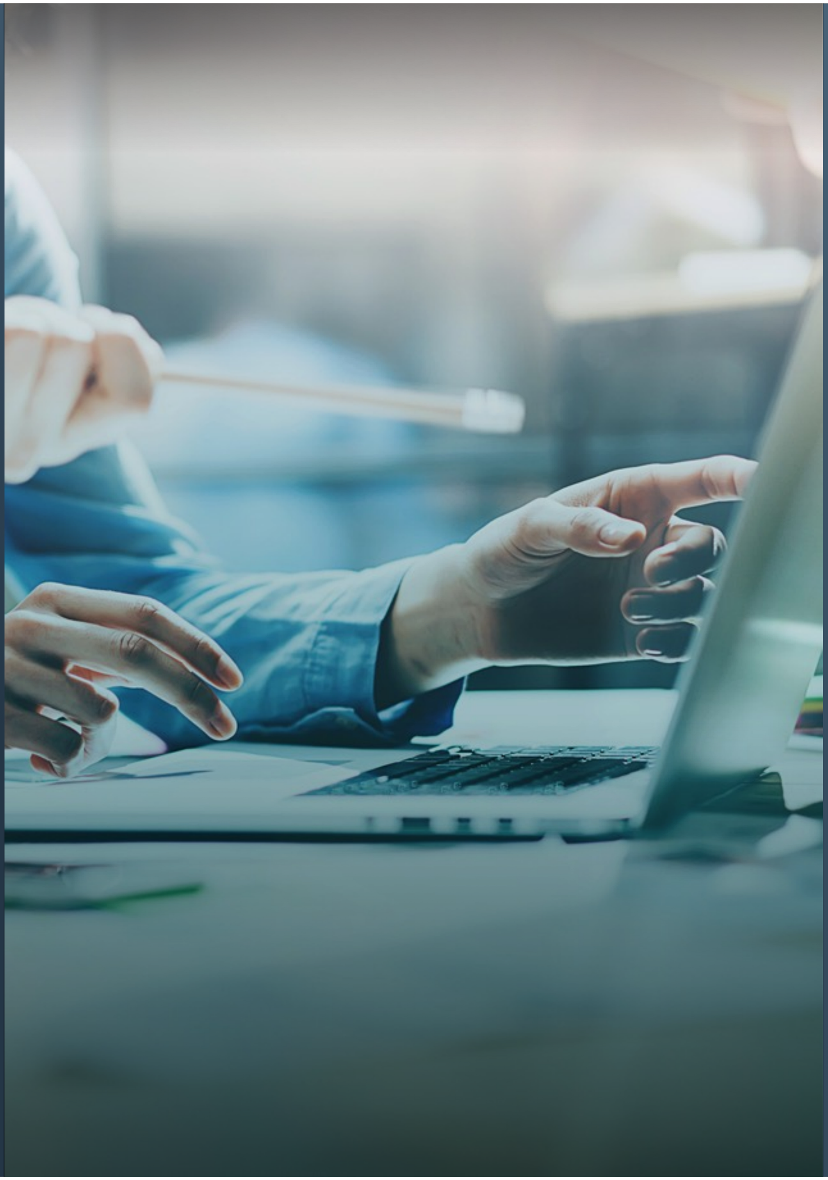
Booz | Allen | Hamilton



ENABLING MULTICLOUD IN THE ENTERPRISE WITH DEVSECOPS

Josh Boyd, Booz Allen Hamilton

Steven Terrana, Booz Allen Hamilton

MAY 2019

DEVSECOPS IS AT THE HEART FOR ENABLING HIGH-PERFORMING IT TEAMS

What is DevSecOps?

Encouraging behaviors and designing processes to optimize coordination of software development and IT operations teams.

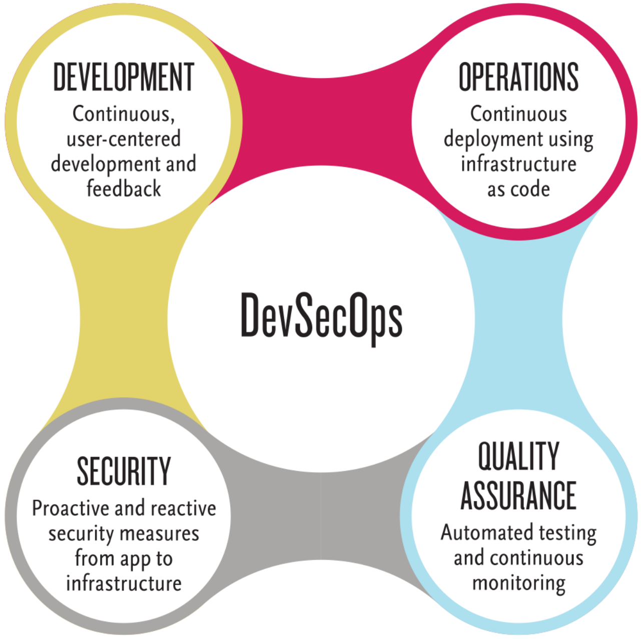
- Emphasis of a **team-culture change** is greater than that of any particular tool or framework
- New approaches **amplify teamwork** to yield a **high-rate** of delivery of **small-scoped** features
- Practicing new activities or performing them in new ways to **eliminate waste**

Why are organizations embracing DevSecOps?

Organizations embrace DevSecOps to continuously deliver high-quality and reliable software to their users.

- Culture and teamwork evolves with the intent to **build better quality software faster**
- High-performing teams are needed to maintain balance in the opposing forces of ***throughput*** and ***stability,*** while both are amplified
- DevSecOps realizes the **Agile benefits of reducing risk, increasing velocity, and improving quality**, but scaled beyond the development lifecycle to the product lifecycle. It **increases resiliency**, **reduces unplanned downtime**, and provides production metrics to close the feedback loop to **adapt to users** and **fix software hastily**.

TRUSTED SOFTWARE SUPPLY CHAIN
BOOZ ALLEN DEVSECOPS PUTS THE SECURITY IN DEVOPS


DEVELOPMENT
Continuous, user-centered development and feedback
OPERATIONS
Continuous deployment using infrastructure as code
DevSecOps
SECURITY
Proactive and reactive security measures from app to infrastructure
QUALITY ASSURANCE
Automated testing and continuous monitoring

CONTINUOUS SECURITY & COMPLIANCE IS PERVASIVE IN OUR DEVOPS APPROACH. IT CROSS-CUTS EVERY PRACTICE AREA

Security and compliance are indicative of the same software delivery sins that spawned the DevOps movement. Work piles up because it is tedious, foreign, or difficult. Security pros are alienated and left to burn down the pile in isolation, as an afterthought. True concerns then become hugely disruptive, which breeds further discontent within the team.

AS WITH QUALITY ASSURANCE, SECURITY ASSURANCE AND COMPLIANCE CAN BE INTEGRATED INTO YOUR SOFTWARE DEVELOPMENT LIFECYCLE

- **Shift-left** many security and compliance activities as a **shared responsibility** of the whole team
- **Educate and automate** security vigilance to establish **early detection, confidence, and trust** required for Continuous Delivery
- Perform vulnerability and compliance **inspection** of dependencies, code, container images, and running applications

DEPENDENCIES

Prevent introduction of vulnerabilities from the outside. Scan libraries in dependency repos, source code repos, and on disk for known vulnerabilities.

STATIC CODE ANALYSIS

Analyze the code written by developers for inadvertent technical and logical flaws that make it vulnerable.

DYNAMIC APPLICATION SECURITY TESTING

Perform automated penetration testing to see how your application will withstand common attacks at runtime.

IMAGE SCANNING

Unpack and scan dependencies and configuration of the image to be used at runtime for vulnerabilities, out-of-date patching, and to ensure a trusted pedigree.

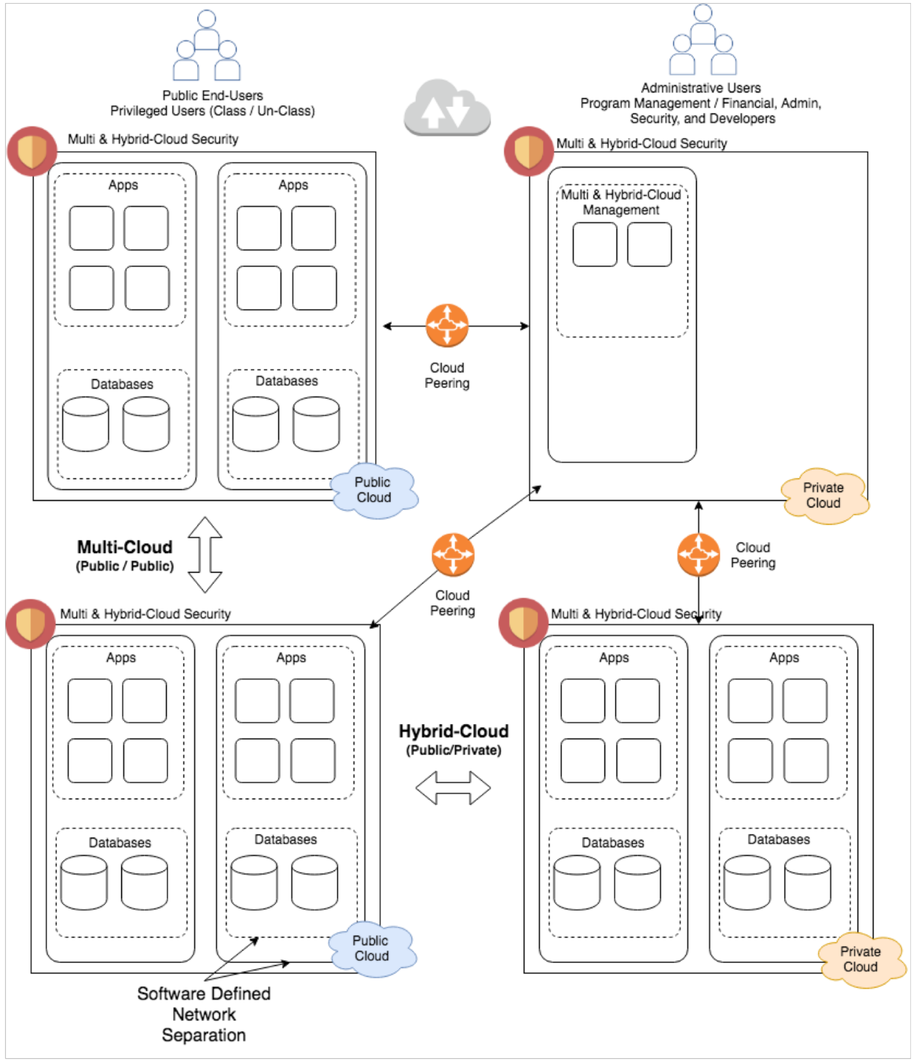
CONTINUOUS COMPLIANCE

Routinely scan the configuration of hosts or containers in their packaged image state or at runtime for compliance with security policy groups (NIST, CIS, FISMA, STIG, etc.), for required patches, or for configuration drift.

ACCESSIBILITY ASSURANCE

Crawl web pages for compliance with section 508 standards to give developers early warning and opportunity to improve the site while accelerating manual 508 testing.

WHAT DOES MULTI-CLOUD MEAN TO US



Public End-Users
Privileged Users (Class / Un-Class)
Administrative Users
Program Management / Financial, Admin, Security, and Developers
Multi & Hybrid-Cloud Security
Apps
Databases
Multi & Hybrid-Cloud Management
Cloud Peering
Public Cloud
Private Cloud
Multi-Cloud (Public / Public)
Hybrid-Cloud (Public/Private)
Software Defined Network Separation

Booz Allen Capabilities:

- **Solutions Delivery Platform** – Booz Allen's open source enterprise DevSecOps capability at scale
- **Virtual Cloud Defense (VCD)** – Booz Allen's capability for a common security framework across cloud service providers
- **Multi-Cloud** – Booz Allen's capability for achieving various levels of maturity

Featured Concepts:

- Multi-Region Databases
- SDN Supported Network Partitioning
- Accelerated Application Accreditation & ATO

Multi-Cloud Capabilities:

Centralized Management / Orchestration

- Ability to manage provisioning, enforce policy and chargeback across multiple cloud service providers.
- Scaling within cloud based on performance demands and resource limits

Workload Optimization

- Position applications within CSP providing necessary services

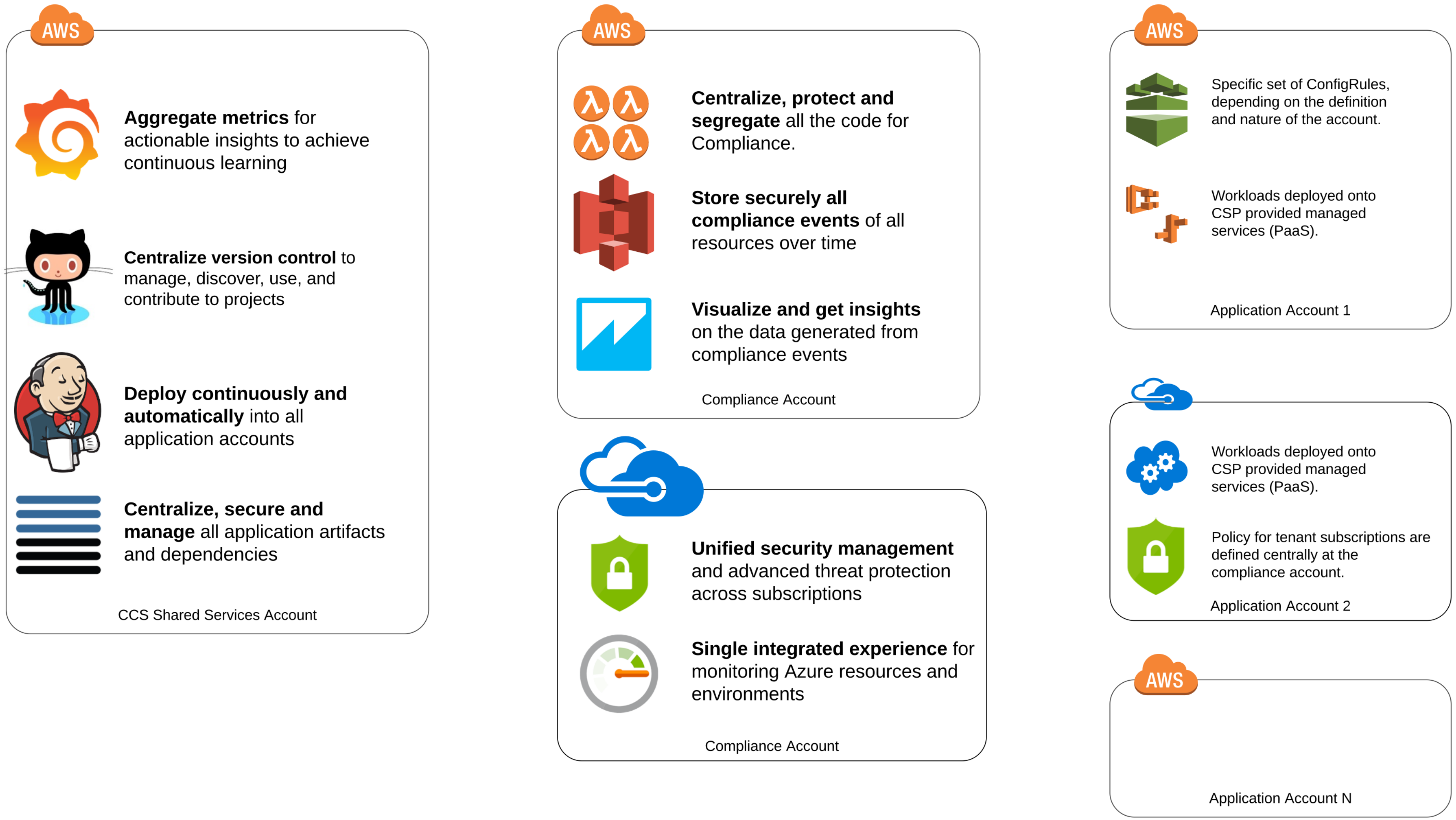
Disaster Recovery / COOP

- Application Replication and Data Synchronization across cloud services providers, Traffic Routing / Failover in the event of outage.

High Availability (Active / Active)

- Ability to simultaneously operate common application payloads across multiple cloud services providers
- Multi-Cloud Data Persistence, Intelligent Traffic Load Balancing
- Scaling across cloud service providers/CSP regions

MULTI-CLOUD/MULTI-TENANT LOGICAL ARCHITECTURE



Aggregate metrics for actionable insights to achieve continuous learning

Centralize version control to manage, discover, use, and contribute to projects

Deploy continuously and automatically into all application accounts

Centralize, secure and manage all application artifacts and dependencies

CCS Shared Services Account

Centralize, protect and segregate all the code for Compliance.

Store securely all compliance events of all resources over time

Visualize and get insights on the data generated from compliance events

Compliance Account

Unified security management and advanced threat protection across subscriptions

Single integrated experience for monitoring Azure resources and environments

Compliance Account

Specific set of ConfigRules, depending on the definition and nature of the account.

Workloads deployed onto CSP provided managed services (PaaS).

Application Account 1

Workloads deployed onto CSP provided managed services (PaaS).

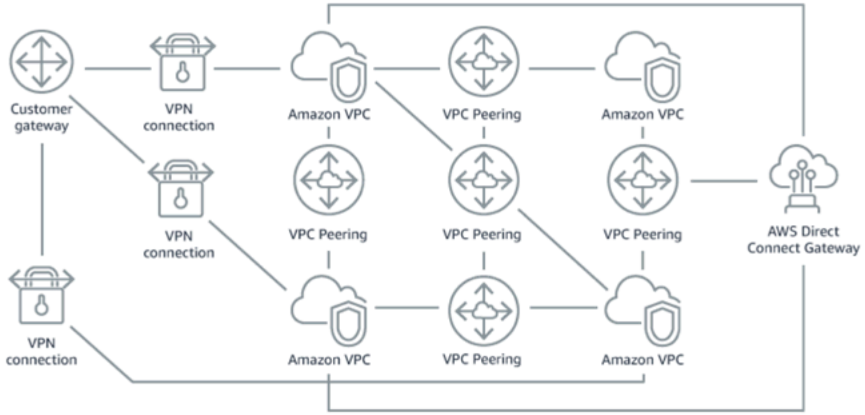
Policy for tenant subscriptions are defined centrally at the compliance account.

Application Account 2

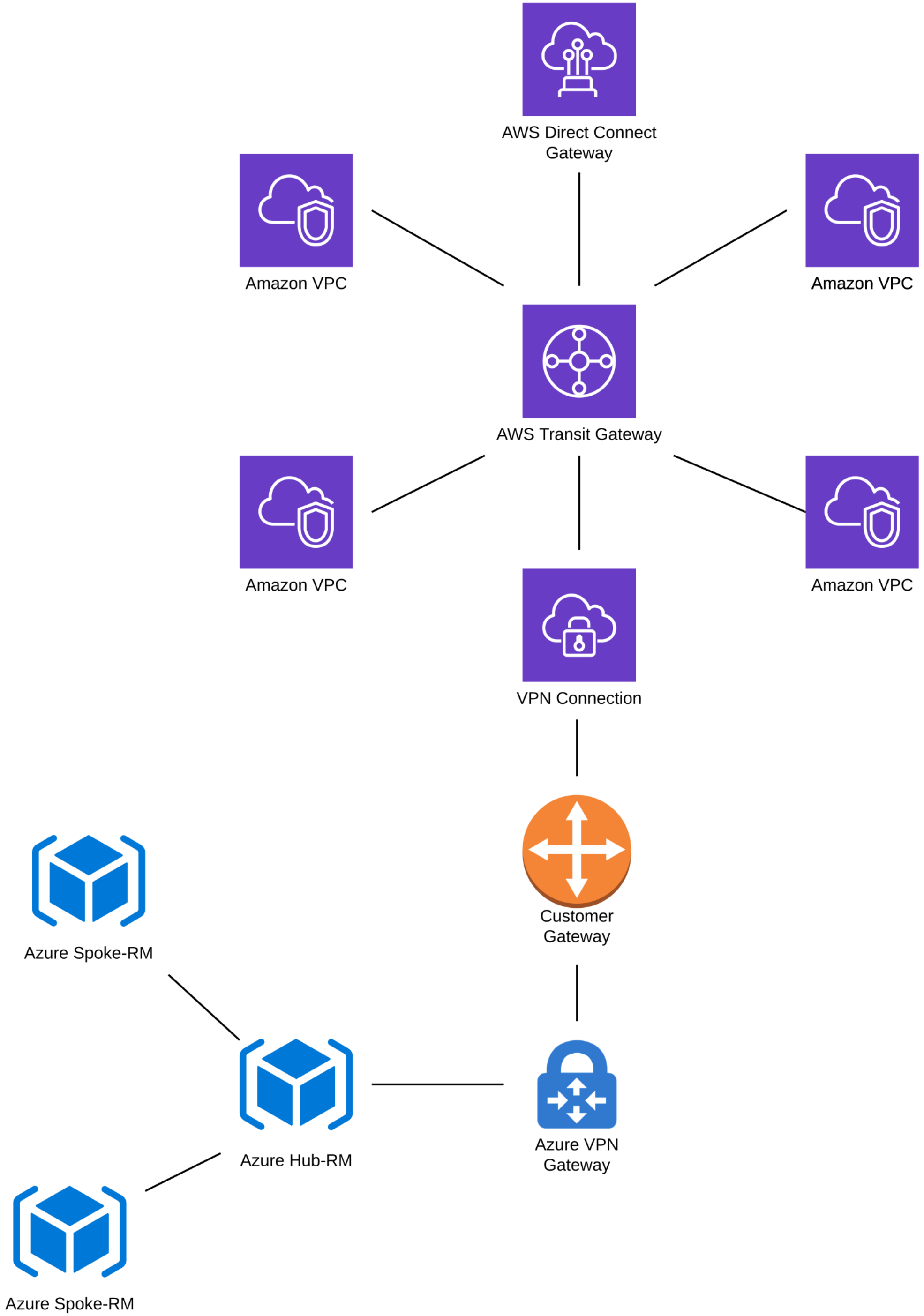
Application Account N

MULTI CLOUD NETWORK TOPOLOGY

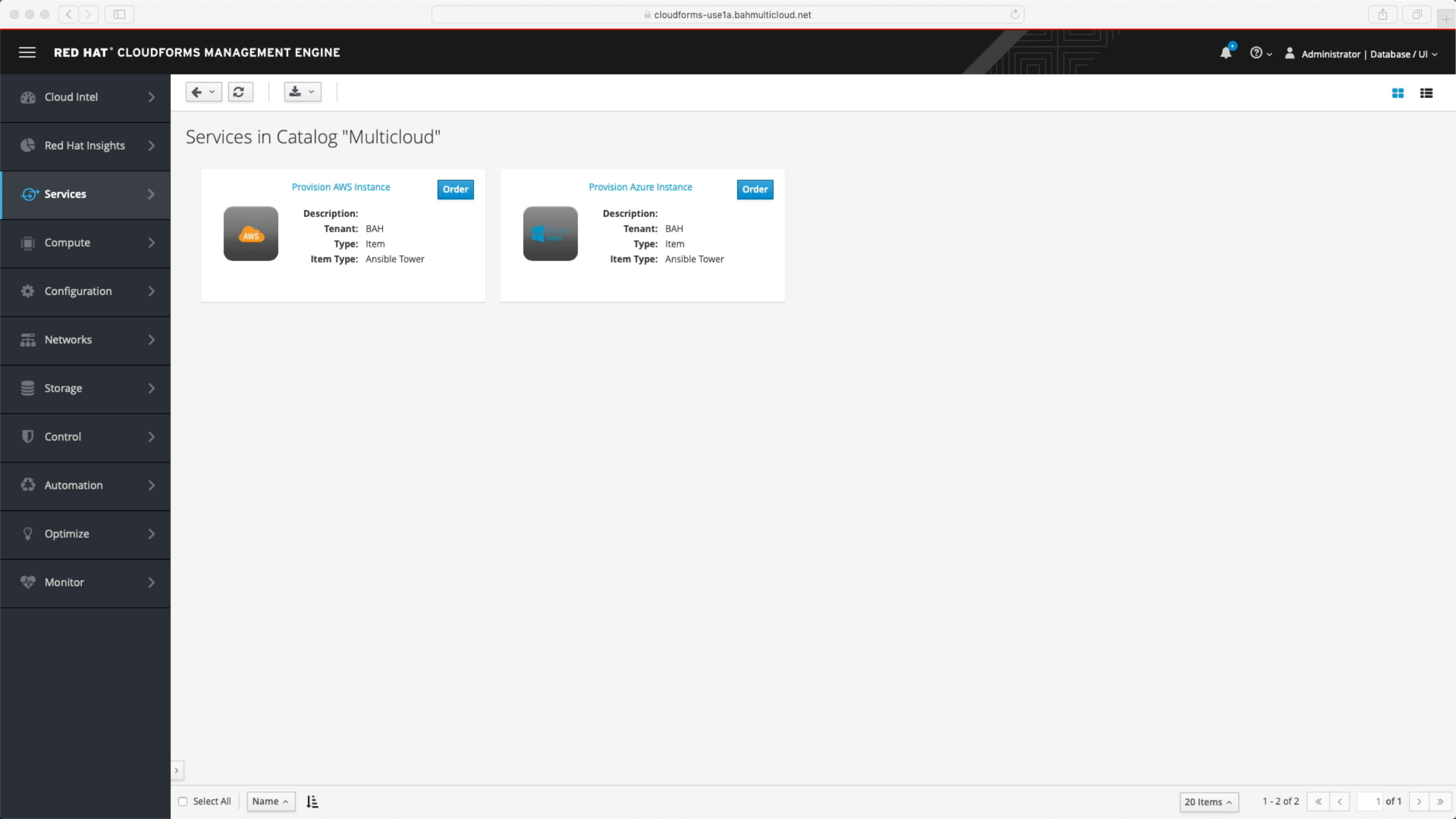
- This used to be a lot harder before November:



- And then you had to configure high availability VPNs in your hubs, now you can do this purely with AWS and Azure provided services.
- AWS Transit Gateway was created to connect VPCs and on-prem networks with a single gateway, but it works great to connect to other CSPs too!



MULTI CLOUD PROVISIONING DEMO



Services in Catalog "Multicloud"

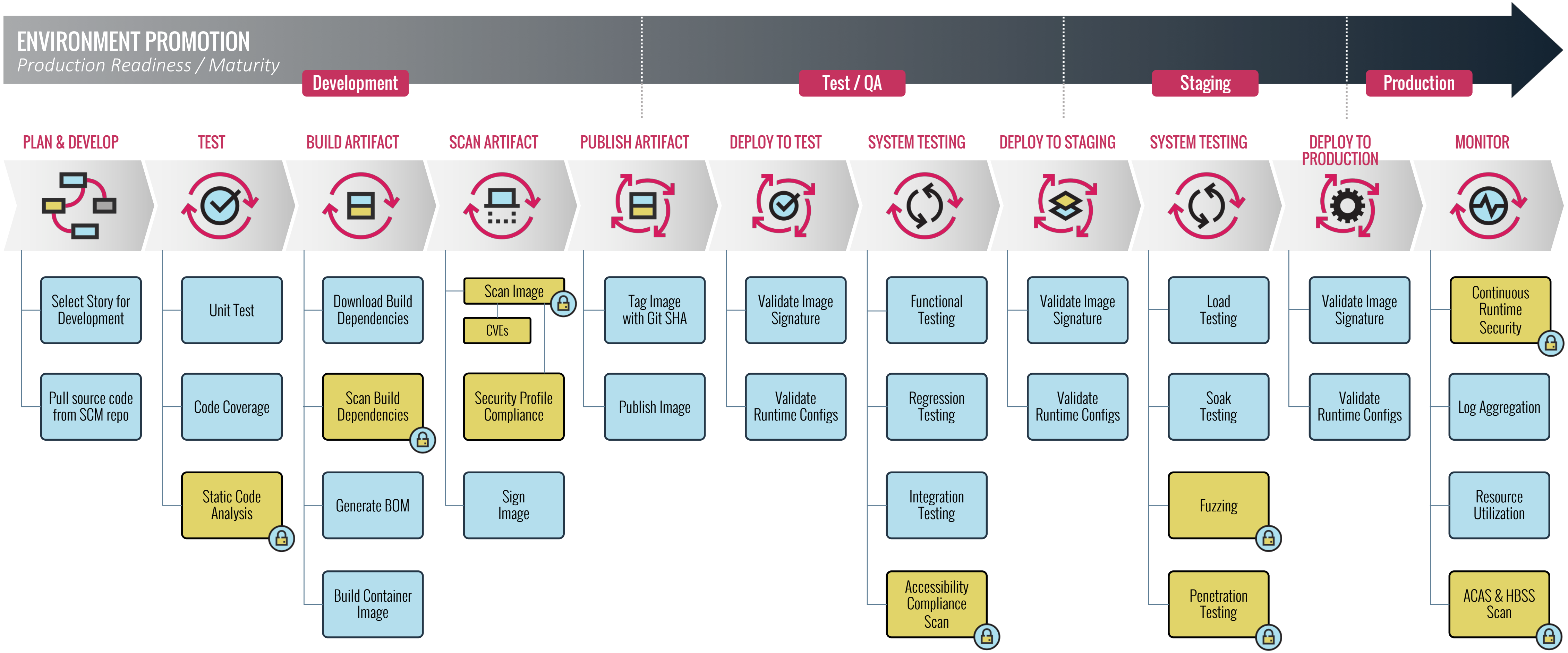
Provision AWS Instance

Description:
Tenant: BAH
Type: Item
Item Type: Ansible Tower

Provision Azure Instance

Description:
Tenant: BAH
Type: Item
Item Type: Ansible Tower

THE DEVSECOPS PIPELINE IS A TRUSTED SOFTWARE SUPPLY CHAIN



ENVIRONMENT PROMOTION
Production Readiness / Maturity

Development | Test / QA | Staging | Production

PLAN & DEVELOP
- Select Story for Development
- Pull source code from SCM repo

TEST
- Unit Test
- Code Coverage
- Static Code Analysis

BUILD ARTIFACT
- Download Build Dependencies
- Scan Build Dependencies
- Generate BOM
- Build Container Image

SCAN ARTIFACT
- Scan Image
- CVEs
- Security Profile Compliance
- Sign Image

PUBLISH ARTIFACT
- Tag Image with Git SHA
- Publish Image

DEPLOY TO TEST
- Validate Image Signature
- Validate Runtime Configs

SYSTEM TESTING
- Functional Testing
- Regression Testing
- Integration Testing
- Accessibility Compliance Scan

DEPLOY TO STAGING
- Validate Image Signature
- Validate Runtime Configs

SYSTEM TESTING
- Load Testing
- Soak Testing
- Fuzzing
- Penetration Testing

DEPLOY TO PRODUCTION
- Validate Image Signature
- Validate Runtime Configs

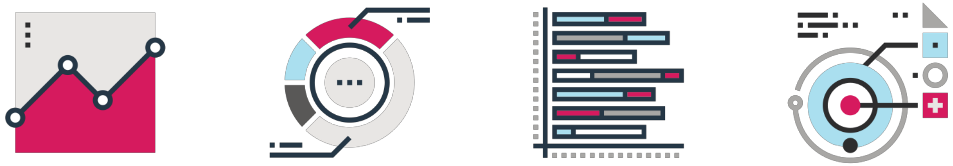
MONITOR
- Continuous Runtime Security
- Log Aggregation
- Resource Utilization
- ACAS & HBSS Scan

THE SOLUTIONS DELIVERY PLATFORM (SDP) IS THE PURPOSE-BUILT SOLUTION THAT ENABLES OUR PHILOSOPHY AND PUTS PROCESSES AND PRACTICES INTO ACTION

REFERENCE MODEL FOR THE SOLUTIONS DELIVERY PLATFORM

DevSecOps Dashboard

Aggregate metrics for actionable insights to achieve continuous learning



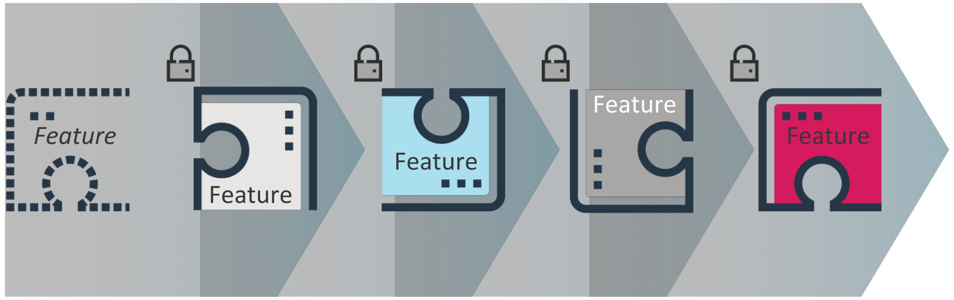
Secure Pipeline Framework

Jenkins Templating Engine

Standardize your organization's continuous delivery

Pipeline Libraries

Automated provenance with a trusted supply chain to production



Continuous & Automated Security and Compliance

Container Orchestration Platform

Host the tooling in an elastic, portable environment

Amazon EKS

Azure Container Service

kubernetes

OPENSHIFT

BENEFITS

- End-to-end **traceability** of delivery
- Real-time **status** at a glance
- **Single view** of multiple apps/ components and teams
- High-fidelity **drill-down** to activity-specific metrics

- **Automate** delivery, and assurance of security & quality
- Enable **secure, on-demand** flow of new features
- Continuous, quantitative, and actionable **feedback**
- **Shifting-left security** and streamlining activities **mitigates risk** by avoiding big and long releases

- **Productivity** increase with self-service, homogenous IT
- **Scalable, resilient** backbone
- Environment **parity**
- Improved resource **utilization**

SOLIDIFYING THE BASE: RED HAT UNIVERSAL BASE IMAGE (UBI)

UBI Attributes

- Subset of RHEL content
- Redistributable
- Base and RHSCL images
- Enabled yum repos
- Microdnf
- Supported
- Cataloged
- Updated
- Tracked
- Reusable

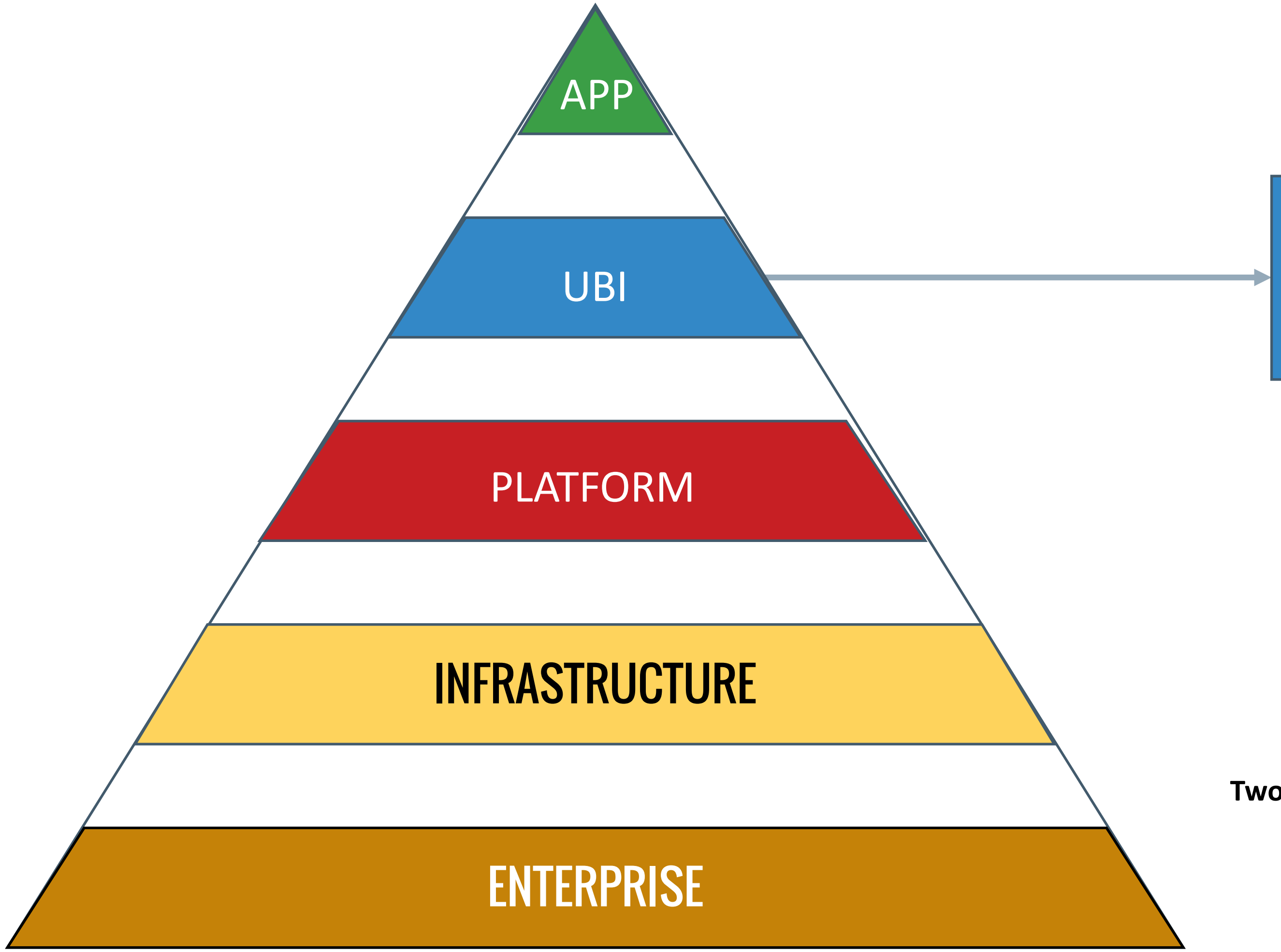
Two Talks on UBI This Week

- Choosing the right container base image for your application, Today, 1:30-2:15pm
- Building production-ready containers, Wednesday, 3:30-4:15pm

DevSecOps Platform Images

- ✓ Jenkins
- ✓ SonarQube
- ✓ OWASP ZAP
- ✓ Nexus
- ✓ Helm
- ✓ The A11y Machine
- ✓ Twistlock
- ✓ OpenSCAP

SOLIDIFYING THE BASE: RED HAT UNIVERSAL BASE IMAGE (UBI)



Red Hat's Universal Base Image adds a new layer of control inheritance when building security hardened PaaS Solutions

UBI Attributes

- Subset of RHEL content
- Redistributable
- Base and RHSCL images
- Enabled yum repos
- Microdnf
- Supported
- Cataloged
- Updated
- Tracked
- Reusable

Two Talks on UBI This Week

Choosing the right container base image for your application, Today, 1:30-2:15pm
Building production-ready containers, Wednesday, 3:30-4:15pm

THE SDP BUILDS TRUSTED SOFTWARE SUPPLY CHAINS

The Solutions Delivery Platform allows you to build *tool-agnostic*, **templated** workflows to integrate security into every step of your software delivery lifecycle

A containerized DevSecOps Platform, SDP leverages Red Hat's **Universal Base Image –** meaning out-of-the-box security compliance within your organization

Instead of building a pipeline *per application* – SDP lets you define the organizational quality and security gates that must be passed while affording teams the **flexibility** to choose the right tools for the job

Leverage the same DevSecOps pipeline regardless of which cloud environment your application is targeting

BOOZ ALLEN'S SOLUTIONS DELIVERY PLATFORM

APPLY ORGANIZATIONAL GOVERNANCE

Standardize software delivery processes

OPTIMIZE CODE REUSE

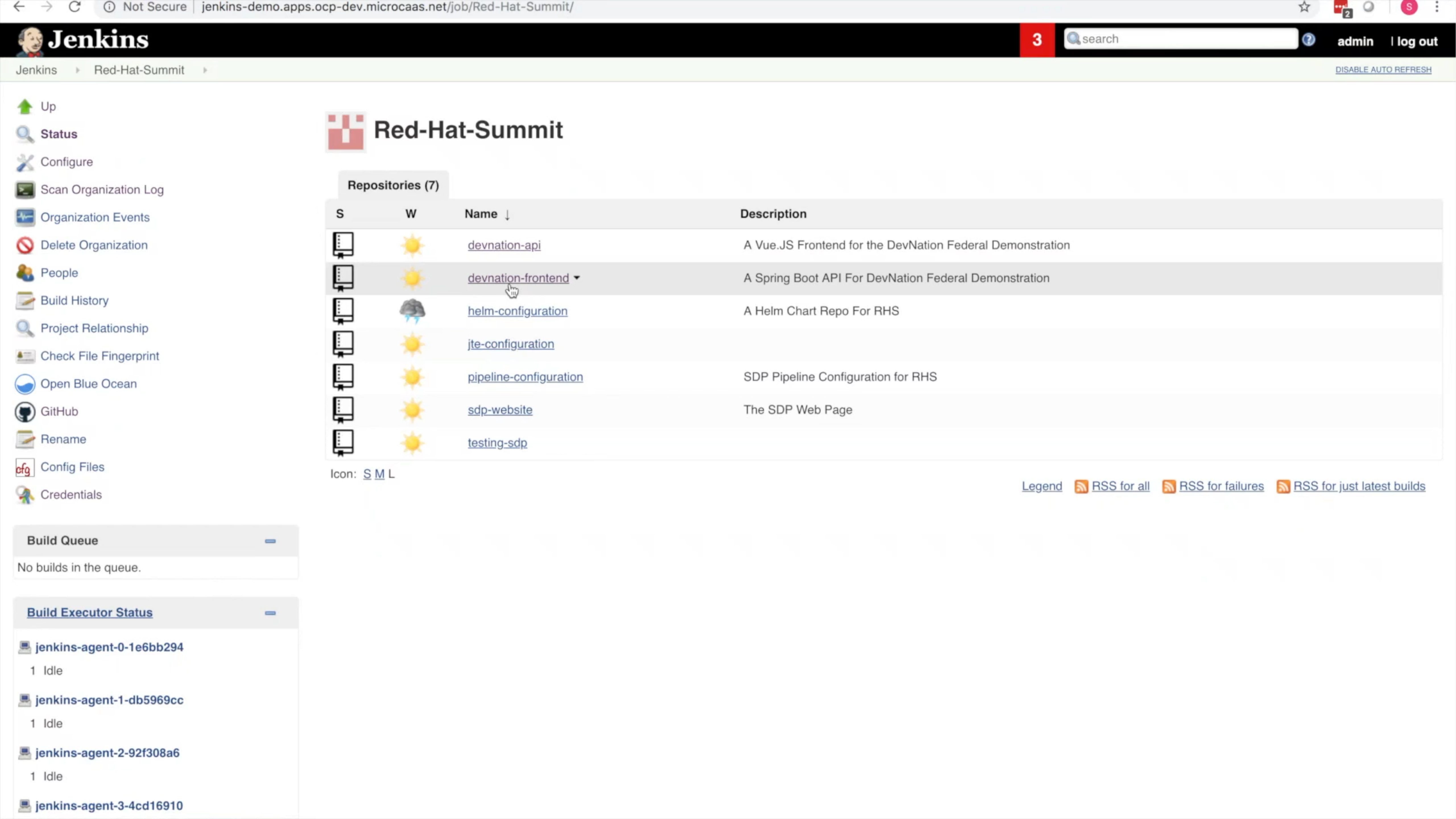
Crowd source quality through common open source libraries

SIMPLIFY PIPELINE MAINTAINABILITY

Manage templates over application specific pipelines

DEMO

LET’S SEE IT IN ACTION



Not Secure jenkins-demo.apps.ocp-dev.microcaas.net/job/Red-Hat-Summit/

Jenkins

3 search admin | log out

Jenkins › Red-Hat-Summit ›

DISABLE AUTO REFRESH

- Up
- Status
- Configure
- Scan Organization Log
- Organization Events
- Delete Organization
- People
- Build History
- Project Relationship
- Check File Fingerprint
- Open Blue Ocean
- GitHub
- Rename
- Config Files
- Credentials

Red-Hat-Summit

Repositories (7)

S	W	Name ↓	Description
📖	☀	devnation-api	A Vue.JS Frontend for the DevNation Federal Demonstration
📖	☀	devnation-frontend	A Spring Boot API For DevNation Federal Demonstration
📖	⛈	helm-configuration	A Helm Chart Repo For RHS
📖	☀	jte-configuration	
📖	☀	pipeline-configuration	SDP Pipeline Configuration for RHS
📖	☀	sdp-website	The SDP Web Page
📖	☀	testing-sdp	

Icon: S M L

Legend RSS for all RSS for failures RSS for just latest builds

Build Queue

No builds in the queue.

Build Executor Status

jenkins-agent-0-1e6bb294

1 Idle

jenkins-agent-1-db5969cc

1 Idle

jenkins-agent-2-92f308a6

1 Idle

jenkins-agent-3-4cd16910

OPEN SOURCE COMMUNITY

The Solutions Delivery Platform components are open sourced under the Booz Allen Public License.

Jenkins Templating Engine: https://github.com/boozallen/jenkins-templating-engine.git
*Licensed under Apache 2.0 and released to the Jenkins Update Center
https://gitter.im/jenkinsci/templating-engine-plugin

SDP Pipeline Libraries: https://github.com/boozallen/sdp-libraries.git
*Licensed under the Booz Allen Public License: http://boozallen.github.io/licenses/bapl

Documentation: https://boozallen.github.io/sdp-docs/

Jenkins Pipeline Authoring SIG: https://jenkins.io/sigs/pipeline-authoring/

Jenkins World 2018: https://www.youtube.com/watch?v=BM9Vmsh2iMI

LEARN MORE ABOUT US

https://boozallen.com/apply

Josh Boyd
@joshboyd
boyd_joshua@bah.com

Steven Terrana
@steven_terrana
terrana_steven@bah.com

https://boozallen.github.io/sdp-docs/

devsecops@bah.com

https://gitter.im/jenkinsci/templating-engine-plugin