Preparing For a New Wave of Automation

Staffing and skillset shortages, ongoing demands for new applications and services, and pre-built automation tools make today an ideal time for state and local governments to more fully embrace automation as a path to meeting business and technology goals. ***Ian Brooks****, principal solutions engineer for Cloudera, discusses best practices for getting the most out of automation on premises and in the cloud.*

How has the use and adoption of automation evolved in state and local government over the past few years?

I'm definitely seeing more organizations in state and local government take advantage of automation. I primarily see it in the DevOps space—in areas that allow them to build environments where users can work and run their workspaces on, but do so in a way that makes it repeatable and a practice. As opposed to doing one-off operations, it's more of a standardized process of standing up environments for users.

What challenges keep organizations from getting the most out of their data and automation initiatives?

The main challenge is lack of experience using the tools and having hands-on knowledge of what they do, how they work and how they can best be leveraged. That's the biggest barrier to higher utilization at the state and local government level today.

What technology approaches can organizations tap into to maintain the pace of automation and innovation around data and applications?

It's twofold. You have on-prem automation, and you have in-the-cloud automation. For on-prem, it's about leveraging some of the out-of-the box automation tools. These tools are very well developed, and the federal government has been using them for years. The cloud is a great place to start your initiatives with automation as a part of them, as opposed to having an environment and then wanting to automate it after the fact. With on-prem, organizations have to look at what's going on as far as supporting legacy operations is concerned, and then in the cloud, they have to look at new types of operations.

How do complex automations increase security, privacy and compliance vulnerabilities? How can organizations mitigate risk?

As an example, consider how common the Log4j vulnerability was. If you have a similar vulnerability that's very common and gets deployed in many places in a standard approach, you've introduced a lot of vulnerabilities into your automation process. It's important organizations have a rigorous and thorough testing process when they're going to use automation tools. They should be continually validating. It's not just a one-and-done deal. They need to keep up with the changes and the new risks that are out there, and they need to validate that they're not introducing risk in a standard approach across the organization. As a practice, it's all about monitoring new risks as they come out and then having a testing and validation process to ensure those vulnerabilities are not in the automation environment.

What approaches will help technical and non-technical teams create or modify their own automations?

As mentioned, a good approach for technical teams is to take advantage of off-the-shelf tools that are designed for both on-prem and in-the-cloud automation. There's no need to invent a new wheel. For non-technical users, it's critical they understand and appreciate what these tools do and how they work. They also need to understand how to best leverage these tools. It's appreciating best practices and what automation tools can do well, but also understanding they're not a silver bullet. In addition, automation tools aren't something you can just turn a blind eye to. There has to be a constant reevaluation of what's being deployed in an automated fashion to ensure everything is working as expected and that you're not introducing vulnerabilities into the environment.

How would you advise organizations as they prepare for the future and the increasing use of automation?

Based on trends in the federal government, I expect both state and local governments to continue adopting the cloud over the next five to 10 years. As organizations consider new deployments in the cloud, it would be great to start with automation from the beginning. Instead of making it an after-the-fact approach, bake it into the solution from the start. Also, don't be afraid to try new tools, and don't be afraid to accept that you might need to get some training for your team. These are new skills, and enablement is valuable from the beginning.

Accelerating Agency Missions with Data in Motion

Government agencies are faced with a multitude of challenges, including aging legacy systems, fraud and abuse, and crippling cyberattacks. More than ever, they need a proven platform that can securely manage their citizen data. Cloudera's technology solutions address these challenges by simplifying data acquisition and delivery while providing public sector leaders with the insights they need to meet their objectives.

Cloudera partners with federal, state and local, and education institutions to support data security and governance mandates, modernize data architectures across any platform and cloud, and meet the administration's zero-trust mandate related to data flow.

With customers across 40 global governments, Cloudera can meet any data platform requirements and accelerate digital transformation to accomplish your mission.