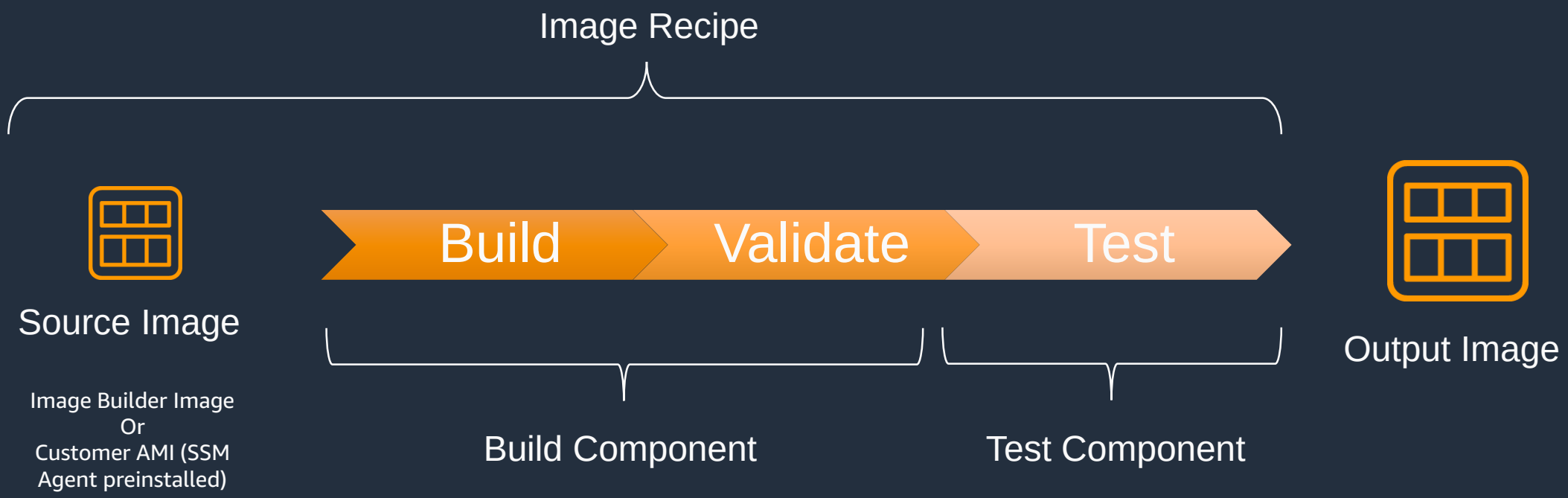
EC2 Image Builder – how it works

All EC2 Image Builder operations run in your AWS account



EC2 Image Builder Image Recipe

Image Recipe defines image configuration. It consists of source image and one or more components applied to the source image. **Component** describes how to build, validate, and test your image.



EC2 Image Builder Image Pipeline

An **image pipeline** is the automation configuration for building secure OS images. The Image Builder image pipeline is associated with an image recipe, infrastructure configuration, distribution configuration, and how the pipeline is triggered.

Image Recipe

Source image, components

Infrastructure Configuration

Instance Type, subnet, SGs, logging, etc

Distribution Configuration

Regions, accounts

Schedule

Manual, schedule

EC2 Image Builder Components

Build components are orchestration documents that define a sequence of steps for downloading, installing, and configuring software packages. **Test components** are orchestration documents that define tests to run on software packages.

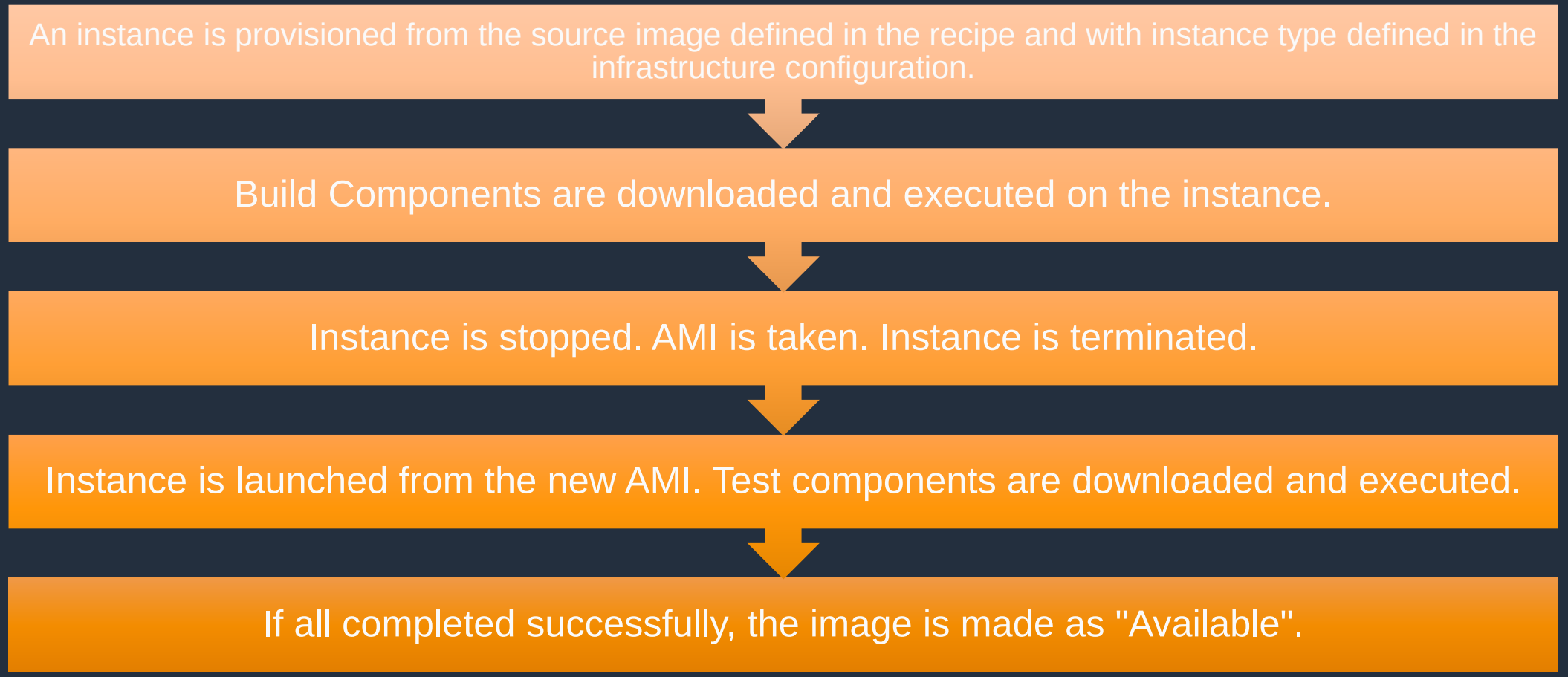
- Phases
- Steps
- Supported Action
- Output Files

https://docs.aws.amazon.com/imagebuilder/latest/userguide/image-builder-application-documents.html

```
phases:
  -
    name: 'build'
    steps:
      -
        name: SampleS3Download
        action: S3Download
        timeoutSeconds: 60
        onFailure: Abort
        maxAttempts: 3
        inputs:
          -
            source: 's3://sample-bucket/sample1.ps1'
            destination: 'C:\Temp\sample1.ps1'
          -
            source: 's3://sample-bucket/sample2.ps1'
            destination: 'C:\Temp\sample2.ps1'
```

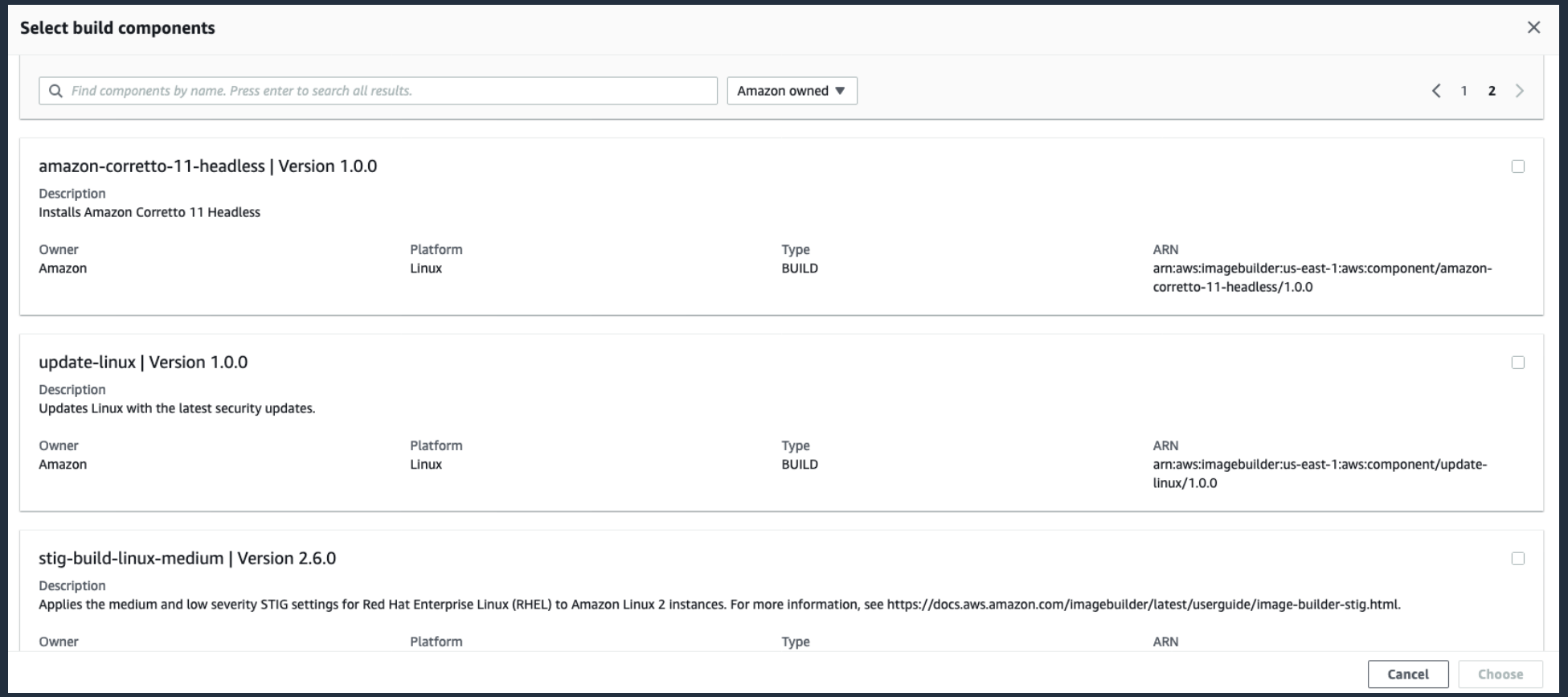
Behind the scene

Component management application orchestrate complex workflows, modify system configurations, and test your systems



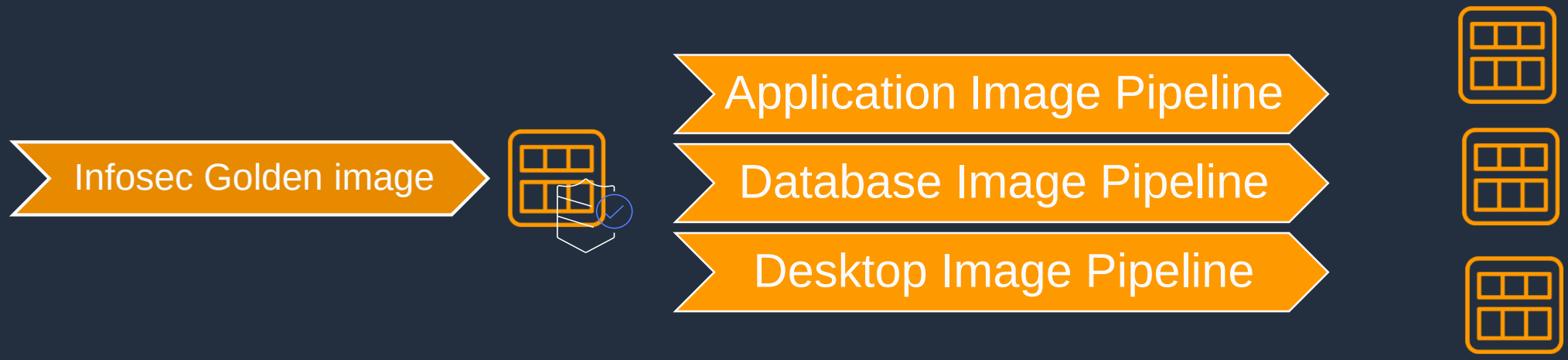
Amazon provided components

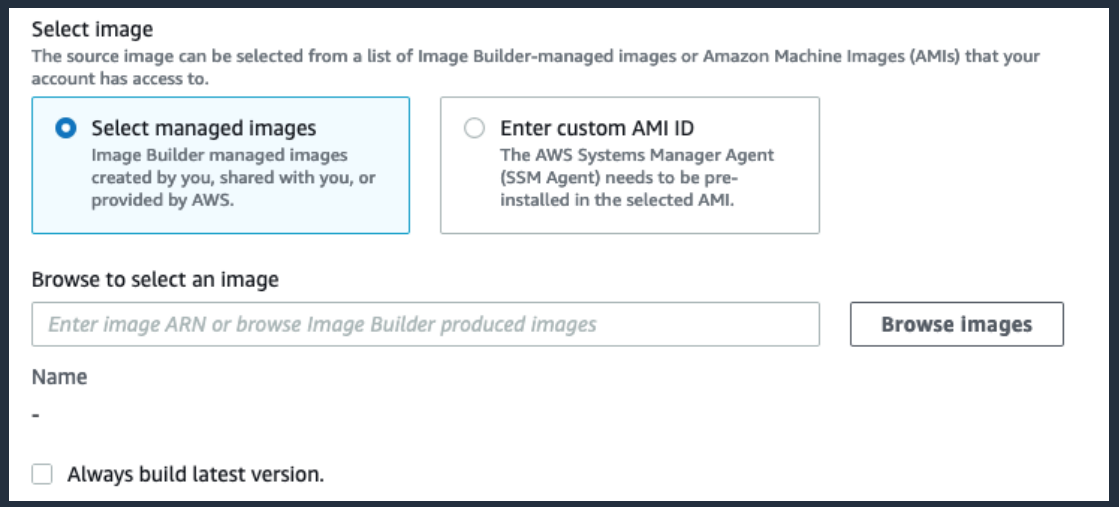
Select from out of the box **components** or build your own.
EC2 Image Builder provides **STIG components** to help you quickly build compliant images for STIG standards.



Cascade Pipeline - Always build latest version

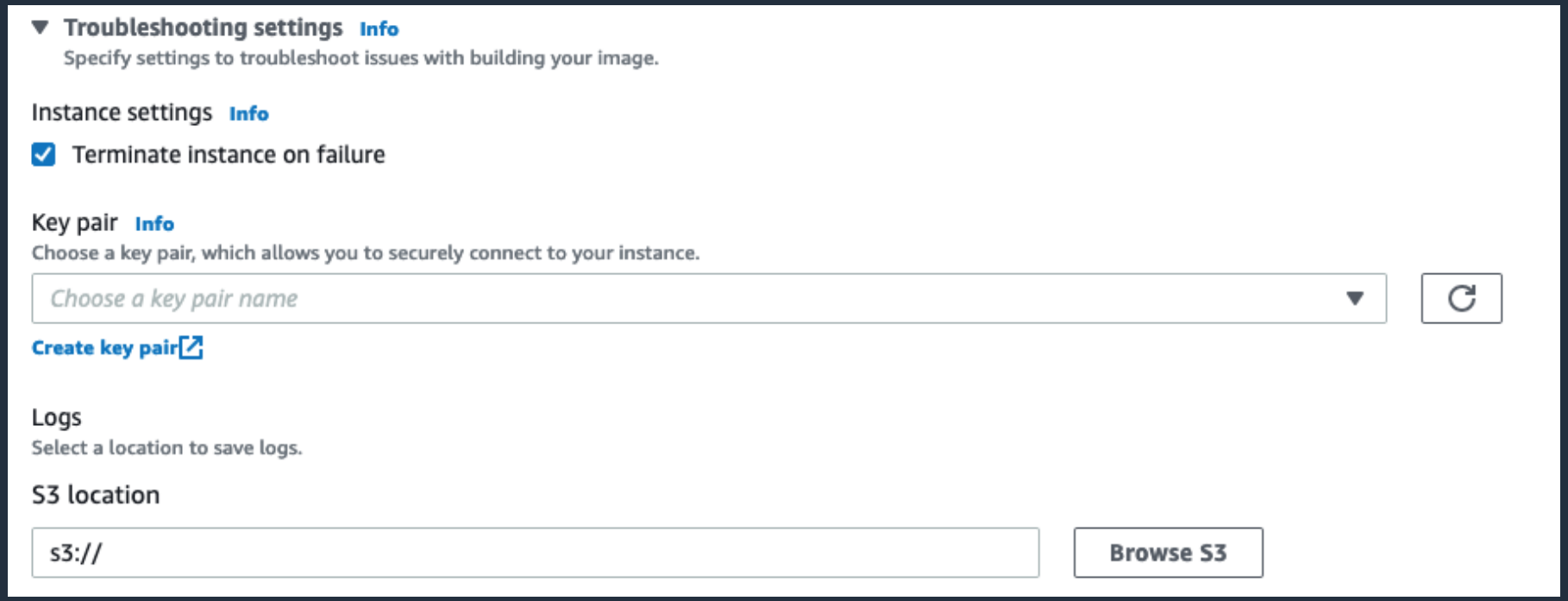
Versioning your image with **Always build latest version** option.
The downstream pipeline use the latest version output image from the upstream pipeline.



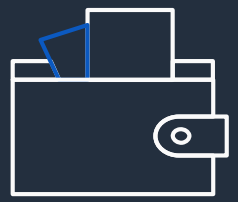


Troubleshooting

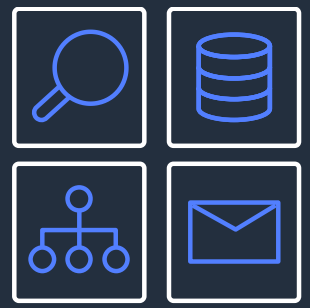
Uncheck “**Terminate Instance on Failure**” option to prevent the termination of the build instance. Use SSH or SSM Session Manager to access the instance to troubleshoot.



Pricing



No cost



All operations run in your AWS account

Pay for the resources used in your account (e.g. EC2 instance usage, S3 usage, SSM Advance, AWS Inspector, etc.)

Summary

Produce automation to build images with ease

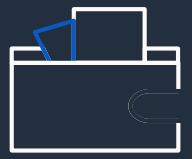
No need to write and maintain code to build automation
GUI wizard to create image building pipelines

Improve security and uptime

Keep images secure and up-to-date
Capture and reuse security settings
Run tests to catch issues before deploying to production

Hybrid use cases

Produce AMIs for use on AWS
Generate on-prem VM images



No cost

Runs in customer account
Pay for resources used in your account