



CloudBees®

Audit Ready Pipelines

*You Don't Have a Secure Supply Chain Issue,
You have a Software Delivery Issue*

Anders Wallgren

Definition: The Pipeline Run *IS* the Audit Trail

- Connected toolchain using only immutable objects
- Fully automated with built-in approval gates
- Outputs of those commands are captured in common data repository
- Governed by centralized RBAC on all artifacts
- End-to-end visibility
- One-click, automated audit reports with trusted data



The Current State of Audit



Uh-oh --- “*THAT*” Email!

^ Unread



Genevieve Cross

Annual Accreditation Review - Tim, The AO will be conducting its annual accreditation/ATO review of all sof...



The Log Slog

- Manually retracing steps across tools
- Interrupt developers to recreate builds where data is missing

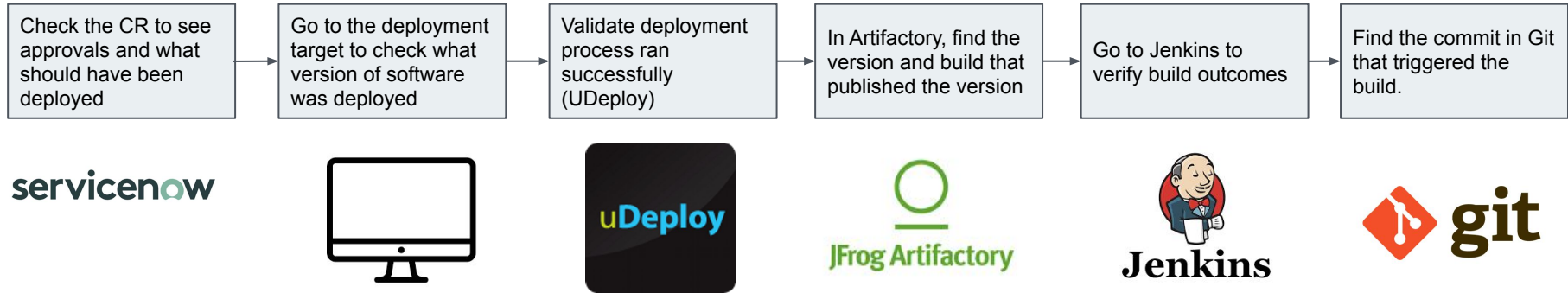
But:

- More time, More Errors, More Costs
- Developers not doing their own jobs
- Risk of failure from incomplete data



Example Audit Process

Manually retrace steps, switching between tools and losing traceability of any manual checks or processes



The Audit Challenge

- Disconnected tools and manual processes
 - Scattered (or no) data
 - Traceability
 - Proof
 - Trust



Audit Risks

- More Time, More Errors, More Costs
- Distracted and disgruntled developers
- Failing to achieve or retain ATO because of incomplete or suspect data



Audit-Ready Pipeline in Real Life



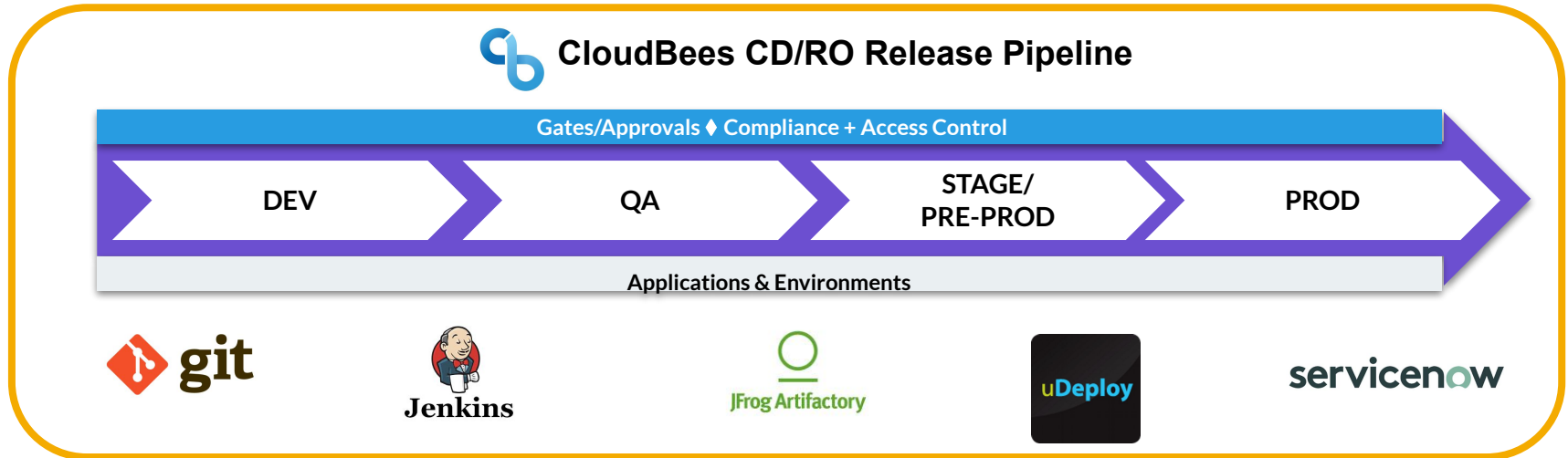
Review: The Audit-Ready Pipeline

- Connected toolchain using only immutable objects
- Fully automated with built-in approval gates
- Outputs of those commands are captured in common data repository
- Governed by centralized RBAC on all artifacts
- End-to-end visibility
- One-click, automated audit reports with trusted data



Example Audit Process

The Release pipeline becomes the audit trail. Orchestrating and governing the release process, connecting DevOps tools, and collecting audit data throughout the process



Example - Evidence links collecting all pipeline data

☰

☆

Release Editor

DSL Editor

Pipeline Runs

Command Center

Planned vs Actual

Release Portfolio

Path to Production

Previous Run:

Delete

Select

All

Forrester / Releases / Motorcycle Release 2.0 / Runs

Run InstanceStageStart TimeDurationRestartedManualActionsExpand

1

Motorcycle Release 2.0_Motorcycle Release Pipeline_294_20200323195254

Mar 23, 2020 - 12:5251 Days, 23:48:102x100%

DEV

1x 100%

Stage / DEV

SummaryErrors

Acme Motorcycle - Deploy on Moto Dev

JIRA Queried Issues Report [Download Report](#)

Changelog report: container-poc - master [Download Report](#)

Jenkins Build #713 [Jenkins Build #713](#)

RunAndMonitorBuild Build motorbike-2 #713

Jenkins motorbike-2:713 report [Jenkins motorbike-2:713 report](#)

Jenkins Report:

Job motorbike-2 #713

1. Pull Jira Tickets

1st

100%

EC-Jira GetIssues

2. Pull

1st

100%

ECSCM-Git CheckoutCode

3. Jenkins Build

1st

100%

EC-Jenkins RunAndWait

4. Deploy and Scan

1st

100%

a. Deploy to Dev

1st

100%

Deployer

b. Run SonarQube

1st

100%

EC-SonarQube Run Sonar Scanner

5. Unit Tests

1st

100%

Unit test

6. EC-ServiceNow CreateChangeRequest

100%

PROD

1x 100%

Stage / PROD

SummaryErrors

Check for Outage

1st

100%

EC-Mooqsoft Get System Summary

2. BLUE-GREEN Deploy to Prod

1st

100%

Deployer

3. Run Smoke Tests

1st

100%

Smoke Test

4. Update Prod Status

1st

100%

Command

5. Verify Switch Blue-Green

1st

100%

Manual

Approved

6. Switch LoadBalancer between BLUE-GREEN

1st

100%

Update Nginx

Audit Reports

1x 100%

Stage / Audit Reports

SummaryErrors

Approval Report

1st

100%

EC-AuditReports generate ApprovalAuditReport

2. Evidence Report

1st

100%

EC-AuditReports generate EvidenceLinksAuditReport

3. Duration Report

1st

100%

EC-AuditReports generate TaskDurationAuditReport



Example - Jenkins Build Data Report

The screenshot displays the Jenkins web interface for a successful CI build. The main view is titled "View successful CI Build: test build pipeline#2 (#2)" and is associated with the run "Motorcycle Release 3.0_Motorcycle Release Pipeline_340_202005140...". The build status is "Summary" (highlighted in green), with tabs for "Code Commit", "Test Results", and "Build Artifacts".

The build details table shows the following information:

Build Name	Go to Jenkins	Start Time	Elapsed time	Launched by	Association
test build pipeline#2 (test build pi...	Go to Jenkins	May 14, 2020 - 00:41	00:12	Started by user admin	attached

The console output shows the following steps:

```
1 Started by user admin
2 Running in Durability level: MAX_SURVIVABILITY
3 [Pipeline] Start of Pipeline
4 [Pipeline] node
5 Running on Jenkins in /var/lib/jenkins/workspace/test build pipeline
6 [Pipeline] {
7 [Pipeline] stage
8 [Pipeline] { (Build)
9 [Pipeline] cleanWs
10 [WS-CLEANUP] Deleting project workspace...
11 [WS-CLEANUP] Deferred wipeout is used...
12 [WS-CLEANUP] done
13 [Pipeline] git
14 No credentials specified
15 Cloning the remote git repository
16 Cloning repository https://github.com/sureshmurthy85/forrester_demo_2020.git
17 > /usr/bin/git init /var/lib/jenkins/workspace/test build pipeline # timeout=10
18 Fetching upstream changes from https://github.com/sureshmurthy85/forrester_demo_2020.git
19 > /usr/bin/git --version # timeout=10
20 > /usr/bin/git fetch --tags --progress https://github.com/sureshmurthy85/forrester_demo_2020.git +refs/heads/*:refs/remotes/origin/* # timeout=10
21 > /usr/bin/git config remote.origin.url https://github.com/sureshmurthy85/forrester_demo_2020.git # timeout=10
22 > /usr/bin/git config --add remote.origin.fetch +refs/heads/*:refs/remotes/origin/* # timeout=10
23 > /usr/bin/git config remote.origin.url https://github.com/sureshmurthy85/forrester_demo_2020.git # timeout=10
24 Fetching upstream changes from https://github.com/sureshmurthy85/forrester_demo_2020.git
25 > /usr/bin/git fetch --tags --progress https://github.com/sureshmurthy85/forrester_demo_2020.git +refs/heads/*:refs/remotes/origin/* # timeout=10
```

The left sidebar shows the build tasks and their status:

- 8 Tasks, 2 Completed
- 1. Pull Jira Tickets (1st run, 100% completed)
- 2. Pull (1st run, 100% completed)
- 3. Jenkins Build (100% completed)
- 4. Deploy and Scan (100% completed)
- 5. Unit Tests (100% completed)
- 6. Run SonarQube (100% completed)
- 7. Create ServiceNow Ticket (100% completed)
- 8. Verify Switch Blue-Green (100% completed)

The right sidebar shows the build artifacts and the build status (1x, 6% completed).



Example - Approvals

CloudBees
CD

My Work

DevOps Insight
Dashboards

DevOps
Foresight

Service
Catalog

Release
Calendar

System Administrator

Forrester / Releases / Motorcycle Release 3.0 / Runs / Pipeline Runs / Reports

Reports

ApprovalsTime DurationEvidence

Pipeline Run Details

Status	Release name	Release run	Current Stage	Start time	End time
✓	Motorcycle Release 3.0	Motorcycle Release 3.0_Motorcycle Release Pipeline_344_20200515061430		05/14/2020 @ 23:14	05/14/2020 @ 23:35

Report Details

Stage	Type	Task Name	Comment	Approver	Status	Date
SIT	Task	Verify QA Notify		admin	✓	05/14/2020 @ 23:24:25
PROD DC1	Pre	WaitforCR_Approval		admin	✓	05/14/2020 @ 23:29:00
PROD DC1	Task	Verify Switch Blue-Green		admin	✓	05/14/2020 @ 23:32:15
PROD DC2	Pre	Approve DC2		admin	✓	05/14/2020 @ 23:32:29
PROD DC2	Task	Verify Switch Blue-Green		admin	✓	05/14/2020 @ 23:35:28

Build Details

Status	Build Name	Branch name	Association	Duration	Username
🔄	Cart#3		attached	00:19	Started by GitHub push by avannathur
🔄	Cart#4		attached	00:20	Started by GitHub push by avannathur
🔄	login#2		attached	00:09	Started by user admin
🔄	login#3		attached	00:11	Started by user admin



Example - Approvals

Approval Audit Report

General Information

Label	Value
Pipeline Execution	Motorcycle Release 2.0_Motorcycle Release Pipeline_294_20200323195254
Pipeline Name	Motorcycle Release Pipeline
Execution Start	2020-03-23T19:52:54.556Z
Execution Complete	2020-05-14T19:41:04.658Z
Status	success

Details

Stage	Type	Label	User	Status	Date	Comment	
DEV	QA	POST	Ensure Passing Tests	[Auto-approved by conditional]	success	2020-03-23T20:01:04.321Z	Auto-approved by conditional: Ensure Passing Tests
	Pre-Prod	PRE	Release Management	System Administrator	Approved	2020-03-23T20:03:45.880Z	
		TASK	Verify QA / Notify	System Administrator	success	2020-05-14T19:39:57.417Z	
	PROD	POST	Gate on Test Results	[Auto-approved by conditional]	success	2020-05-14T19:40:00.210Z	Auto-approved by conditional: Gate on Test Results
		PRE	WaitforCR_Approval	System Administrator	Approved	2020-05-14T19:40:39.458Z	
		TASK	Verify Switch Blue-Green	System Administrator	success	2020-05-14T19:41:00.100Z	



Example - Evidence Links

CloudBees
CD

My Work

DevOps Insight Dashboards

DevOps Foresight

Service Catalog

Release Calendar

System Administrator

Forrester / Releases / Motorcycle Release 3.0 / Runs / Pipeline Runs / Reports

Reports

Approvals

Time Duration

Evidence

DEV	Jenkins Job	Deployed App: http://jenkins.acme-global.com:8080/job/motorbike-2/255/
DEV	Git Commit	Deployed App: /commander/pages/ECSCM-Git-3.9.0.77/reports?jobId=a3b2f6a7-89c8-11e9-a1f2-06fe7d1e6f5a
DEV	JIRA Updated Issues Report	Download Report
SIT	Site Link	Deployed App: http://dev.acme-global.com/app
SIT	Test Results	Click here for report
SIT	ServiceNow Change Request:	Go to CHG0039613 on service-now.com
PROD DC1	Site Link	Deployed App: http://prod.acme-global.com/app
PROD DC2	Site Link	Deployed App: http://prod.acme-global.com/app
Audit Reports	Approval Audit:	Summary Report
Audit Reports	Evidence Links Audit:	Summary Report
Audit Reports	Task Duration Audit:	Summary Report

Build Details

Status	Build Name	Branch name	Association	Duration	Username
<div><div></div><div></div></div>	Carts#3		attached	00:19	Started by GitHub push by avanmathur
<div>Code Commits</div> <div>Commit 97202bae6e12f02d7d05a02af211a62f171d4e48</div>		<div>Test Results</div> <div><div>83%</div><div>17%</div></div> <div>Test Result</div> <div>8 ms</div> <div>See All</div>		<div>Build Artifacts</div> <div>com.demo:helloworld</div>	
<div><div></div><div></div></div>	Carts#4		attached	00:20	Started by GitHub push by avanmathur
<div>Code Commits</div> <div>Commit 12b8f19f52a5fa8ff4f676aef012770a531k3f2</div>		<div>Test Results</div> <div><div>83%</div><div>17%</div></div>		<div>Build Artifacts</div> <div>com.demo:helloworld</div>	



Example - Duration

CloudBees
CD

My Work

DevOps Insight
Dashboards

DevOps
Foresight

Service
Catalog

Release
Calendar

System Administrator

Forrester / Releases / Motorcycle Release 3.0 / Runs / Pipeline Runs / Reports

Reports

Approvals

Time Duration

Evidence

PROD DC2	Task	BLUE-GREEN Deploy to Prod	project: Forrester	01:33	✓
PROD DC2	Task	Run Smoke Tests	project: AcmeGlobal	304 ms	✓
PROD DC2	Task	Update Prod Status	admin	00:00	⚙️
PROD DC2	Task	Verify Switch Blue-Green	admin	01:24	✓
PROD DC2	Task	Switch LoadBalancer between BLUE-GREEN	project: RollingDeployments	738 ms	✓
PROD DC2	Task	Update BLUE-GREEN	project: Forrester	588 ms	✓
Audit Reports	Task	Approval Report	project: EC-AuditReports-1.4.1	960 ms	✓
Audit Reports	Task	Evidence Report	project: EC-AuditReports-1.4.1	00:01	✓
Audit Reports	Task	Duration Report	project: EC-AuditReports-1.4.1	979 ms	✓

Build Details

Status	Build Name	Branch name	Association	Duration	Username
🔄	🔄 Carts#3		attached	00:19	Started by GitHub push by avannathur
🔄	🔄 Carts#4		attached	00:20	Started by GitHub push by avannathur
🔄	🚩 login#2		attached	00:09	Started by user admin
🔄	🔄 login#3		attached	00:11	Started by user admin
🔄	🔄 login#4		Triggered by CI	00:13	Started by user admin



The Way Forward



Auditing the New Way

- “Automation is Auditing”
- Orchestration layer over the top of everything
- Centralized mechanism for one-click audits



Seven Steps to Audit-Ready Pipelines

- Get key stakeholders involved
- Conduct value stream mapping
- Adopt a holistic approach to software delivery
- Watch closely for vulnerabilities
- Understand everything you have in production
- Prioritize culture
- Don't try to boil the ocean

