WHITE PAPER

Multi-instance vs. multi-tenant: Why is this important to the US Federal Government?

servicenow

The US Federal Government is in the process of transforming its information technology to embrace modern service delivery capabilities. There is great interest into using private sector innovation to improve mission capabilities and speed delivery of new service, while maintaining cybersecurity and driving down costs. There's an additional sense of urgency to rationalize software applications, consolidate government data centers, and move appropriate workload to private sector cloud service providers. And while decision-makers feel the need to modernize IT, the "rush to the cloud" is tempered by concerns over security in commercial managed infrastructure, platforms, and software.

Agency officials are wrestling with cloud-first federal initiatives that move workload into commercial clouds, while at the same time providing oversight of and protections for government data wherever it resides and comply with programs like FedRAMP, FITARA, and the Megabyte Act that ensure commercial cloud service providers protect federal data.

The first commercial cloud services emerged in the late 1990s, growing out of legacy mainframe infrastructure and inheriting a legacy multi-tenant database structure in which many customers share the same database. While this technology offered an opportunity for agencies to push workload into the cloud, there were significant issues with visibility and control for executing "inherently governmental" oversight of their data.

In multi-tenant architectures, customers share the same copy of the application code and their data utilizes a shared database. This architecture has major implications for the government customer. Should the database go offline due to corruption, failure, or a cyber incident, all customers who share that database are affected. This architectural approach requires scheduled maintenance windows and downtime, which can negatively impact agency availability and increase security risk. Since customer data shares the same database, visibility and control over individual customer data is not provided. In this type of legacy environment, a federal official must rely on an extensive service level agreement (SLA) to attempt to fulfill the inherently governmental data protection requirements.

The next evolution of commercial cloud services were born in the cloud and provide a multi-instance architectural approach. This new database structure delivers a separate database for each instance of customer software. Because there are unique databases provisioned, the visibility and control required by federal officials is provided natively. A multi-instance database structure also allows the federal customer to extend their computing boundary into the commercially provided cloud with the same—or better—security controls than on-premises deployments. Federal customers can apply security controls down to the database table level, if required.

“
The next evolution of commercial cloud services were born in the cloud and provide a multi-instance architectural approach.

Multi-instance simplifies maintenance, making delivery upgrades and issue resolution much easier because it can be done on an individual customer. This drives a high availability rate for multi-instance customers and makes it possible to perform mission critical functions with little to no down time.

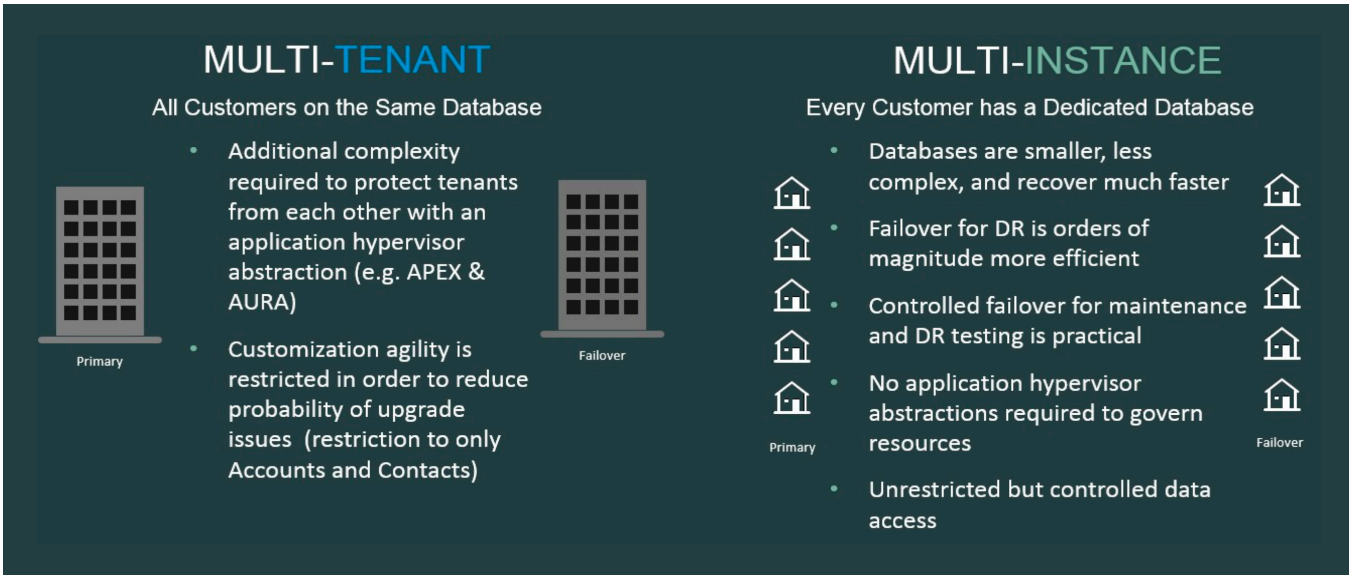

Figure 1: Modern multi-instance cloud environment versus a legacy multi-tenant architectural approach.

The advantages of the multi-instance database are simple and straightforward:

Data isolation in a multi-instance cloud:

- Physical separation of customer data from that of others with each customer using their own database and infrastructure.
- Data is more secure using isolated environments.
- Less risk of harmful attacks that can impact data compromise, system performance and reliability.

Management in the multi-instance environment:

- Greater flexibility and control of configuration, customization, updates, and upgrades.
- Updates and upgrades can be performed on individual customer instances where and when it best fits requirements and the needs of the customer.
- The ability to move customers individually with zero impact to others.

Visibility and control by the individual customer:

- The customer controls exactly when they'll upgrade to the next version of ServiceNow.
- Customer has direct access to their database and tables.
- The customer has complete flexibility and control of configuration and customization.

Today's modern, multi-instance architecture significantly reduces the government's cyber risk, improves mission availability, and reduces downtime (Figure 2). As the U.S. Federal Government continues its move toward commercial clouds, they will require that the private sector provide technologies that meet mission needs and deliver secure, 24/7 availability. Multi-instance cloud database architectures alone fulfill the inherently governmental requirement for federal officials to know where their data resides, who has access to that data, and the necessary security controls on that data.

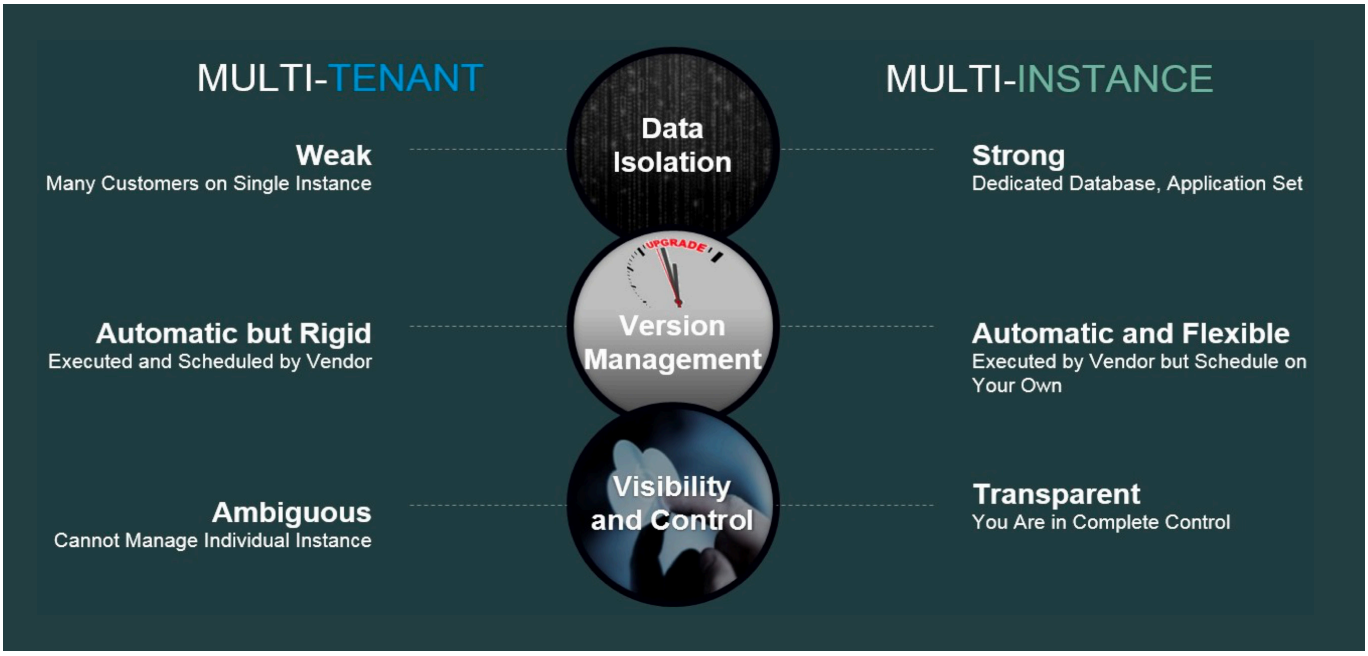

Figure 2: Multi-tenant versus multi-instance

servicenow