The role discovery and CMDB play in troubleshooting and reliability

How discovery and configuration management help minimize downtime in IT systems

Benefits

- Visibility of service delivery across hybrid, multicloud IT
- Faster incident identification and resolution times
- Accurate, real-time configuration information across IT
- Comprehensive view across IT environments, endpoints, networking, and devices

All organizations aspire to 100-percent uptime across their information technology systems—and the ability to quickly resolve problems when they do occur. They want to avoid business disruptions, revenue losses, reputational impacts, and regulatory penalties.

Yet the complexity of modern IT systems and the rise of new threats, such as sophisticated cyberattacks, make this extremely challenging. The strategies organizations use as they attempt to retain control can also be a contributing factor in the difficulties of achieving operational resilience.

Siloed solutions and strategies reduce effective responses

Many organizations have complemented their core IT service management (ITSM) teams with new or expanded teams that are responsible for managing applications, infrastructure, and cybersecurity. Each of these complementary teams has then invested in dedicated tools to monitor performance and faults in its focus area.

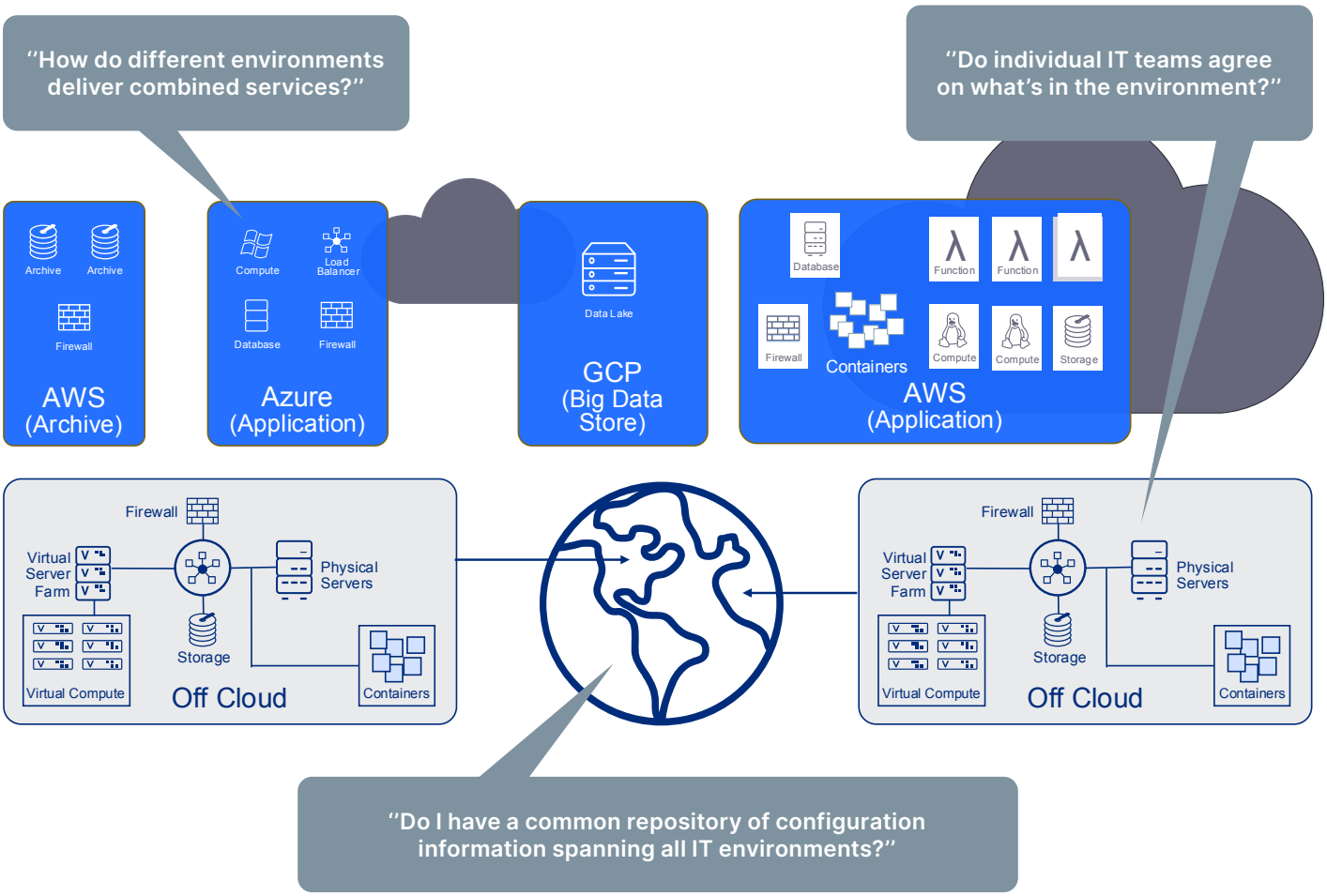
Problems arise, however, when these various solutions are not integrated or don't draw on the same information about the organization's technology environment and business processes. This can affect reliability upfront and troubleshooting after an issue occurs.

A team may not realize the key role a particular application or piece of infrastructure plays in the organization's overall operations, then inadvertently cause a disruption by making configuration or other changes. Indeed,

configuration changes are one of the most significant sources of IT system downtime. A recent survey finds that configuration and change management issues are behind 64 percent of IT and software-related failures.[1]

After an issue occurs, the lack of accurate, shared information can slow down an organization's response as teams work together to understand and resolve the problem. For example, a cybersecurity team might identify a piece of malware and request the ITSM team to make a configuration change on a server. However, the teams struggle to work together because their information about the server doesn't agree.

This inconsistency ties up resources and wastes precious time, which can quickly equate to millions of dollars of losses. In its The True Cost of Downtime 2024 report, Siemens estimates that unplanned downtime costs the world's 500 largest companies 11 percent of revenue, or a collective $1.4 trillion a year. As an example, it says that every unproductive hour costs an automotive manufacturer $2.3 million—a figure that has doubled in five years.[2]



Considerations for the role discovery plays in troubleshooting and reliability

The value of maximizing visibility and avoiding silos

The key to solving these challenges is to maximize visibility across the IT environment and to ensure that all teams responsible for keeping the organization up and running are working from a common framework and information source, rather than operating in silos.

The mechanism for achieving this is a vendor-agnostic discovery and configuration management and database (CMDB) solution. This solution should:

- **Know your infrastructure:** Identify and maintain a real-time record of all the organization's servers, networking equipment, and work-from-anywhere devices, whether they are located on premises or at one or more cloud service providers.

1 Uptime Intelligence, *Annual outages analysis 2023*, March 2023

2 Siemens, *The True Cost of Downtime 2024*, 2024

Configuration and change management issues are behind 64 percent of IT and software-related failures.[1]

- **Know your software:** Identify and maintain a real-time record of all software applications being used, from traditionally installed tools on in-house servers to harder-to-see software running in containers at third-party cloud service providers.
- **Be centralized:** Keep identification and configuration information for all these infrastructure and software elements centrally, and update that information after changes are made, even if teams use a range of different monitoring and management tools.
- **Be aware of value:** Understand how all the infrastructure and software in an organization's environment come together to support business processes. This should include understanding the relative importance of different items. For example, one server could be critical to a service, while another plays no role.

Contributions to both reliability and compliance

Such a high level of visibility is invaluable in preventing outages by understanding the impact of changes on service delivery, and troubleshooting and resolving issues when they occur.

Having a comprehensive and effective discovery and CMDB solution also makes it easier for organizations to meet their software licensing and regulatory obligations. For example, organizations are better placed to know if their systems have been correctly configured to protect personally identifiable information, as required in many nations.

The European Union Digital Operational Resilience Act (DORA) now also requires financial institutions to know who and what will be affected if incidents, changes, vulnerabilities, or outages occur in the delivery of their digital services. Captured organizations must also report on their incident management processes, including troubleshooting and recovery.

Resource

Learn more about OpenText Universal Discovery and CMDB and the role discovery can play in other areas of IT operations ›

OpenText Universal Discovery and CMDB

OpenText adheres to these principles with OpenText™ Universal Discovery and CMDB—a vendor-neutral configuration management solution, deployed as SaaS, on premises, or in the cloud. OpenText Universal Discovery and CMDB automatically collects (by discovery or seamless integrations with IT tools and platforms already in place), reconciles, manages, and presents configuration items for hardware, software, applications, services, and their interdependencies across on-premises and multicloud IT environments. The result? Your IT landscape snaps into sharp focus, empowering you to increase security and compliance.

opentext™