ANALYST INSIGHT

DevOps: Advances in release management and automation

The Ovum rainbow map for DevOps solutions comparing 11 vendors

Reference Code: OI00172-072

Publication Date: September 2011

Author: Michael Azoff

SUMMARY

Catalyst

DevOps originated with operations as a means of streamlining and improving the effectiveness of operations in the face of increasing workload. Traditionally operations had the time to deal with application stability, risk, and performance issues on one hand, and infrastructure management and procurement tasks on the other. This changed with the simultaneous adoption of Agile practices in development resulting in increased deployment frequency, while at the other end the trend towards cloud and virtualization speeded up and lowered the costs relating to hardware issues - almost overnight operations became the bottleneck. The availability of new deployment solutions has significantly helped operations by automating many manual operations. The solutions from a range of leading vendors and innovators in release management and automation are compared side by side in the Ovum rainbow map for DevOps. This solution guide and comparison will help IT managers choose a solution that is a good fit for their operations needs.

Ovum view

DevOps is variously defined as a movement or a set of principles, practices, methods, or concepts - the reality is that it is a mix of all these attributes. In addition, especially as vendors begin to address the concerns of DevOps and the pain points that IT operations are suffering, DevOps is

evolving. Perhaps unsurprisingly given the relative newness of the subject, DevOps and related ITIL terminology differ in emphasis between vendors; in particular they refer to different shades of meaning between continuous delivery and continuous deployment. What can be agreed is that DevOps originated from within IT operations.

Ovum has researched the leading players in an area receiving renewed focus, release management automation, and has conducted a comparative study of these solutions. A DevOps features matrix was created and the resulting comparison shows Electric Cloud, HP, IBM, Serena, and UrbanCode to have the most comprehensive coverage of the features desired in advanced DevOps solutions. The areas that were most lacking amongst solutions were build and performance testing, with vendors typically relying on third party solutions to offer those features.

The report, 'DevOps: agile operations and continuous delivery', has been written to accompany this report, examining the issues around DevOps for development and operations, and how vendors are extending concepts - see the references for details.

In summary:

- DevOps is supported by release management and deployment tools; this market is diverse, attracting renewed vigor by established players and new entrants.
- The focus of deployment solutions is on supporting the planning and orchestration of releases; some tools have origins in development and include build management, others have an operations background and are strong on process workflow.
- The maturity of integration between development and operations is indicated by whether the solution is able to support continuous delivery: straight through release from code check-in to final staging (test or production as required).

Key messages

- The release management and automation tools market has been re-vitalized by DevOps.
- Ovum believes application security needs to be a first level concern in software lifecycle management, due to the shift to web and mobile applications and the lack of reliance on the environment for security.

THE RELEASE MANAGEMENT AND AUTOMATION TOOLS MARKET HAS BEEN RE-VITALIZED BY DEVOPS

Release automation market players and trends

A new breed of solutions in release management and automation has emerged. Key vendors include: BMC, HP, IBM, Electric Cloud, Nolio, Puppet Labs, rPath, Serena, ServiceNow, Streamstep, ThoughtWorks Studios, UrbanCode, and Xebialabs. These new generation tools automate the deployment process, providing source and binary file version control for scripts and configuration files, providing a workflow or process engine for automating complex build processes, and offering straight-through development to production or testing stage automated deployment, taking out numerous manual steps in traditional deployment processes.

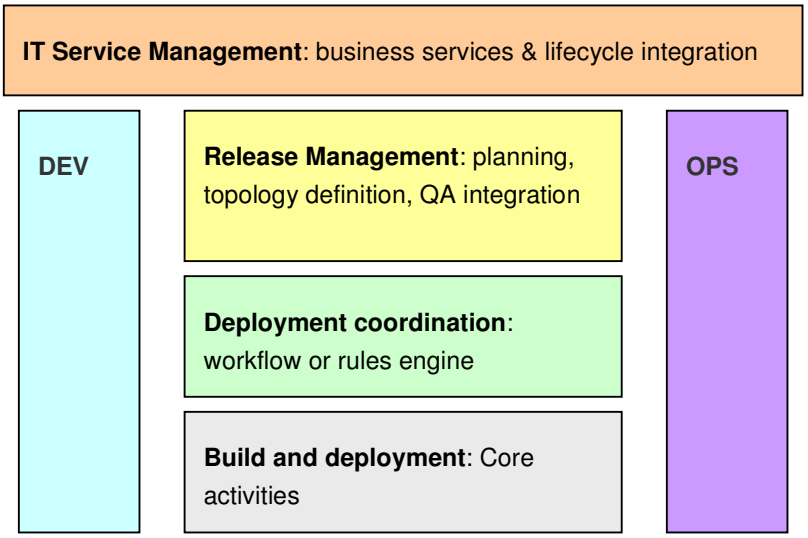
The DevOps tooling space can be thought of as four layers with a left (dev) and a right (ops) side representing the historical roots of the vendors: see figure 1. In the lowest category are the actual build and continuous integration tools, all of which are open source: Ant, Maven, Gradle, Opscode Chef, Glu, Puppet (open source), Jenkins, and Hudson. The middle layer covers deployment coordination, which is where the workflow or rules engine provides the deployment process definition and execution. The next layer offers release management with planning, topology definition, and integration between the developer's defect management tools and the business side help desk. All the vendors participating in this report's solution comparison study span the second and third layers. The top layer represents integration with IT Service Management (ITSM) and is offered by the larger IT vendors. The key benefit is in integration between help desk tickets and defect management logs.

In addition IBM and HP, with wide solution portfolios, are beginning to take DevOps automation one step further by addressing performance testing and management and QA activities into one complete end-to-end lifecycle activity with feedback from production back into development.

Ovum invited some of the leading players in the DevOps space to participate in a comparative study of their release management and automation solutions. The participating list is not exhaustive of vendors in this space and there are other players that should be investigated, including CA, CFEngine, Cisco, Citrix, Microsoft, Nolio, Opscode, Oracle, Puppet Labs, Red Hat and VMware.

A brief snapshot of each vendor examined in this review follows next, after which the results of the comparison are presented in the Ovum Rainbow Map for DevOps:

Figure 1: Layers of DevOps tools



Source: Ovum

Serena

Serena has embarked on a strategy to address the needs of DevOps through the Serena Release Management Solution, comprising three modules: Release Control powered by Serena Business Manager (SBM) for planning, management and release approval; Release Vault powered by Dimensions CM and ChangeMan ZMF for secure, auditable path to production; and Release Automation powered by Nolio (under an OEM agreement) for the automation of application configuration and deployment tasks. Serena Service Manager provides a process-based approach to orchestrating the service management lifecycle: Serena Release Manager provides a view into Serena's ALM dashboard with release management KPIs, and the Release Control product makes use of Release Trains and Release Calendars to schedule and coordinate releases. The final link in Serena's plans around ITSM integration is in the current pipeline. The solution performs strongly in most sections of the Ovum DevOps Rainbow except performance testing, though Serena has indicated this is in its future product plans.

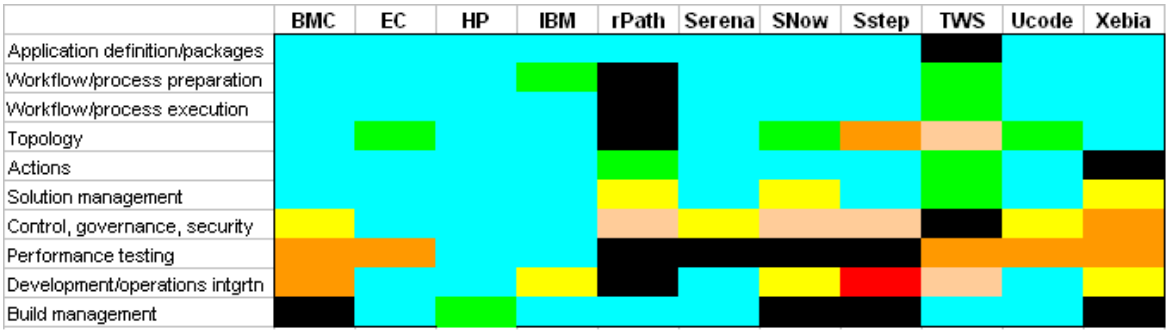
Ovum Rainbow Map for DevOps: solution feature comparisons

Ovum invited 11 leading vendors in the DevOps space to participate in a comparative study of features. Each vendor completed a comprehensive Ovum Features Matrix for DevOps and this information was rolled up into sections and rainbow-mapped according to the key given below. The Ovum Rainbow Map for DevOps is shown in Figure 2.

The results of the comparative study show that Electric Cloud, HP, IBM, Serena, and UrbanCode have comprehensive coverage of the features desired in advanced DevOps solutions. A number of the vendors have a policy of relying on third party tools to fulfill areas of functionality and will be suitable for many users with existing tools in place. Build and performance testing were the most common such gaps in the DevOps solutions examined here.

Many factors go into the selection of a solution and it is important to note this study is restricted to solution features. Other considerations are price, customer service and customer relationship, choice of hosted cloud/SaaS offering, and specific integrations unique to each customer. Ovum believes all the vendors in this comparative study are worthy of consideration when selecting a release management and automation solution.

Figure 2: Ovum Rainbow Map for DevOps



Source: Ovum.

Vendor key: EC = Electric Cloud, SNow = ServiceNow, Sstep = Streamstep, TWS = ThoughtWorks Studios, Ucode = UrbanCode

key	%
	83.3-100
	66.7-83.3
	50-66.7
	33.3-50
	16.7-33.3
	0.01-16.7
	0.0

OVUM

The features matrix is based on the following categories of solution features:

- **Application definition/packages**: Define the application and application package, be able to release both packaged and unpackaged applications, define the application configuration requirements, and be able to make necessary changes in databases and application servers through advanced integration.
- **Workflow/process preparation**: A visual design and modeling tool for the release workflow, allowing design by drag-and-drop, or design by scripts, and offer a content library of prebuilt workflows for common processes.
- **Workflow/process execution**: Be able to execute the workflows directly from the visual modeling environment or from algorithm-based workflow environments, be able to execute from the workflow dashboard, create parallel workflows for complex releases, define release processes for multi-tier applications including versions of tiers required to support tier objects, create programmatic loops for advanced release requirements, offer real-time status visibility of process steps, be able to start, pause, and stop processes, as well as rollback a process.
- **Topology**: Discover existing application and infrastructure topologies, integrate with a CMDB to learn about assets to automate, pull versioned deployable artifacts from an asset database (an ITIL Definitive Media Library), offer integration between the deployment engine and the artifact repository, and include an integrated artifact repository, define configurations for database, system, network etc, define private/public/hybrid cloud/virtual environments, and define configuration property mappings/dependencies between tiers.
- **Actions**: Covering installation, verification, and other actions. Providing audit trails of all actions. Using either script-less interface for defining actions or scripted actions.
- **Solution management**: Server agent management; workflow and topology plans, version control of plans/workflow/topology; workflow capacity planning, capacity modeling; permissions management / Role Based Access Control (RBAC) compliance; reporting on what is installed, where, when, and custom reporting; collaboration support including IM, wiki/knowledge base, automatic emails, logging, scheduling, and notifications; dashboard/console for managing deployment processes; unlimited number of target machines; covers Windows, Linux, Unix, Mac - machines/cross-platform neutrality; covers mainframes; and covers mobile applications.

- **Control, Governance, Security**: Register deployment changes in a CMDB; detect out-of-process changes to operational environment; provide traceability between application and operations assets; perform preliminary validation; define hardware, software, network checks; and for security offer integration of development time vulnerability analysis with run-time threat management, identity, and access control. Ovum believes application security needs to be raised as a first level concern due to the shift to web and mobile applications where the environment can not be relied upon for security and therefore the application needs to be responsible for security.
- **Performance testing**: Capture operational performance metrics for applications in normal production situations, automated performance testing for updated applications against current baseline performance, and capture test output for governance purposes.
- **Development/Operations Integration**: All development and operational assets kept in a single asset DB, be able to audit operational configurations for changes to operational environments, have integrated change/release management processes for development and operations; be able to offer Continuous Deployment: from check-in to production (solution allows this possibility with all automated testing included); production incident/defect tracking and remediation; linking operational incidents to defect reports; coordination of defect root cause analysis between development and operations; shared information on known defects, workarounds etc; incident/defect service level and performance tracking/reporting across the lifecycle and organizations.
- **Build Management**: Capture files dependencies, and perform intelligent builds so that rebuilds only affect changed components; perform pre-production automated build, verify, and test.

APPLICATION SECURITY AS A FIRST LEVEL CONCERN

Ovum believes application security needs to be a first level concern in software lifecycle management, due to the shift to web and mobile applications and a consequent lack of reliance on the environment for dealing with security. Web applications are designed to punch through the firewall and mobile application development is a relatively immature industry. As we increasingly read in the newspaper headlines, platforms such as Apple iOS and Google Android are being targeted by malware writers, who are discovering weak security and holes in these environments.

It is not just web and mobile, of course, where application security needs to be a top level concern, we should include all types of software applications. Application security is difficult for a number of

reasons: expertise is not widespread in the developer community; it is a specialist activity and is often needed to be brought in from externally. The nature of application security is continually changing as the code is changed throughout the lifecycle. The application architecture should have security as one of its concerns, but architecture alone is not sufficient - security needs to be thought of at the design detail level.

Related to these considerations is security testing. Vulnerability analysis workshops (see for example http://www.infoq.com/articles/threat-modeling-express) can be run at the start of a project to assess what issues may impact the application. These sessions focus on domain specific threats, also known as white box threats, where knowledge and expertise of the application domain is used to examine what could happen. Discussions range beyond what tools can cover and include operations disruptions, theft, harm to human safety etc. In part two of the workshop, these threats are prioritized and are then mapped to weaknesses in the application. In the final stage of the workshop the discussion focuses on counter-measures. One of the elements in application testing is to ensure that these issues have been addressed and once the application is in production then operations need to alert to the issues as well.

RECOMMENDATIONS

Recommendations for enterprises

The DevOps solutions covered in this report provide the tiers of tooling and automation necessary to deal with operations pressure. In a nutshell, at the top we have planning and scheduling, below that is the coordination and execution management, and the lower tier is the core automation for build and deployment. DevOps is not static, already vendors are integrating solutions with ITSM services. These trends will have a significant impact on how IT is executed in enterprises - the time to review and plan a DevOps strategy is now. Creating a DevOps role is also advisable for the larger organizations.

The activities being improved in operations start in development and this is where the complete cycle of build, test, and continuous integration has been driven by Agile methodologies like test driven development. Solutions that provide continuous deployment take the next step and enable straight through development change to production deployment, when and where it is needed. Vendors whose solutions covered here that can offer continuous deployment are: Electric Cloud, HP, ThoughtWorks Studios, UrbanCode, and XebiaLabs.

Recommendations for vendors

There are opportunities opening up in the DevOps automation space. The release management tools space is still a young market - penetration into IT departments is low, with many organizations relying on manual operations and open source software, which while suitable for small operations, are not adequate for those running complex applications or medium to large scale departments. It is also the case that operations is a mission critical function for businesses today, and these businesses will pay for the right solution. Ovum believes that opportunities exist for technical innovation in this market and for far greater penetration of release management automation into IT departments and data centers.

APPENDIX

Further reading

- DevOps: Agile operations and continuous delivery. Michael Azoff, September 2011.
- DevOps: Connecting IT development and operations. Laurent Lachal. Ovum report OI00005-001, 20 October 2010.
- ALM and ITIL: Spanning the divide with IT operations. Tony Baer. Ovum report OVUM052423, 1 September 2010.
- Software Lifecycle Management 2011. Michael Azoff, Tony Baer, Chandranshu Singh. Ovum TEC Report OI00068-004, 10 May 2011.
- Solutions Guide: Desktop Virtualization. Ovum report OI00127-011, 14 June 2011.

Methodology

This report is based on Ovum's extensive research experience in the software lifecycle management space, interviews with vendors, and consulting with our end users. The product comparison used a comprehensive Ovum Features Matrix for DevOps which the participating vendors completed. The features matrix and weightings used in this research are given below:

Ovum DevOps August 2011 Features Matrix

Vendor product feature scoring (not shown): 1 = out-of-box from product portfolio, 0.5 = partial fulfillment, 0 = no capability, T = available through third party (scored as zero)

		Weight	Subweight
Application definition/packages	Define applications	10.42	1

	Add unpackaged software		1
	Add packaged software		1
	Define application configuration requirements		1
	Advanced integrations with databases and application servers		1
Workflow/process preparation			
	Visual design and modeling of workflow	7.29	5
	Design by drag and drop		1
	Design by scripts		1
	Content library of prebuilt workflows for common processes		1
Workflow/process execution			
	Executable workflow	7.29	5
	Create parallel workflows		2
	Define multi-tier processes, including versions of tiers		2
	Create programmatic loops		1
	Real-time status visibility of process steps		1
	Start, pause, and stop processes		2
	Process rollback		5
Topology			
	Discover existing application topologies	10.42	1
	Integrates with a CMDB to learn about assets to automate		1
	Pulls versioned deployable artifacts from an asset database (an ITIL Definitive Media Library).		1
	There is integration between the deployment engine and the artifact repository		1
	Includes an integrated artifact repository		1
	Define configurations for database, system, network etc		1
	Define private/public/hybrid cloud, virtual environments		1
	Define configuration property mappings/dependencies between tiers		1
Actions			
	Installation, verification, other actions	10.42	1
	Audit trail of all actions		1
	Script-less interface for defining actions		1
	Scripted actions		1
Solution management			
	Agent management	10.42	1
	workflow and topology plans		1
	version control of plans/workflow/topology		1

	workflow capacity planning, capacity modeling		1
	Permissions management / Role Based Access Control compliance		1
	Reporting: what is installed, where, when, custom reporting		1
	Collaboration: IM, wiki/knowledge base, automatic emails		1
	Logging, scheduling, and notifications		1
	Dashboard/console for managing deployment processes		1
	Unlimited target machines		1
	Covers Windows, Linux, Unix, Mac machines/cross-platform neutrality		1
	Covers mainframes		1
	Covers mobile		1
Control, Governance, Security	Register deployment changes in CMDB	12.50	1
	Detect out-of-process changes to operational environment		1
	Traceability between application and operations assets		1
Preliminary validation	Define hardware, software, network checks		1
Security	Integration of development time vulnerability analysis with run-time threat management, identity, and access control		3
Performance testing	Capture operational performance metrics for applications in normal production situations	7.29	1
	Automated performance testing for updated applications against current baseline performance		1
	Capture of test output for governance purposes		1
Development/Operations Integration	All development and operational assets in asset DB	15.63	1
	Audit operational configurations for changes to operational environments		1
	Integrated change/release management processes for development and operations		1
Continuous Deployment: from check-in to production	Solution allows this possibility with all automated testing included		5
Production incident/defect tracking & remediation	Linking operational incidents to defect reports		1
	Coordination of defect root cause analysis between development and operations		1
	Shared information on known defects, workarounds etc.		1
	Incident/defect service level and performance tracking/reporting across the lifecycle and organizations		1
Build Management	Capture file dependencies	8.33	1

Author

Michael Azoff, Principal Analyst, Software Technology Team

michael.azoff@ovum.com

Ovum Consulting

We hope that the analysis in this brief will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.