Next-Generation Enterprise Cloud Version Control

Meeting the Demands of Developers and IT Management

ASSEMBLA

Application development in the cloud is the new reality. This tidal wave of change is truly unstoppable. A recent study by OpsRamp shows that 32% of organizations already use public cloud services for development and testing, and this proportion is expected to increase dramatically by 2019.[1]

The drivers of this migration are numerous and quite compelling. For many organizations, allowing developers to focus on code only and utilize cloud services for the infrastructure aspects of the application provides speed and agility that they don't currently have in on-premises development projects. Cloud-based development efforts can also immediately leverage the latest development technologies, such as containers for portability or micro-services to more quickly build and deploy new applications. Container use is already quite strong, with Forbes reporting that 83% of the respondents to their State of the Cloud survey already use this technology.[2] These are just the starting points. Cloud services will provide the latest and most modern development tools, a stark contrast to what is available in the legacy, on-premises infrastructure. In addition, building a new generation of cloud-native applications will make IT more efficient and effective in the future.

Moving development activities to the cloud also supports an organization's digital transformation strategy. Cloud development using DevOps supports more frequent releases of updated applications, improving speed and agility, which are hallmarks of the digital organization. Using the cloud for development also enables you to produce applications that have much better scalability, helping to ensure the performance necessary to delight both employees and customers.

1. Five Trends Reveal the Emergence of Cloud-First Enterprises, OpsRamp, 2017
2. 2017 State of Cloud Adoption and Security, Forbes, April 2017

Moving Development to the Cloud Requires a Thoughtful Version Control System

As organizations start migrating development activities to the cloud, it is critical that they put in place a thoughtful, comprehensive, and workable strategy for cloud prior to any large-scale changeover. One of the sad lessons some IT organizations have learned is that a hasty move to cloud development without foresight and planning results in higher costs, security problems, silos within the organization and other issues that are difficult to remediate after the fact.

A starting point for building an effective cloud development plan is to ensure that legacy activities are not "walled off" from the cloud. Creating two siloed development environments results in higher costs, redundant work, and the inability to effectively leverage both cloud and legacy infrastructure. The reality for most mid- to large-sized organizations is that it will have a mixed environment, and it's not going away anytime soon. The strategy for cloud development must be created with inclusion in mind. An important way to ensure this integration is to bring similar tools to the cloud projects. Using common tools such as Perforce, Subversion, and Git helps maintain the consistency that is so important.

The second step of the strategic plan must be focused on security. As organizations add cloud development to the mix, new and important security issues accompany the migration. There are two primary types of vulnerabilities: The first is that using the cloud will greatly expand the number of APIs that will be used, and some may have security issues. The second issue is that cloud development will typically result in greater use of open-source components. And if you use open-source components, you need a process for managing open source vulnerabilities. That isn't because open source is less secure, but there is no "vendor" to ensure updates and patches are delivered. A more proactive and attentive approach is necessary.

Meeting the needs of both the developers and IT management is a "must have" in the plan. Focusing solely on the wants and needs of the developers is not acceptable and would result in a long-term "shadow IT" organization, creating problems for operations and security that will take years to resolve. The right strategy must meet the needs and requirements of both groups if the migration is to benefit organization.

Perhaps the most important technology that must be included in the plan is an effective version control system (VCS). Managing versions becomes exceedingly important because development in the cloud will result in many more releases being delivered to operations. Without strong controls, this could result in chaos. Also, using a consistent VCS provides a single pane of glass that works across different repository products for both legacy and cloud. This is an essential part of a solid management process. But that doesn't mean older code can't take advantage of newer security systems. If your organization incorporates code written years ago, take advantage of cloud offerings and run static code analysis or vulnerability testing.

Organizations have an opportunity to improve their security strategy by shifting security focus and spending earlier in the software development lifecycle (SDLC), as well as subjecting older code to the benefits of newer security tools.

A Checklist for Next-Generation Cloud VCS Solutions

The fundamental role of VCS solutions in cloud development requires that IT organizations choose best-in-class products that deliver all the necessary functionality. And this includes meeting the needs of both IT management and the developers. This section of the document will list the most important features you should look for in an enterprise-grade cloud VCS solution.

- Ensure security, compliance, and management without being intrusive—As organizations move toward new Agile, Lean, DevOps (ALDO) development models, especially in the cloud, it's essential that the VCS integrates security and compliance, while providing full management capabilities. The VCS is critical in ensuring that these three needs are met. It provides an important capability for secure application development by both controlling access to repositories and ensuring security functionality is included in releases. VCS also provides security for the entire software development lifecycle, an important element of overall cybersecurity. Continuous monitoring of every layer of the VCS infrastructure, from network/hardware through to the application, is also a key component of the VCS. Finally, real-time backup is required to ensure that no work is lost if there is an outage.

- A compliance-ready environment—Building from strong security functionality, the VCS must also enable the cloud repositories to meet key compliance requirements, such as HIPAA, SOC2, PCI, and GDPR. Without this native functionality, enterprises will be required to "force fit" compliance after the fact and at much higher costs.

- Support a "Crawl-Walk-Run" migration to the cloud—While it may appear attractive, a complete "lift and shift" of development activities to the cloud is not realistic. Not only is a phased migration much more likely to be successful and provide the desired benefits, but a phased approach with the right VCS solution allows developers to continue using the tools they know in a secure environment.

- The cloud VCS must work across the most commonly used repositories—There is no greater negative impact on a developer's productivity than forcing them to change the tools they are skilled at using. For this reason, the VCS solution must support the most commonly used tools, such as Git, Perforce, and Subversion. The VCS must also support integration across the repositories.

- Provide a common ground across legacy and cloud development—The reality for nearly every enterprise will be a mixed environment. The VCS must not only support this, but it must act as an effective bridge between the two. Any VCS solution that creates silos between legacy and cloud development will introduce substantial complexity and cost to the development process.

Assembla's Enterprise-Grade Cloud VCS Is an Optimal Solution

Assembla, a leader in version control systems, uniquely understands the needs and requirements for effective VCS in the mixed environments common in the enterprise. This offering delivers on the critical checklist items outlined above. There is strong support for cybersecurity within their **Enterprise Cloud Version Control** (ECVC) product that is enhanced by their strong integration with key partners, including CloudFlare, HackerOne, and others. ECVC also provides a platform that meets or exceeds key compliance standards, such as HIPAA, SOC2, PCI, and GDPR. There is also full integration with key developer tools, including Git, Perforce, Subversion, Slack, Trello, Jenkins, and Zapier. All this functionality is provided in a solution that solves the unique problems of moving development to the cloud.

Summary

The movement of some enterprise development activities to the cloud is a given. However, utilizing the cloud should solve problems, not create new ones. To ensure the move to the cloud is successful, enterprises need a comprehensive and well thought-out migration plan. Among the most important aspects of the migration is to ensure that no silos between legacy systems and cloud services are created. You also want to make sure developers can utilize common tools in both environments. Perhaps the most important enabler of this is the use of an effective VCS. Deploying a VCS that links commonly used repositories, provides a compliance-driven development framework, and increases cybersecurity is a critical step.

Assembla provides a best-in-class solution for VCS with their Enterprise Cloud Version Control offering. It meets current and future needs of the enterprise that is starting to migrate development activities to the cloud. For more information, please visit www.assembla.com.