Building a Secure and Efficient Foundation: Infrastructure Automation

A Unissant Accelerator

Unissant White Paper Series

Building a Secure and Efficient Foundation: Infrastructure Automation

A Unissant Accelerator

Table of Contents

Maturing the foundation through automation 2
Unissant's infrastructure automation best practices 3
- Fully vet automation template components 3
- Design for agility 3
- Integrate pervasive security 4
- Establish mature governance 5
- Leverage infrastructure automation to control costs 6

Optimizing efficiencies, enhancing end user services 7
About Unissant 8

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency."

~ Bill Gates

Federal agencies are undergoing a critical shift, transforming their IT operations from a cost center to a strategic engine for mission success. This transformation demands a robust, adaptable, and high-performing IT infrastructure—the foundation upon which innovation can flourish. While the adoption of DevSecOps practices has improved IT responsiveness, agencies recognize the need to elevate the practice of infrastructure automation.

Mature infrastructure automation serves as an enterprise enabler, empowering agencies to manage complex configurations and processes with precision and efficiency. Infrastructure automation unlocks opportunities for streamlined workflows, accelerated deployments, and optimized resource utilization.

The benefits extend far beyond efficiency. Strategic use of infrastructure automation strengthens an agency's security posture by enforcing consistent configurations and automating patching processes, minimizing human error and vulnerabilities. It supports proactive threat detection and swift response, further bolstering cyber resilience.

Ultimately, a mature approach to infrastructure automation isn't just about technology or cost savings. It's about enabling agencies to deliver exceptional citizen services. By streamlining processes and ensuring reliable infrastructure performance, automation fosters a citizen-centric experience characterized by faster response times and seamless interactions strengthening trust between agencies and the public they serve.

Maturing the foundation through automation

Unissant empowers agencies to achieve sophisticated infrastructure automation by combining advanced technology with proven best practices. Our Infrastructure Automation Accelerator fast-tracks federal agencies' path to high-performing infrastructure automation.

Our accelerator provides a tailorable set of cloud-agnostic tools optimized for cloud-native environments. Unissant experts curated a wide range of applications, identifying technology stacks optimized for automation of microservices, data ingestion, AI/ML models, enterprise applications, and DevSecOps lifecycles. Leveraging Infrastructure as Code (IaC) principles, our accelerator equips agencies with the tools to efficiently set up and manage complex environments and platforms. Additionally, it fosters zero-trust compliance using open-source products configured for scalability.

The benefits for federal agencies are numerous. Agencies can leverage a pre-vetted foundation of open-source software to build upon quickly. Provisioning infrastructure becomes faster and more secure, allowing agencies to deploy in a matter of hours instead of months. The accelerator also streamlines CI/CD pipeline adoption with well-structured libraries, ultimately supporting a more efficient Authority to Operate (ATO) process.

Designed to support federal agencies in their modernization efforts, Unissant's Infrastructure Automation Accelerator also serves as a core component of each of Unissant's accelerators. It embodies our experience and best practices for infrastructure automation within a federal ecosystem. By implementing these best practices, agencies can unlock the transformative power of mature infrastructure automation and deliver a more secure and responsive foundation for their IT operations.

Unissant's infrastructure automation best practices

Best practice: Fully vet automation template components

While IaC offers a powerful approach to automating infrastructure provisioning and management, the code is only as reliable as its underlying components. Failure to vet components—including open-source elements—can introduce significant security vulnerabilities, performance bottlenecks, and compatibility issues. This can undermine the very benefits automation seeks to achieve, leading to disruptions, delays, and increased costs.

Unissant's approach:

Unissant carefully vetted each component of our Infrastructure Automation Accelerator. We applied our integrated Vulnerability Assessment (iVA) accelerator to identify potential risks within the software supply chain. Fully vetting components—and continuously evaluating them for potential risk—allows us to introduce our accelerator to federal environments with confidence.

We architected our Infrastructure Automation Accelerator with a focus on loose integration. This allows for easier component replacement when modern technologies emerge or when an agency wants to leverage existing investments. Taking a configuration-based automation approach, we ensure more consistent and reliable infrastructure provisioning and management. This approach enables agencies to achieve their zero-trust architecture goals.

Best practice: Design for agility

While infrastructure automation offers numerous benefits, overly complex configurations can hinder agility, introduce errors, and increase security risks. Large codebases take longer to develop, test, and maintain, while intricate dependencies and logic complicate troubleshooting. Custom code elements and external dependencies produce a larger attack surface, increasing risk.

Unissant's approach:

Unissant's Infrastructure Automation Accelerator prioritizes a lightweight approach, emphasizing simplicity and minimalism. We leverage built-in features of IaC tools, promoting modularity and reusability, and minimizing dependencies. We optimize use of IaC tool features, avoiding the creation of custom scripts.

Taking a configuration-based approach, we define the desired state of the infrastructure in code using configuration files. We apply that definition across all environments for more consistent infrastructure deployments. By eliminating manual configuration and applying IaC version control, we reduce the potential for human error, increasing reliability.

When implementing a mature infrastructure automation program, we look for opportunities for reusability. We treat infrastructure code as a product itself, exploring the potential to package components and publish them for wider adoption. With a focus on building once and leveraging wherever appropriate, Unissant empowers agencies to achieve a more agile, secure, and maintainable infrastructure automation posture.

Best practice: Integrate pervasive security

While infrastructure automation offers significant efficiency gains, it also introduces a new attack surface. Security considerations must be deeply embedded within the infrastructure automation process. Pervasive security goes beyond simply applying security policies after infrastructure is deployed. Rather, it is a comprehensive approach that integrates security best practices throughout each stage of the infrastructure automation lifecycle. By defining infrastructure configurations in code, organizations can ensure consistent application of security policies across all environments and all services used.

Unissant's approach:

Unissant matures infrastructure management practices through automation, applying the complementary practices of IaC and pervasive security. We integrate security best practices throughout the infrastructure automation lifecycle, weaving security into the fabric of IaC and infrastructure automation tooling. Our Infrastructure Automation Accelerator introduces built-in security features such as Policy as Code, which allows us to define security policies alongside our infrastructure definitions, enforcing them during deployment. We enforce secure coding practices within our IaC templates; this includes using least privilege principles, minimizing resource exposure, and eliminating hardcoded credentials. Our Accelerator supports security testing to resolve code issues originating from interactions with third-party open-source libraries.

By proactively addressing security throughout automation, agencies achieve several key benefits. Applying this best practice helps minimize the attack surface, reducing the potential impact of security breaches. Automated security monitoring and response workflows enable faster detection and mitigation of incidents. Furthermore, pervasive security helps ensure that infrastructure automation adheres to relevant security regulations and compliance standards. Ultimately, pervasive security is not an afterthought. It is a core principle that strengthens the foundation of infrastructure automation, leading to a more secure and resilient IT environment.

Best practice: Establish mature governance

Like all enterprise IT functions, an infrastructure automation program requires a strong governance approach. Without clear guidelines, automation can lead to inconsistencies, security vulnerabilities, and wasted resources. Governance defines approval processes, access controls, and best practices to ensure automated infrastructure deployments are aligned with business goals, comply with regulations, and maintain a secure environment. Applying a structured approach fosters trust and avoids potential pitfalls, allowing the infrastructure automation program to deliver its full potential.

Unissant's approach:

When implementing a new infrastructure automation program or expanding upon existing agency capabilities, we focus on maturing those areas most relevant to the agency ecosystem and ways of working. We document baselines, identify gaps, and recommend discrete actions for improving approval processes, access controls, version control, compliance management, auditability, and knowledge sharing/training.

Based upon our experience, two areas stand out for assessment—approval processes and knowledge sharing/training. These governance elements are the most dependent upon human interaction, rather than automation and, as such, require close attention throughout the life of the infrastructure automation program. Approval processes and knowledge sharing/training components of an infrastructure automation program must have clearly defined responsibility matrices (RACI charts) to drive accountability. In addition, both components require regular assessment of not only compliance but also value delivered to determine whether changes should be made. Governance mechanisms should incorporate feedback loops, processes to identify gaps or shortcomings, and a methodology for applying continuous improvement such as Lean/Six Sigma.

Best practice: Leverage infrastructure automation to control costs

Federal IT organizations face constant pressure to optimize budgets and deliver efficient services. Infrastructure automation offers a powerful toolset to achieve significant cost control by automating repetitive tasks, improving efficiency, optimizing resource utilization, and reducing downtime, and speeding time to new capabilities. Infrastructure automation can scale resources up or down based on real-time needs, eliminating the risk of overprovisioning resources and paying for unused capacity. Automation tools provide better visibility into resource utilization, enabling better planning and procurement decisions. This helps avoid unnecessary hardware purchases or software licenses.

Unissant's approach:

The use of automation directly supports efforts to control costs, reducing reliance on reactive, human-driven approaches. Automation can monitor software usage patterns in real-time. This allows agencies to identify underutilized licensed resources and optimize deployments to consolidate resources or negotiate lower costs with vendors based on actual usage data.

When setting up templates, we emphasize the importance of data retention, lifecycle policies, thresholds, alerts and tagging in such a way that costs can be exposed to authorized individuals. We recommend a tagging mechanism that enables transparency into total enterprise costs, cost by service, and even cost allocation to a given organization for use of a service.

From a governance perspective, we design approval processes in such a way that cost management stays front of mind. We establish some templates as approved for general use, meaning that any authorized personnel can spin up that resource—the cost risk for that resource is low. Where licensing and utilization costs have the potential to grow exponentially, we establish an approval workflow, supported by threshold-driven indicators to prevent potentially costly errors. For example, any agency may establish a workflow that requires authorization to provision a high-performance computing environment or software with a perpetual licensing model.

Optimizing efficiencies, enhancing end user services

The adoption of mature infrastructure automation is a game-changing move for federal agencies. By employing Unissant's Infrastructure Automation Accelerator, agencies can transform their IT operations from cost centers to strategic engines of innovation. Our accelerator provides agencies with a robust, adaptable, and high-performing IT infrastructure, unlocking opportunities for streamlined workflows, accelerated deployments, optimized resource utilization, and improved security posture. The benefits of our approach extend beyond operational efficiency. Agencies recognize the importance of enhancing the delivery of citizen-centric services, characterized by faster response times and seamless interactions. Adopting our best practices can profoundly transform an agency's IT operations, delivering a more reliable, secure, efficient, and responsive foundation for mission success.

About Unissant

Mission-focused, data-driven—Unissant Inc. (Unissant) delivers for the agencies that keep our nation healthy and safe. Keeping people and mission at the forefront, we apply our domain expertise, data acumen, and technology know-how to achieve breakthrough results. Agencies turn to Unissant for our expertise in AI, advanced analytics, digital excellence, and cybersecurity solutions. Our proven frameworks drive successful execution of complex projects at enterprise scale. With an unwavering commitment to advancing mission outcomes, our teams engineer human-centered, innovative solutions that accelerate time to value. We bring honesty, integrity, and dependability to every interaction with our employees, clients, and partners.

For more information, visit us at **www.unissant.com**.