IBM Global Business Services
White paper

January 2018

IBM Cloud Modernization and Migration with Amazon Web Services (AWS)

Part 2: Planning, migrating, and managing

Abstract

IBM's cloud enablement offerings extend to all the major cloud providers as part of its multi-cloud approach to transforming the enterprise. This is the second in a series of papers that will focus on Amazon Web Services (AWS) and IBM's collaboration that is focused on helping customers modernize and migrate applications to the cloud.

In this paper, there will be a discussion on building the virtual data center, including account structure, region, and network connectivity, and defining the processes, standards, and conventions to better manage your AWS environment. IBM will walk you through planning the overall migration for each application, looking at the resources needed and tasks to be performed. The paper will also look at tasks specific to rehosting, replatforming, and refactoring an application.

Finally, the paper touches on re-architecting an application, as well as managing and optimizing the resources around the five pillars of a well-architected framework: security, reliability, performance efficiency, cost optimization, and operational excellence.

Overview

This is the second white paper in our series on how IBM and Amazon Web Services (AWS) are working together to simplify cloud migration for our joint customers. We will pick up where the previous paper in the series left off.

In that paper, we described a quick start where we created a cloud enablement strategy, gathered information about your data center and cloud consumption, and did a proof point deploying some of your applications to AWS. We also conducted a series of assessments. These are the first steps toward making sure your company's unique business drivers are properly addressed during the migration process. We then described how we evaluate the costs and effort involved with migrating individual applications, before helping you arrive at a recommended outcome for each one: retire, retain, rehost, replatform, refactor/re-architect, or repurchase.

We briefly discussed the deliverables that are created following the assessment phase, including a blueprint for the AWS Virtual Data Center that covers topics such as account structure, security, and connectivity. We also discussed supplying a customized list of reference deployments you could use when deploying your applications to AWS.

The information provided in the previous paper was intended to help you establish the building blocks for a cloud migration plan. Now, in this paper, you will learn how to create such a plan, and then put it into action to migrate your applications to AWS. The paper will elaborate on the different types of application migration we introduced in the previous document:

- **Rehost:** Lift and shift with minimal changes
- **Replatform:** Updates to software and OS versions, and only minor changes
- **Refactor/Re-architect:** Updates to take advantage of AWS and third-party services or application built on the cloud
- **Repurchase:** Replace the existing application with a new application purchased on the cloud

Cloud Innovate is IBM's solution delivery methodology built on years of cloud experience, deep expertise, and industry best practices. Delivering a holistic approach, Cloud Innovate covers the full engagement lifecycle and integrating all aspects of solution delivery—through each stage of your cloud transformation journey.

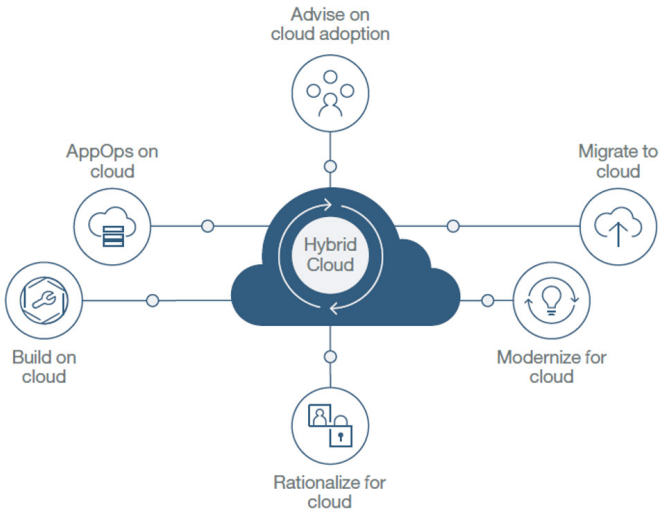

Figure 1. IBM Cloud Innovate methodology

To put this paper in context, Figure 2 provides an overview of IBM's Cloud Innovate - Migrate to AWS Cloud process. Quick Start and assessment were covered in the prior paper. One of the deliverables from the assessment phase was a blueprint for a Virtual Data Center and reference implementations. also called quick starts. This paper will start by elaborating further on these deliverables and then move into the remaining phases.

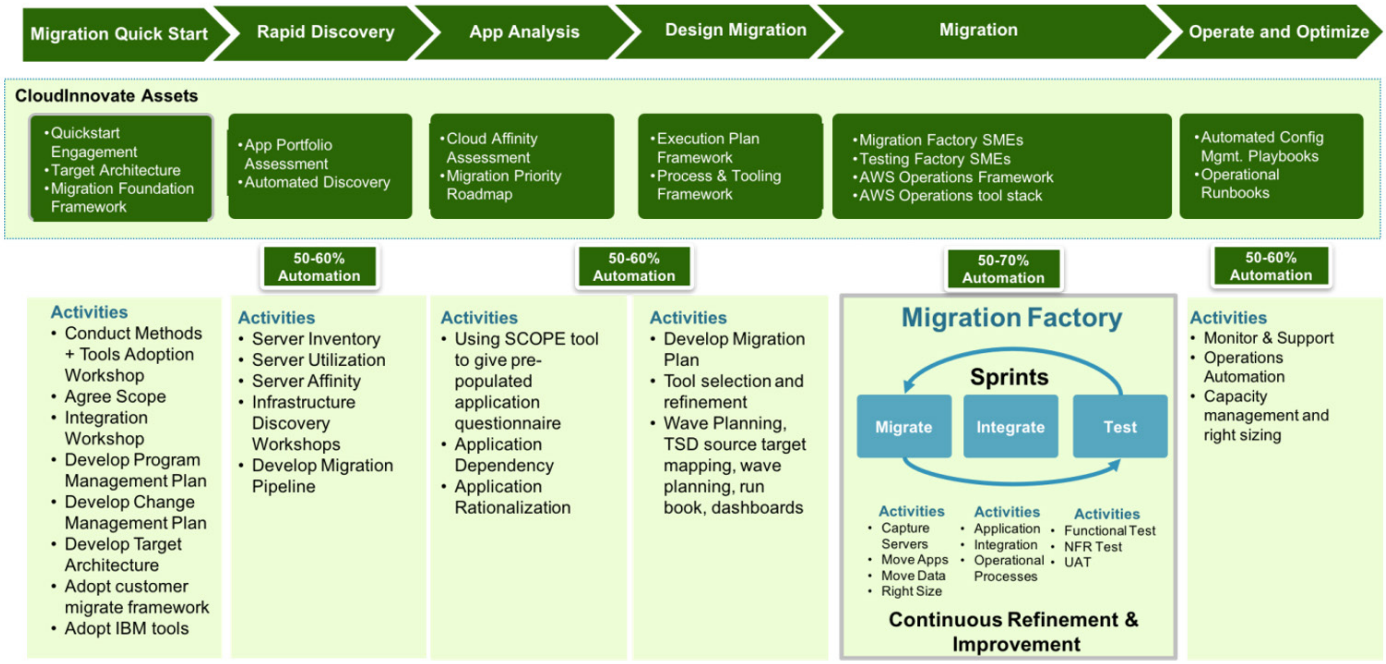

Figure 2. IBM's Cloud Innovate – Migrate to AWS Cloud approach

Blueprint for an AWS Virtual Data Center

Before going any further, let us look at some enterprise-level concerns you may have when building your virtual data center and defining an implementation architecture on AWS. AWS has five pillars of a well-architected framework—security, reliability, performance efficiency, cost optimization, and operational excellence—and a set of best practices that align to those pillars. The blueprint created for your AWS Virtual Data Center needs to adhere to these best practices.

Checklist of concepts defined in your blueprint for AWS Virtual Data Center:

- Billing and account management
- Security and access management: AWS API and console, operating system, network, data access
- Asset management: provisioned AWS resources
- Business continuity: high availability, resilience, disaster recovery, backups
- Monitoring and integration into the incident management process
- Configuration and change management
- Release and deployment management

At a high level, you will need to define your account structure; where your users and data centers are located; your network design and how you are connected to them; and your security, identity and access management policies. You will also need to establish a series of processes and procedures, standards, as well as conventions for naming resources, CIDR addresses, and more.

Accounts, users and groups

AWS allows you to have a master account and child accounts. These child accounts can be used to separate departments and billing, separate support from production deployments, or isolate deployments requiring compliance with industry regulations such as FFIEC or PCI-DSS. While these accounts have an important role, too many can become unwieldy. AWS Organizations can be used for policy-based management of multiple AWS accounts.

Users can be defined at the account level, and can be organized into groups that restrict them to specific AWS services. For example, a group can be defined that only handles user management and access to AWS services.

Network

Amazon Virtual Private Cloud (VPC) lets you provision a virtual network where you can launch AWS resources. The applications will be deployed on virtual servers (Amazon Elastic Compute Cloud, EC2) in the virtual network, along with other AWS resources.

VPN connections between AWS and your network can be made with a physical device or a software application. For solutions that require a continuous large data transfer, such as a hybrid cloud, you may need a high speed (1 gigabit or 10 gigabit) direct connection.

Figure 3 shows multiple VPN connections to a single VPC, creating redundant geographically dispersed locations.

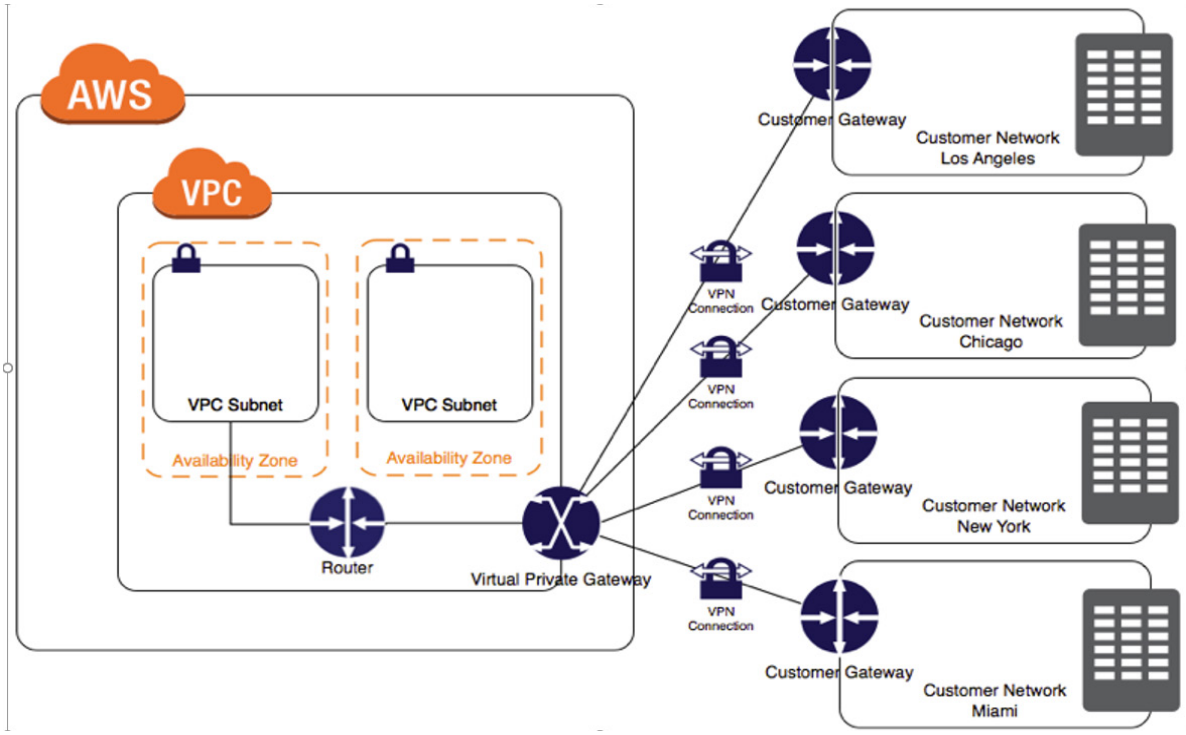

Figure 3. AWS Virtual Private Cloud

Security

Landing zone needs to be safe and secure. To ensure that policies for accessing and making changes to AWS resources need to be created. Audit logs that track who accessed AWS APIs are configured using AWS Cloud Trail. AWS resource and infrastructure changes are monitored using AWS Config. VPC flow logs for network traffic are analyzed. Amazon CloudWatch Alarms are set up to trigger when metrics are breached.

Identity and Access Management

By configuring and integrating with AWS Identity and Access Management (IAM) service, you can control who can do what in your AWS environment when and from where. AWS IAM can integrate with your existing corporate directory. You can set up identity federation and single sign-on (SSO). Fine grained policies can be configured for access management.

Planning

During the Planning phase, you will prioritize the applications you intend to migrate based on factors such as importance to the business, ease of deployment, and changes that may be ongoing. Once the applications have been prioritized, we will help you create a migration schedule that maximizes throughput. The planned implementations will start with only a few migrations, and then use continuous feedback to improve the quality and pace of the migrations. The project schedule will feature migration waves at fixed intervals, with applications cutting over to production in batches.

Each application may take a different amount of time to migrate. The duration depends on several variables, including the complexity of the application, the type of migration occurring, and any business constraints that may affect the application. This means that some applications can cut over almost immediately, while others will be part of a later batch. This concept is illustrated in Figure 4.

Incorporated into the planning should be lessons learned from the proof point. In the prior paper, we discussed a quick start where IBM migrated applications as a way of walking your team through the process. The proof point should have exposed unexpected issues and the feedback incorporated into the planning, thereby instilling confidence in the plan for all stakeholders.

Application design

IBM uses AWS reference deployments (AWS QuickStarts) and has developed a library of our own to share with customers. During the assessment phase, each application is aligned to a reference deployment as a part of the estimation process.

These reference deployments, along with the standards set in the implementation architecture, will be used by the IBM migration team when deploying the application into the virtual data center, which helps ensure consistency across the portfolio, increase quality, and reduce maintenance costs. Other artifacts created during the migration process will include AWS CloudFormation scripts (infrastructure as code), a migration checklist, and deployment and operations information for a run book. IBM recommends that these documents be maintained with a managed source control service such as AWS CodeCommit.

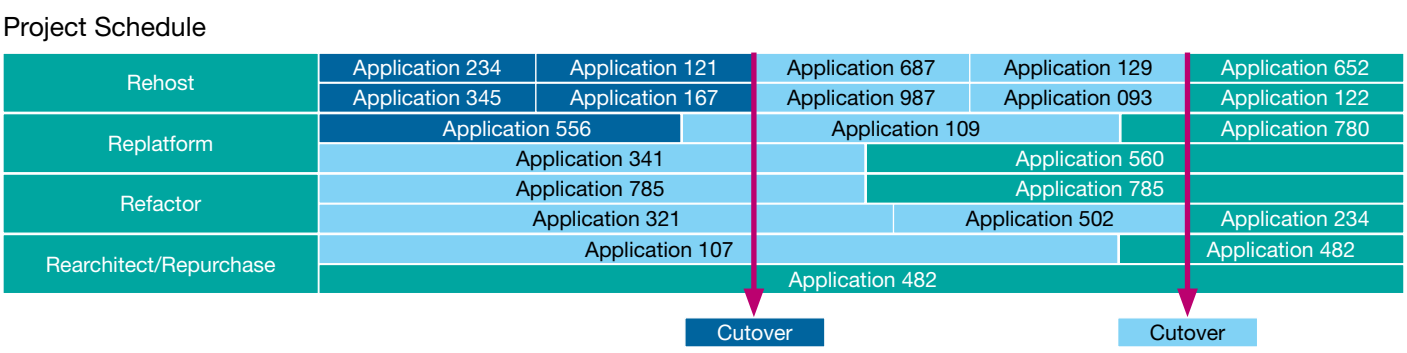

Figure 4. Application cutover is performed in regularly scheduled batches.

Application deployment

Figure 5 shows an example of a project plan for an application deployment.

Application 2357	
Develop	
Requirements	Joint
Develop Migrate Scripts	IBM
Develop Test Scripts	Client
Milestone: App 2357 Scripts Ready	
Integrated-Dev Env	
Execute Migrate Scripts	IBM
Execute Test Scripts	Client
Review	Joint
Feedback	Joint
Sign Off	Client
Milestone: App 2357 Int-Dev Done	
...	
Performance Env	
Execute Migrate Scripts	IBM
Execute Test Scripts	Client
Review	Joint
Feedback	Joint
Sign Off	Client
Milestone: App 2357 Perf Env Done	
...	
Milestone: App 2357 Production Ready	
Production	
Execute Migrate Scripts	IBM
Execute Test Scripts	Client
Review	Joint
Feedback	Joint
Sign Off	Client
Cut Over	IBM
Milestone: App 2357 Migrated	

Figure 5. Application deployment project plan

At a high level, here are the steps that will appear in the project plan. Not all steps apply to all the migration types we discussed previously.

- Start migration:
  - **Requirements:** An IBM engineer gathers the remaining application data necessary to design the solution and execute for the chosen migration type.
  - **Develop migrate scripts:** The IBM engineer iteratively designs and deploys the solution in a sandbox, including data migration. The engineer leverages a series of tools from IBM's own toolbox, as well as AWS and third-party tools.
  - **Develop test scripts:** The client team develops a test plan and a series of automated or manual test cases, collaborating with the IBM engineer.
- Support environment migration:
  - **Execute migrate scripts:** The IBM engineer deploys the application to the first support environment, which is often an integrated development environment.
  - **Execute test scripts:** The client team executes the test plan.
  - **Review:** The client team and the IBM engineer hold a joint review.
  - **Feedback:** The teams make any adjustments to the migration scripts and documentation that may be needed based on the results of the review.
  - **Signoff:** The teams jointly sign off on the migration.
  - This effort is then repeated for any additional support environments. Dev-Integration → Test → UAT Performance → Production
- Application ready to migrate:
  - **Production ready:** The application is ready to migrate to production, and will be moved at the end of the next sprint.
- Production/DR migration:
  - The process, scripts and documents used for migrating the support environments are also used for production/DR.
  - Cutover. The users are now pointed to the new production environment.

Cutover to production would use the same scripts that were used in establishing the support environments. To lower costs, the class and quantity of virtual servers (Amazon EC2 instances) may be reduced in the support environments that will not be used for performance testing. Additionally, in some cases, only a portion or representation of the data would be moved because of size or privacy issues. In these cases, the migration plan would have to extrapolate to estimate the time for setting up the environment and moving the data.

Migration types

This section of the paper will provide a closer look at different types of application migration you might choose to undertake. As the different types of migration progress from simpler to more complex, there will be overlap of the activities involved. For instance, Replatform would follow the same steps used during Rehost, with some new steps added in.

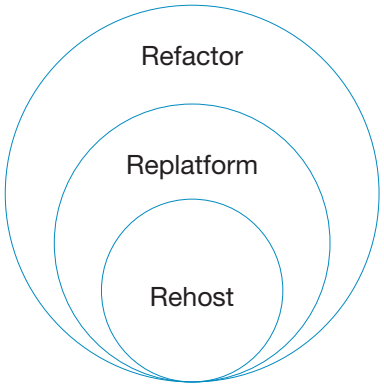

Figure 6. Overlap of activities between different migration types

On average, customers are wasting 35% of their spending on the public cloud due to an inability to adjust their use to match what they really need.[1]

Rehost

Rehosting is a lift and shift and confirmation of connectivity. No changes are made to the application, the software, or the versions. Potential cost savings from rehosting an application would come from a like-for-like comparison of compute, storage and network charges, with labor costs remaining about the same.

- IBM responsibilities:
  - Align migration with a reference deployment and reference template
  - Build AWS CloudFormation template, custom data migration scripts, and a process that includes a task list for migration. Develop documentation to be put into a runbook
  - The AWS CloudFormation template will be used to deploy the application and may include:
    - A virtual network (Virtual Private Cloud) and subnets for the application with connectivity to users, other applications, and external services
    - The target virtual servers (Amazon EC2 instance) to be used based on the source servers
    - Additional AWS resources, such as Elastic Load Balancers
    - If the application requires high availability, then the template would ensure deployment across multiple locations
    - Best practices for backups, monitoring and logging
  - The data migration strategy would depend on several factors. AWS and its partners have a series of tools that can assist you in data migration.
  - AWS offers the VM Import service specifically for rehosting migrations. Through a command line script, IBM can convert a VM into a virtual machine image (Amazon Machine Image, AMI) and then use the virtual machine image (EC2 AMI) to stand up a virtual server (EC2 instance).
- Client responsibilities:
  - Provide any needed pre-migration remediation, such as identifying and resolving hard-coded IP addresses
  - Perform acceptance testing, including failover testing for high availability applications
  - Perform any required security and compliance audits
  - Provide third-party licenses for software
- Joint responsibilities:
  - Review target infrastructure and software, capacity management, storage allocation, and other key topics
  - Review cutover plan
  - Sign off at cutover intervals and other major milestones

Replatform

Replatforming is an upgrade of the software in the technical stack, but does not require changes to the code. In terms of total cost of ownership, it is like rehosting, in that the savings would come from a like-for-like comparison of compute, storage and network charges, with labor costs remaining about the same.

- IBM responsibilities:
  - Perform custom software package installations. Third-party, COTS and application-dependent packages in the source environment would all need equivalent packages in the target environment.
- Client responsibilities:
  - Remediate any issues that prevented the application from being rehosted. This could include application dependency on the source operating system, file systems, hard-coded hostnames and IP addresses, and even compilers.
  - Because of the changes you will make, the application should be tested more thoroughly than a rehosted application would be.

Refactor/Re-architect

Refactoring takes advantage of AWS and third-party cloud services to improve efficiency and consumption of resources, thereby reducing compute, storage, network and operating costs. Depending on requirements, the application might need to be re-architected and rebuilt. Like rehosting and replatforming, the user experience after Refactoring would be like the user experience when running the application on premises.

- IBM responsibilities:
  - IBM collaborates with your team in building out the AWS CloudFormation and migration scripts, and reviews the application to determine what configuration or coding changes are needed.
  - If new application needs to be custom built or rearchitected, extracting the functional and non-functional requirements and implementing them within a new application.
- Client responsibilities:
  - Because of the changes you will make to the application, we recommend thorough end-to-end testing.

Repurchase/Replace

When an application contains required business functionality, but cannot remain on premises or be migrated to the cloud, it needs to be replaced. The replacement application can be purchased and deployed on premises or in the cloud. Alternately, the new application may be offered using a software as a service (SaaS) model.

Delivery Execution

IBM has a Global Cloud Migration Factory that executes Cloud Innovate - Migrate to the AWS Cloud framework with one method, one solution, one process, and one end-to-end toolset for the AWS Cloud modernization and migration projects. Global delivery centers with skilled practitioners, both onshore and offshore resources have been set up in the US, Argentina, Mexico, Romania, China, and India. AWS migrations follow an agile delivery execution model as shown in Figure 7.

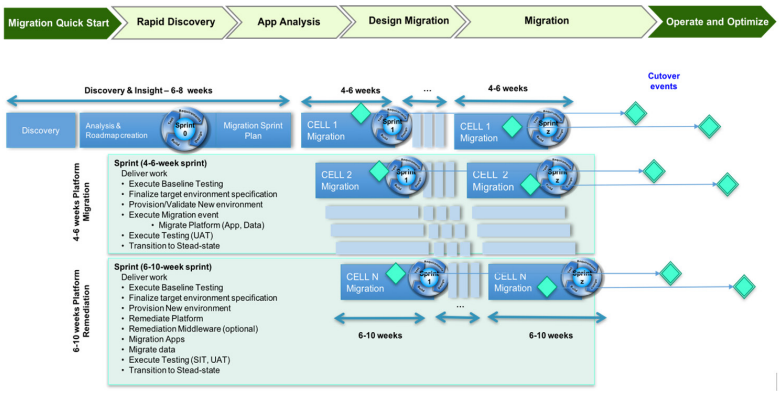

Figure 7. Cloud Innovate - Migrate to AWS Cloud execution

Manage

Moving to the cloud frees IT Operations of some, but not all, of its management concerns. IT Cloud Operations still needs to manage the virtual machine, including operating systems, middleware, databases, data security, network security, and access controls.

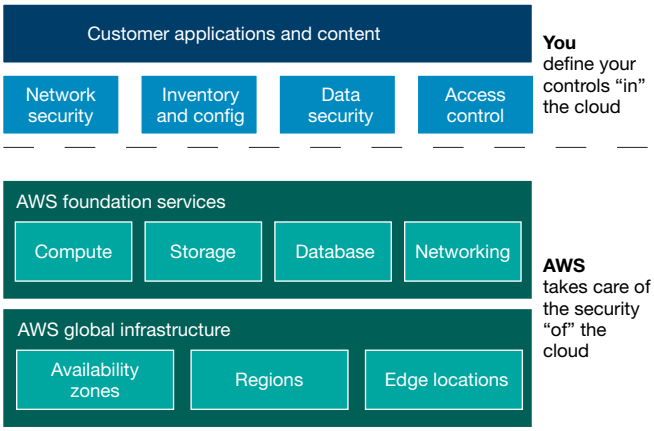

Figure 7. Cloud Innovate - Migrate to AWS Cloud execution

Managed Services

Managing your virtual data center 24/7/365 and maintaining an experienced staff trained in the latest tools around operations requires an investment for work that does not necessarily provide a competitive difference. You can look to managed service providers to perform this work while your staff focuses on building and enhancing systems in support of the business.

AWS and its partners offer managed services to clients taking on more responsibility for the infrastructure. AWS offerings include change and incident management, security and access management, continuity management with backups and restores, and OS patching. You have access to the data being used by AWS to manage your infrastructure. In addition, a cloud services delivery manager provides a monthly report that includes performance metrics and recommended optimizations.

The accountability for your systems still rests with you. This includes the consequences of downtime, and failure to meet regulatory requirements. It is important to properly vet your managed service provider to ensure they have a record of accomplishment meeting the level of service required. It is equally important that they carry liability insurance to protect you should they not meet the required level of service at a critical point in time.

Optimize

Now that you have migrated your applications to the cloud, you can start taking advantage of the tools AWS and other cloud vendors offer to optimize your applications.

As mentioned earlier, AWS has five pillars of a well-architected framework: security, reliability, performance efficiency, cost optimization, and operational excellence. As part of your migration, the applications will have been properly configured, patterned after the reference implementation architectures, standards, and conventions following AWS best practices. The applications will be leveraging monitoring (AWS CloudWatch) and logging (AWS CloudTrail) services.

The data from these services can allow you to examine resource usage, application performance, and operational health, and then optimize to align the AWS resources to the business need. The data can also be used for security reviews and audits. AWS offers premium services such as AWS Trusted Advisor, which provides real-time guidance to help you reduce cost, increase performance, and improve security.

Analytics can go beyond traditional monitoring. Data can also be captured about how users are interacting with the application. IBM Digital Analytics solutions can analyze visitor behavior trends in near real-time.

DevOps

Moving to the cloud is an opportunity to look at your DevOps maturity level across applications and for an individual application. The assessments and the move of the application by rehosting, replatforming, or refactoring should have provided sufficient data to review your overall application development lifecycle management and inefficiencies in specific applications. The next paper in the series will discuss IBM's approach to building DevOps in an enterprise.

For more information

To learn more about IBM Cloud Migration Services, visit us at ibm.com/services/consulting/migrating-to-the-cloud/ or contact your IBM representative

Glossary

AWS CloudFormation

AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS CloudFormation's templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application. You can also visualize your templates as diagrams and edit them using a drag-and-drop interface with the AWS CloudFormation Designer.
https://aws.amazon.com/cloudformation/

AWS CloudTrail

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.
https://aws.amazon.com/cloudtrail/

Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.
https://aws.amazon.com/cloudwatch/

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories.
https://aws.amazon.com/codecommit/

AWS Config

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config Rules enables you to create rules that automatically check the configuration of AWS resources recorded by AWS Config.
https://aws.amazon.com/config/

Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Think of EC2 as a virtual server.
https://aws.amazon.com/ec2/

AWS Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to route application traffic.
https://aws.amazon.com/elasticloadbalancing/

AWS QuickStart

QuickStarts are reference deployments implementing key technologies on the AWS cloud.
https://aws.amazon.com/quickstart/

AWS Trusted Advisor

An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices.
https://aws.amazon.com/premiumsupport/trustedadvisor/

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
https://aws.amazon.com/vpc/

AWS Organizations

AWS Organizations makes it easy to create policies to manage multiple AWS accounts. You can use Organizations to create groups of accounts, and then attach policies to those groups. Organizations helps you automate the creation and management of new accounts, without requiring custom scripts and manual processes.
https://aws.amazon.com/organizations/

Resources

AWS security best practices
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

AWS Operational Checklist
https://d0.awsstatic.com/whitepapers/aws-operational-checklists.pdf

AWS guidelines for accounts, users and groups
https://aws.amazon.com/blogs/security/guidelines-for-when-to-use-accounts-users-and-groups/

Amazon Virtual Private Cloud
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

AWS data migration strategy tools
https://aws.amazon.com/cloud-data-migration/

AWS Well-Architected Framework for Optimizing Applications
https://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

aws partner network

Advanced
Consulting
Partner

About the authors

Daniel (Dan) Carr

Dan is the Global AWS Practice Leader at IBM Global Business Services. He is focused on delivering cloud transformations for IBM's largest enterprise customers, where he brings extensive experience and expertise in enterprise architecture, DevOps, and cloud migrations.

KD Singh

KD is a Global Lead Partner Solution Architect with Amazon Web Services. He brings his expertise in cloud migrations, enterprise architecture, DevOps, and big data analytics to help AWS strategic partners build cloud offerings and implement digital transformations using the cloud.

Endnote

[1] *InformationWeek*, "*RightScale: Cloud Customers Overspend on Services.*" http://www.informationweek.com/cloud/infrastructure-as-a-service/ rightscale-cloud-customers-overspend-on-services /d/d-id/1327490.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2018