FEATURE

AWS Migration—Advantages, Risk and Mitigation Measures

It is no surprise that many enterprises, ranging from early start-ups to mature global enterprises, have considered or implemented a migration to Amazon Web Services' (AWS) cloud computing services.

A move to AWS can generate significant cost savings and free up time and resources that an enterprise can put to other uses. However, for a successful migration, enterprises must understand the advantages and risk factors of using AWS cloud services, and they must design and implement appropriate security controls and governance.

Advantages of Migrating to AWS

With powerful computing capabilities and an industry-leading reputation, more businesses are migrating their IT infrastructures to the cloud with AWS. Migrating to AWS provides numerous advantages, including the following:

Faster Connection and Increased Uptime
Amazon's data centers are globally placed, allowing users around the world to receive high-quality connections to their content stored on Amazon servers. These data centers also boast fast Internet connections that translate to both low latency and high bandwidth. AWS delivers input/output operations per second (IOPS) proportional to the size of the block storage, and AWS block storage demonstrates a controlled throttling that occurs at different points in time depending on block disk size. Finally, Amazon guarantees high uptime—99.95 percent of the minutes in a month, according to its service level agreement (SLA).

> "IN PRACTICAL TERMS, AWS OFFERS ENTERPRISES LIMITLESS COMPUTATIONAL POTENTIAL DUE TO THE VAST SERVER FARMS IT OPERATES."

Flexible Scaling
In practical terms, AWS offers enterprises limitless computational potential due to the vast server farms

Ray Cheung, CISA, CITP, CPA
Is a managing director and leads the high-tech group in risk consulting at Crowe Horwath LLP, one of the largest accounting, consulting and technology firms in the United States. He has more than 25 years of experience in public accounting and private industry, solving business problems by identifying control inefficiencies through implementing technology and control process improvements. Cheung has significant experience providing independent board and senior management-level consulting services in the high-tech sector and across other industries. Previously, Cheung was a managing director in risk advisory services for a national accounting firm and a Big Four firm. He was also the chief information officer for a start-up and a vice president of the technology management group at Visa International. Cheung can be reached at ray.cheung@crowehorwath.com.

Vikas Sharma, CISA
Is a manager in the IT assurance group of risk consulting at Crowe Horwath LLP. He assists with managing Service Organization Control 1 and Service Organization Control 2 attestation engagements, including supervising and directing fieldwork and reviewing reports and work papers. He works closely with senior-level management in developing recommendations for organizations' IT departments and conducting meetings on their control environment. Sharma can be reached at vikas.sharma@crowehorwath.com.

Bhupinder Singh, CISA, CISM, ITIL v3, PMP, QSA
Is a manager in risk consulting at Crowe Horwath LLP, specializing in technology risk services. He has more than 20 years of IT operations experience. Singh can be reached at bhupinder.singh@crowehorwath.com.

it operates. An enterprise can scale up as needed and spin up as many servers as necessary to provide its service.

Enterprises might experience high- and low-traffic cycles. Most often, an enterprise's service is used extensively during the day, and usage drops off dramatically in the middle of the night. AWS features load balancing, which dynamically and automatically allocates new servers to respond to cycles or sudden bursts of high traffic and to scale down after the traffic subsides, reducing expenses. When operating its own data center, an enterprise can achieve only limited downscaling, so the equipment is left unused during low-traffic periods, expending resources for little output.

Cost-Efficiency

Cloud service is generally cost-effective. Conventional wisdom might say that self-hosted solutions are less expensive, but it takes more than simply buying the hardware to run a data center. An enterprise must make both capital expenditures (for floor space, facilities, servers and extra hardware in case of breakdown and to provide high availability) and operating expenditures (for Internet access, air conditioning, electricity, additional staff, etc.).

> "ONE DISTINCT ADVANTAGE OF AWS IS ITS CERTIFIED ABILITY TO SATISFY NUMEROUS COMPLIANCE STANDARDS."

Compliance costs can also add up quickly. US-based customers in sectors such as healthcare, finance and government must meet stringent compliance standards regarding the privacy and security of data. These include the Payment Card Industry Data Security Standard (PCI DSS), system and enterprise

controls (System and Organization Controls [SOC] 1, SOC 2, SOC 3, SOC for Cybersecurity), the US Federal Risk and Authorization Management Program (FedRAMP), and the AWS government cloud (GovCloud). Similarly, an enterprise serving customers in the European Union must comply with the General Data Protection Regulation (GDPR).

An enterprise may find it less complicated and cheaper to let AWS handle its infrastructure and service needs. That said, self-hosted infrastructure is preferable in certain circumstances, such as when infrastructure is critical for an enterprise. (See the Dropbox example in the Real-World Cases section.)

AWS provides different product lines, such as Amazon Simple Storage Service (S3) and block storage with lower billing rates for higher storage quantity, which allows an enterprise to tailor its cloud infrastructure to its individual needs. These services charge a fee for every request made, however. Many other cloud vendors also are available, and the competition means costs will likely remain fairly low.

Compliance and Control Efficiencies

One distinct advantage of AWS is its certified ability to satisfy numerous compliance standards. The entire business of AWS is to provide solid infrastructure for its enterprise customers, and it

specializes in hardware and infrastructure controls. As a result, the customer list of compliance controls is complemented by AWS, as opposed to the customer managing and implementing the controls entirely in-house. However, AWS's compliance abilities do not replace the enterprise's responsibility for meeting compliance and control standards.

A mediocre self-hosted solution is unquestionably more dangerous than hosting through a reputable vendor. If an enterprise opts to maintain its own data center, additional time, resources and money are required to match the performance, uptime, risk controls, compliance abilities and more that AWS maintains to keep its infrastructure running at high performance.

The Risk of Migrating to AWS

Of course, cloud service providers are not without potential pitfalls. As with every technology solution, migrating to the cloud carries some risk. The primary issues to weigh when assessing any cloud service provider are relying on the provider for critical infrastructure needs, and exposing sensitive data to the provider's storage systems. However, using a cloud provider does not inevitably lead to significant risk. An enterprise can mitigate risk factors, and possibly even reduce its overall risk exposure, by considering these issues.

Business Continuity and Planning

The enterprise's planning must encompass the cloud service and the possibility of disaster striking in the form of a security breach, natural disaster or otherwise. It is important to also consider damaging mistakes that can occur on the enterprise's end, such as an administrator accidentally deleting a configuration or causing disruption to the infrastructure.

Enterprises must understand the AWS SLA and ensure that risk factors associated with it are mitigated. For example, if one of the AWS data centers experiences an outage that is not covered by the SLA, the enterprise will need to have arranged for duplicate servers at different data center locations that can take on extra traffic.

Vendor Reliability

Vendor reliability is another consideration when moving infrastructure to AWS. After all, the enterprise is trusting AWS with its core functions. It is important to consider that every data center (including self-hosted solutions) will go through maintenance and downtime at some point, but unplanned major outages can wreak havoc on a much larger scale. AWS suffered one such outage on 28 February 2017.[1] It lasted five hours and disrupted or halted service to major sites and services. Again, an enterprise can mitigate this risk by deploying servers across a variety of geographical locations. The outage occurred only on the US East Coast location of AWS, and negative consequences could have been prevented for customers who had chosen to run duplicate servers on US West Coast data centers.

Security breaches are a related risk of AWS migration. Although breaches of major cloud providers have been rare to date, smaller cloud providers can be and have been hit with attacks—some have even been shut down. Major providers such as AWS go through certification and compliance testing that demonstrate their competence in preventing and addressing such disasters.

> "FROM A CONSERVATIVE STANDPOINT, ALL UNENCRYPTED DATA UPLOADED TO A CLOUD PROVIDER ARE POTENTIALLY COMPROMISED."

Data Security and Threat Model

The security and privacy of data in the cloud are paramount. All interactions with the cloud are conducted over the Internet, making secured connections imperative, whether for managing data or transmitting data for everyday business operations. One of the biggest mistakes that an enterprise can make when using AWS is leaving a server or data bucket open to the Internet without any authentication.

Enterprises should evaluate their threat models. From a conservative standpoint, all unencrypted data uploaded to a cloud provider are potentially compromised. For some enterprises, such as those working with government and security, this is a deal breaker. At a minimum, data considered sensitive or valuable should be encrypted before transmission.

Three Keys to Successful Migration

Many factors contribute to successfully migrating to AWS, and they can be different for each enterprise. Enterprises migrating to AWS should pay particular attention to three issues in the process, the related risk and the measures they can take to control the risk.

> "ENTERPRISES SHOULD MAINTAIN SOME LOCAL SYSTEMS FOR A TIME AFTER THE TRANSITION TO ALLOW FOR EASY ROLLBACK IN CASE ANY ISSUES ARISE."

Cloud Structure

There is more to using AWS's infrastructure than having everything on either it or the enterprise's own data centers. Some enterprises adopt a hybrid cloud strategy, where some of their service is handled by on-site data centers and some of the work is done in the cloud. An enterprise could, for example, place data that require elasticity to increase or decrease at a moment's notice on AWS while using its own data center to keep data that require high-quality connectivity and high confidentiality. This approach provides flexibility and agility along with the ability to scale up and down according to demands.

Selecting Appropriate Applications and Data

When determining which applications to migrate to AWS, enterprises should verify and test the complete suite of products and data sets. In the process of migrating to the cloud, legacy and inflexible applications might not be compatible with the cloud infrastructure. It would be a mistake to assume that if an application is working on a physical server, it is going to work in the AWS environment.

Seamless Transition for Users

The last thing any enterprise pursuing migration wants is to lose customers due to disruption as it transitions from local data centers to AWS. Enterprises can reduce this risk by gradually off-loading service from local centers to AWS. This way, the load can be handled and errors can be fixed without too great an effect on users. In addition, enterprises should maintain some local systems for a time after the transition to allow for easy rollback in case any issues arise.

Real-World Cases

Companies across a variety of industries have tested the waters with AWS and have different reasons why they have or have not taken the plunge.

Dropbox, for example, used AWS since its founding, but in 2016 it migrated to its own data centers. As a storage company, Dropbox's business is dependent on infrastructure. At the time of the migration, it was serving 500 million users and storing 500 petabytes of data. Dropbox was an early adopter of Amazon S3, which gave it the ability to scale operations quickly and reliably, but moving storage in-house allowed it to customize the entire stack end to end and improve performance.[2] The company reports that it enjoys "substantial economic value" from operating its own infrastructure.[3]

Netflix went in an almost opposite direction, migrating computing and storage needs to AWS from its own content delivery network known as Open Connect. The Netflix case presents a strong

example of the importance of cloud structure. As Netflix spokesperson Joris Evers told *Network World*,[4] Netflix's metadata, interface and "everything you see on Netflix up until the play button" are stored and served from AWS. However, Netflix continues to use Open Connect to host its videos. High-definition video takes up massive amounts of data even after compression, and streaming videos to millions of users is impractical. Open Connect solves this by working with service providers to host videos at regional routers, avoiding bandwidth depletion.

Proceed With Caution

Companies planning a move to AWS should consider the issues involved, assessing all pros and cons. If a decision is made to migrate, the enterprise must protect its data and minimize disruption to its operations.

Endnotes

1 AWS, "Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region," *https://aws.amazon.com/message/41926/*

2 Gupta, A.; "Scaling to Exabytes and Beyond," Dropbox Tech Blog, 14 March 2016, *https://blogs.dropbox.com/tech/2016/03/magic-pocket-infrastructure*

3 Metz, C.; "The Epic Story of Dropbox's Exodus From the Amazon Cloud Empire," *Wired*, 14 March 2016, *https://www.wired.com/2016/03/epic-story-dropboxs-exodus-amazon-cloud-empire*

4 Butler, B.; "Netflix Is (Not Really) All in on Amazon's Cloud," *Network World*, 24 February 2016, *https://www.networkworld.com/article/3037428/cloud-computing/netflix-is-not-really-all-in-on-amazon-s-cloud.html*