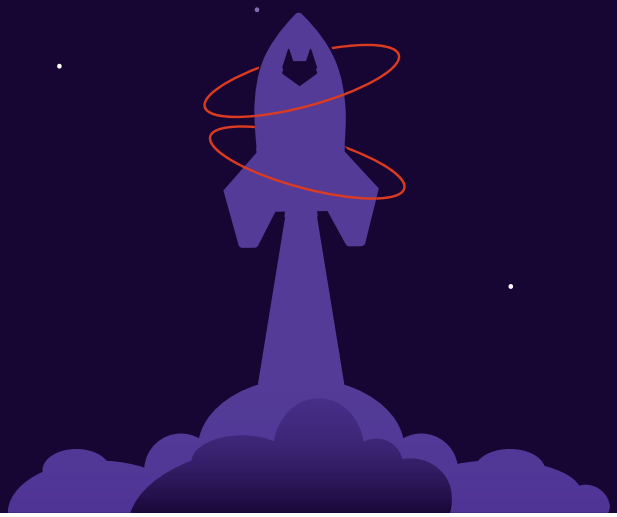
GitOps: A foundation for your cloud journey

GitLab



How GitOps helps government agencies improve security and expand their infrastructure boundaries

With the advent of the President's Executive Order on **Improving the Nation's Cybersecurity (14028)**, public sector agencies are under immense pressure to increase deployment of new technologies—without forsaking a sound security posture. The EO joins other federal cloud regulations and frameworks, including NIST EO 11 recommendations, DISA STIGS, and more, that call for a balance between accelerated development processes and strong security measures through DevOps and DevSecOps.

Unfortunately, agencies are often limited by the boundaries of their legacy infrastructures, which can stymie continuous integration and delivery, innovation, and security. The widespread adoption of cloud computing and cloud-native technologies creates additional security concerns while testing the limits of the government's outdated architectures—the same architectures that are holding infrastructure teams back, preventing them from keeping pace with their developer colleagues.

Enter GitOps

GitOps is an operational framework that takes DevOps and DevSecOps best practices used for application development (such as version control, collaboration, compliance, and continuous integration/continuous delivery (CI/CD)) and applies them to infrastructure automation.

Simply stated, GitOps uses a Git repository (or "Git repo") that contains descriptions of the desired production environment infrastructure, and pairs them with automated processes to ensure the production environment matches the desired state outlined in the repository. This translates to delivering better and more secure software, faster!

GitOps applies a developer-centric approach to operating infrastructure by using developer tools like:

1. a Git repository for version control,
2. merge requests (MRs) for collaboration, and
3. Open source CI/CD for automation.

A GitOps framework makes infrastructure automation possible, and while automation has value in itself, it's not the only advantage to GitOps. Organizations that adopt GitOps enjoy other benefits that can make a long-term impact.

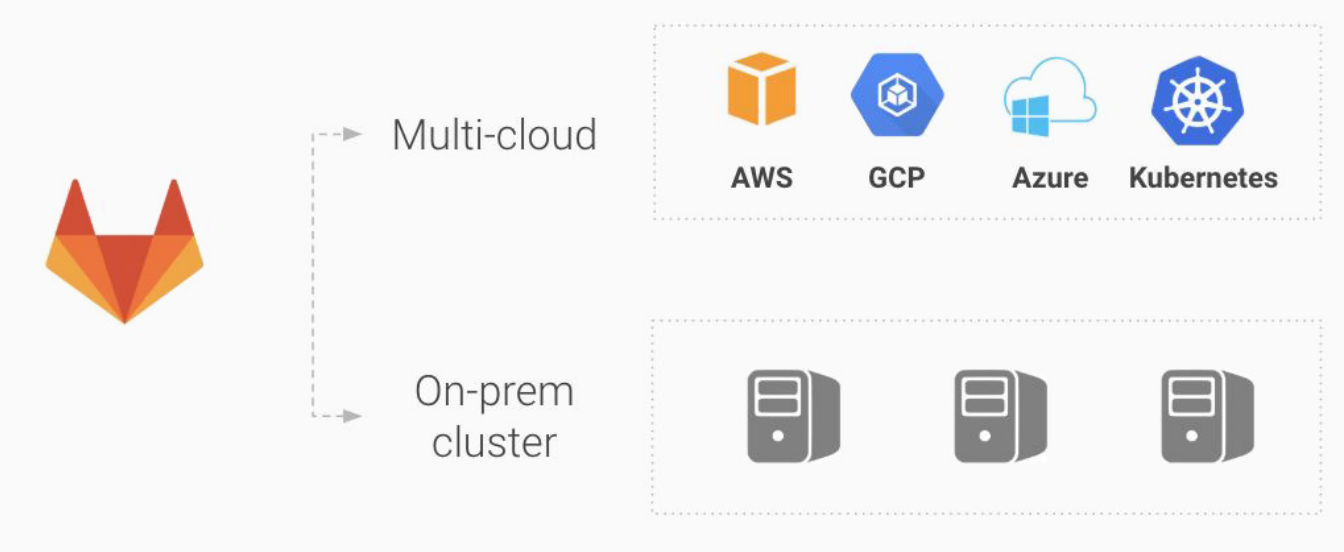
- **Reduced costs and downtime.** GitOps' automation of infrastructure definition and testing eliminates manual tasks, improves productivity, and reduces downtime due to built-in revert/rollback capability. It also allows infrastructure teams to better manage cloud resources, which can reduce overall cloud costs. This helps agencies achieve their mission objectives while optimizing efficiencies and staying within budgets.
- **Less risk.** With GitOps, all changes to infrastructure are tracked, reducing risk while supporting governance and compliance requirements.
- **Less error-prone.** GitOps contributes to risk mitigation by ensuring the infrastructure definition is codified and repeatable. This makes infrastructure management less prone to human error.
- **Improved access control.** GitOps eliminates the need to give credentials to all infrastructure components, since changes are automated (only CI/CD needs access).
- **Secure cloud-native development and deployments.** GitOps is optimized for cloud-native security through Container Scanning, Container Host Security, and Container Network Security.
- **Support for NIST EO 11 recommendations.** GitOps supports NIST EO 11 security recommendations, including those related to application scanning, fuzzing, and more.
- **Collaboration on infrastructure changes.** GitOps allows senior engineers to focus on other areas beyond critical infrastructure management, as every change goes through the same merge request/review/approval process.
- **Collaboration with compliance.** With GitOps, almost anyone can propose a change, which opens the scope of collaboration broadly while strictly limiting the number of people with the ability to approve and finalize a change.
- **Simplified auditing.** Using GitOps, all changes made to environments are stored in the Git log, making audits simple.
- **Faster time to deployment.** Execution via code is faster than manual point-and-click. Test cases are automated and repeatable, so stable environments can be delivered rapidly.
- people with the ability to finalize a change.

Achieving multi-cloud success with GitOps

The cloud has enabled new ways of designing software for immense resilience and scale. Designing an application with a cloud infrastructure in mind is known as being "cloud-native"—taking advantage of containers, microservices, service meshes, and other technologies native to cloud environments. These tools—and a cloud-native approach—can greatly aid government agencies in their search for cost savings, better security automation, greater flexibility, and continuity of service to their constituents.

That said, agencies want to choose cloud providers for their inherent value and use services that best meet their needs. A multi-cloud future gives organizations the flexibility to deploy anywhere and run workloads across multiple clouds.

> "
> Choosing a cloud provider should depend on the agency's mission objectives, it should not be constrained by technology, and GitLab wants to enable every one of our government customers to have this freedom," says Sid Silbrandij, co-founder and CEO at GitLab



GitOps helps agencies achieve this multi-cloud journey by supporting multiple cloud providers and avoiding reliance on cloud-dependent processes that create inconsistent workflows. Instead of prioritizing infrastructures or working within the confines of a certain cloud, development teams can spend more time creating applications that provide real value to their users, whether they are fellow agency employees or their constituents.

Infrastructure teams can then leverage the GitOps workflow using GitLab CI/CD to automatically deploy infrastructure code and apply it to their cloud environment of choice. Resources that were changed and updated in the agency's cloud environment and resources that are removed from the infrastructure code are automatically spun down and deleted. This enables infrastructure teams to write infrastructure code, commit it to the Git repository, and take full advantage of all the benefits of the DevOps process.
GitLab provides a complete end-to-end DevOps platform that allows government development and infrastructure teams to have the same productivity metrics and governance, regardless of which cloud they choose.

Mitigating risk through continuous threat monitoring

Government agencies are doing an increasing amount of development work within Linux containers, but containers are notoriously difficult to monitor for potential vulnerabilities and threats. It is difficult to "see" everything that is happening within the container—and whatever is happening tends to happen much quicker than in a traditional development environment. Thus, there are more opportunities for failure; a single misconfiguration could make all the data being stored within the container vulnerable.

Traditional, static approaches to security simply do not work in a containerized environment. Agencies need to take a more agile, adaptable, and continuous approach to dynamic application security testing (DAST) and monitoring.

GitOps employs a continuous monitoring approach that digs deep into the container, scanning for vulnerabilities and potential issues. Container Scanning allows developers to quickly identify and remediate security findings within their containerized developer workflows. Meanwhile, Container Host Security and Container Network Security ensure greater runtime protection. where and run workloads across multiple clouds.

Operating at cloud speed

The cloud of tomorrow is actually here today. Right now, agencies large and small can function at "cloud speed" thanks to a cohesive cloud strategy that begins with a solid GitOps workflow.

That said, GitOps is not magic; it just takes developer tools agencies already know and wraps them in a DevOps-style workflow. This allows for better revision tracking, fewer costly errors, and quick, automated infrastructure deployments that can be repeated for a multi-environment or even multi-cloud setup.

With GitOps, agencies can:

- **Eliminate or minimize manual steps** and make deployments faster, repeatable and reliable.
- **Reduce mean-time-to-repair (MTTR)** by allowing agencies to quickly roll back to an earlier stable state.
- **Improve infrastructure maintenance** through standardization and change tracking.
- **Gain better security and compliance** by enforcing access control and security checks.

GitLab: A trusted partner for government IT

Each of the "Big Five" agencies rely on GitLab, and we have partnered with the U.S. Intelligence Community for several years, working with the IC to develop specific solutions for their stringent requirements. Members of the IC are on GitLab's Customer Advisory Board, and In-Q-Tel—one of the country's leading IC-centric venture capital firms—is among GitLab's investors. These organizations understand that working with the right partner increases their odds of success by minimizing learning curves and helping to build, maintain, and run their environments.

Learn more about how your agency can benefit from a GitOps workflow. With GitOps from GitLab, you can manage and deploy to physical, virtual and cloud native infrastructures (including Kubernetes and serverless technologies) across a variety of cloud platforms.

Contact us to discover how GitOps can deliver a secure, reliable, and automated infrastructure for your organization.