Cloud Foundry: The Gaps

Cloud Foundry Summit

John Wetherill
Principal Architect

May 23, 2015
BNY Mellon

• Founded 1784
• $29.1 trillion in assets under custody and/or administration
• $1.6 trillion in assets
• 13,000 people in global enterprise IT staff
• We’ve been building PaaS / Cloud / Microservices / Java for 16 years
NEXEN Platform

BNY Mellon eXtreme Platform (BXP)

1.8+ bn Requests Per Month

100% App Monitoring

Mature
- Third generation BNY Mellon utility platform
- Primary environment for web technology
- Foundational element for NEXEN ecosystem

Digital
- Private cloud, multi-datacenter, public-ready
- Integrated developer tools
- Open source common software stack
- Rapid onboarding of developers and apps

Platform
- Infrastructure and applications in one bundle
- Not just a cloud – platform as a service allows switching out infrastructure providers
- Cloud Foundry provides industry-standard open source foundation for continued cloud innovation
### Powering the World’s Investments

#### During Development

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SETUP AND CODING</strong></td>
<td><strong>SETUP AND CODING</strong></td>
</tr>
<tr>
<td>2 to 4 weeks</td>
<td>One Day</td>
</tr>
<tr>
<td>- Tools selected, funded, purchased each time</td>
<td>- Everyone uses same tools and collaborates</td>
</tr>
<tr>
<td>- Application specific versions</td>
<td>- Automated self-serve setup</td>
</tr>
<tr>
<td>- Multiple steps and approvals</td>
<td>- Easy to scale teams and share resources</td>
</tr>
<tr>
<td>- Manual install steps, configuration, updates</td>
<td>- Lower-cost cutting-edge open source tools</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>TESTING AND QA</strong></th>
<th><strong>TESTING AND QA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 to 12 weeks</td>
<td>One Day</td>
</tr>
<tr>
<td>- Environments are silo-funded, and built for each app</td>
<td>- Defined once and spun up as needed, variable cost</td>
</tr>
<tr>
<td>- Capital and labor to install, configure, and debug</td>
<td>- Continuous integration and delivery for alignment</td>
</tr>
<tr>
<td>- Expensive and difficult to make “just like production”</td>
<td>- Higher velocity development, “fast fail” innovation</td>
</tr>
<tr>
<td>- Difficult to keep patched and upgraded</td>
<td>- Automated approval and staging</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>PRODUCTION</strong></th>
<th><strong>PRODUCTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 to 16 weeks</td>
<td>One Day</td>
</tr>
<tr>
<td>- Environments are silo funded and built for each app</td>
<td>- Defined once and spun up as needed, variable cost</td>
</tr>
<tr>
<td>- Capital and labor to install, configure and debug</td>
<td>- Common platform and active-active disaster recovery</td>
</tr>
<tr>
<td>- Disaster recovery is complex and active-passive</td>
<td>- Test and certify once for all for risk and info security</td>
</tr>
<tr>
<td>- Difficult to keep patched and upgraded</td>
<td>- Automated refresh &amp; patching tools for rolling upgrades</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>INFRASTRUCTURE</strong></th>
<th><strong>INFRASTRUCTURE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 to 16 weeks</td>
<td>Less than one hour</td>
</tr>
<tr>
<td>- Each team secures capital funding</td>
<td>- Funded and built one time, pay as you go</td>
</tr>
<tr>
<td>- Each application engineered separately</td>
<td>- Resiliency and availability features are built in</td>
</tr>
<tr>
<td>- Multiple design and approval steps and labor to install</td>
<td>- Automation for installs and refreshes frees up staff</td>
</tr>
<tr>
<td>- Maintenance and patching falls behind</td>
<td>- Common solution reduces errors and downtime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SYSTEM SOFTWARE</strong></th>
<th><strong>SYSTEM SOFTWARE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 to 8 weeks</td>
<td>Less than one hour</td>
</tr>
<tr>
<td>- Each application is a separate manual software install</td>
<td>- BXP assemblies support rapid builds of complex apps</td>
</tr>
<tr>
<td>- Multiple skillsets, steps, approvals to configure &amp; maintain</td>
<td>- Installed, configured, and maintained automatically</td>
</tr>
<tr>
<td>- Patches and upgrades fall behind, create business risk</td>
<td>- Staff focused on DevOps, not software administration</td>
</tr>
<tr>
<td>- Hard to integrate with other systems, lots of duplication</td>
<td>- Integration features are part of the stack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>APPLICATION SOFTWARE</strong></th>
<th><strong>APPLICATION SOFTWARE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Weeks to months</td>
<td>Hours to days</td>
</tr>
<tr>
<td>- Application-specific stacks, tools, and feeds</td>
<td>- Solutions built quickly assembling APIs and services</td>
</tr>
<tr>
<td>- Separate installation, certification, review, &amp; maintenance</td>
<td>- Components pre-tested for security, risk, scale, resiliency</td>
</tr>
<tr>
<td>- Hard to share and reuse, multiple skillsets</td>
<td>- Teams delivering solutions, not jockeying the data center</td>
</tr>
<tr>
<td>- Capital, funding, purchasing, and installs for each team</td>
<td></td>
</tr>
</tbody>
</table>
Challenges

• Highly regulated industry
• High volume mission critical transactions
• HA a high priority
• Multi-global data center DR
• Security is paramount
• Legacy codebase, technologies, processes
• Silos
• Mergers and Acquisitions
• Integration: Partners, Vendors, Customers
Highly Regulated Industry

- Audits
- Secrets
- Reproducibility
- Fraud detection
- Social responsibility
- Financial reporting and disclosure agreements
- Privacy
- Consumer protection
- Rigid approval processes
Separation of Duties

• Driven by regulations
• Every process improvement or change regulated
• Internal and external auditors are stakeholders
• Coders must not deploy
• Deployers must not code
• Impacts entire SDLC
• Significant impact on PaaS
High Volume Mission Critical Transactions

- Two billion requests / month
- Every request consumes a server thread
- Financial penalties for processing delays
- Challenge: run really critical stuff!
- Peak times: before markets close all transactions sent to exchange
- Delays incur financial penalties
Global Financial Provider

• We deal with exchanges and financial institutions across the globe
• 24x7 operation
• No luxury of downtime
• Strict SLAs, time limits, response times
• Regional and global regulations complex and evolving
DR Across Multiple Global Data Centers

- DR is regulated requirement
- Apps run in second DC
- Minimum distance is regulated
- Entire application stack must be duplicated
- No SPOFs
- Need to show that it runs
- Once a year - validate this
- Typically we run these tests every quarter
- Then report to regulatory bodies results of DR testing
- Testing for disaster much harder than Handling disaster
- Must simulate failover
DR Validation

• Need to demonstrate DR to regulatory bodies
• Yearly validation
• We validate DR run these tests every quarter
• Must report DR testing results to regulatory bodies
• Testing for disaster much harder than simply handling disaster
• Must simulate failover without interruption
Security

• Strict regulations
• Apps need multi-factor auth
• Multiple-id/security questions, PINs, unique picture, captchas
• Driven by industry best-practices and regulations
• Discover, detect and eradicate vulnerabilities immediately
• Site scanning
Overcoming the Challenges
Strategies

- Devops
- Microservices
- Containerization
- Hybrid Cloud
- Monitoring
- Unified Security Model
- Cloud Native / 12 Factor
- Transparency
- Agility
- Continuous Delivery
- API Driven
- Testing and Chaos
- Practices and Patterns
- Open Source
We Embrace Open Source

• Reduce technology obsolescence
• Better manage risk
• Avoid vendor lock-in
• Cut costs
• Significantly improve developer productivity
• Variable-cost instead of capital expenditure
Strategies

• PaaS
• Onboarding
• Rapid development
• Consistent environment
• Reproducible
• Regulations and policies
• Complex approval processes
Cloud Foundry at BNY Mellon

• BNY Mellon is Gold member of Cloud Foundry Foundation
• Cloud Foundry is integral part of our cloud strategy
• No vendor lockin
• Monitoring
• Log aggregation
• Security
• Self-service
• On demand
• Scaling
• Versioning
• Hybrid Cloud Strategy
The Gap

- OS Certification
- Integration with existing user management system
- Multi-datacenter support
- Network topology constraints
- Complex application topologies
- Docker Ecosystem
The Gap

- Non-HTTP workloads
- Service Discovery
- Multi-Datacenter Orchestration
- Failover Support
- Application Grouping (Assemblies)
- OS Support
- Rack-awareness
- Hot/Cold Storage
The Gap

- Shared local filesystem
- SSO / Auth
- Buildpack complexity
- Dealing with centralized dependency management and failover
- Secrets
- Security (what do I mean here?)
- Versioning
- Some features not-ready-for-prime-time
The GAPs in Detail
OS Certification

• Many enterprise products not certified to run on Ubuntu
• Compliance and certification constraints
• Specific apps and services restricted to certified OS’s
  • SiteMinder
  • eTrust
• We certify a targeted and limited list of supported OSs
Multi-Datacenter Orchestration

- Use case for DR test:
  - flip all traffic
  - move to other DC
  - quiesce primary workloads
  - run for a while
  - then flip back
  - complex workers reading files, pulling from queue must be stopped, checkpointed, restarted
Multi-Datacenter Orchestration

• Must be seamless, simple, fully automated
• Need “Uber-PaaS” to orchestrate across multiple DCs
• Single control pane to manage:
  • single app/collections of apps
  • multiple AZs
  • multiple clouds
• Further challenge: integrating with Vendor tech: monitoring, LB
Network and Application topology constraints

- Two instances of app that don’t even each other
- Inter-application (inter-container) communications
- Complex isolation requirements
Container Ecosystem

• Assemblies (docker-compose)
• Need container “login”
• Simple network partitioning
• Internal and external Docker registry
• Volumes, networks, users
• PoCs: Docker Hub
Buildpack complexity

- Eg: Java buildpack is Ruby
- 17000 lines
- Requires in-house Ruby expertise to customize
- Overhead of internal maintenance of custom bp codebase
Non-HTTP workloads

• Non-HTTP
• Any protocol, or no protocol (binary data)
• UDP too
• These need to provisioned, wired, routed, monitored, versioned
Application Grouping (Assemblies)

• We have complex apps with multiple “partitions” including:
  • Vendor software
  • Twelve-factor apps/services
  • Legacy apps
  • Cronjobs, batch jobs, and misc. workers
  • HA services
Application Grouping (Assemblies)

- Twelve factor is the easy part, the rest is hard
- Entire application needs:
  - Automation
  - Cloud practices
  - Versioning
  - Rollback/rollforward
- We need abstractions that can weave all this together into a single manageable assembly
Application Grouping (Assemblies)

• Dependency Management:
  • Find latest version of service and use it
  • Have app team bind in the required dependencies
  • Can be tested in dev
  • We haven’t solved this. Neither has CF.
  • More important as we add more microservices
Affinity / Rack-awareness / Hot - Cold / GPUs / FPGAs

• Locality for Hadoop
• Need to tag hardware resources for specialized use
  • hot/cold storage
  • Specialized processors
    • GPUs
    • FPGAs
• Location Awareness, rack awareness
Need shared local filesystem

• Some legacy apps require shared local filesystem
• Need quick way to deploy these
SSO / Auth

• Lots of customers
• Lots of integration points and integration systems
• Need to support all SSO standards
• Integrate B2C and B2B
• Third parties… vendors, customers, acquisitions
• Must integrate backward with everything from AS400 to Mesos/Kubernetes
Secrets

• Secret management is regulated
• Developer and deployer must never access secrets
• Exposing secrets via environment is risky
• Need sophisticated secrets management
• Trust
Cloud Foundry: The Fit

- Strong Community
- Open Source
- Twelve Factor
- Microservices
- Hybrid Cloud
Cloud Foundry: The Fit

- Workload Portability Between Private/Public Clouds
- Docker
- Rapid deployment
- Service Broker
- URL Provisioning
Cloud Foundry: The Fit

• Logging
• Polymorphism
• Security groups
• No Vendor Lockin
• Multi-cloud
Cloud Foundry: The Fit

• No IaaS tie-ins
• Separation of Concerns
• Works well with across multiple zones within a high-speed DC
Our Solution

• Use our existing PaaS (BXP)
• Incorporate Cloud Foundry as PaaS component
• Single Cloud Foundry instance running in each DC
• Cloud Foundry deals with all the things it’s good at
• BXP takes care of the gaps
Overall Cloud Foundry Benefits

- Dramatically simplified app deployment
- Simplified application descriptors (assemblies)
- Faster developer onboarding
- Automated URL provisioning for non-prod
- Instant Docker PoCs (with Diego)
- Instant hybrid cloud support (AWS, Azure, internal)
Questions?

John Wetherill
@bcferrycoder
john.wetherill@bnymellon.com
BNY Mellon Innovation Centers

- Palo Alto USA
- Jersey City USA
- Pittsburgh USA
- Pune India
- Chennai India
- London England
We’re hiring:  https://jobs.bnymellon.com/

- Principal Hadoop Architect-Engineer
- Principal Hadoop Performance Architect-Engineer
- Platform Java Engineer-Open Source
- Principal Engineer-Cloud Developer
- Platform Engineer-Nexen Gateway
- Innovation Center Engagement Director
- Blockchain Senior Product Manager
- Technical Project Manager/Scrum Master
- Front End Developer/Engineer
- API Principal Product Manager
- Platform Java Engineer-Open Source
- Senior Front End Developer-Engineer

BNY Mellon is an Equal Employment Opportunity/Affirmative Action Employer. Minorities/Females/Individuals With Disabilities/Protected Veterans
Attend today’s panel discussion:

Hybrid Cloud in Finance

4:50pm Tuesday May 24
Ballroom B