

How to Accelerate AWS Migrations for Financial Services

Planning & Building Compliant Architectures on AWS



In financial services, mitigating risk is front and center to keep business thriving, customers satisfied, and regulators content. Requirements change, applications evolve, and priorities shift. In this ever-evolving world, where governance, security, compliance, speed, efficiency, and innovation intersect, how can IT teams accelerate migration to the cloud while minimizing disruption to existing governance?

In this eBook, we'll outline concrete steps and real case studies for finance companies that migrated legacy applications to AWS. We'll show you how to set up a framework that makes migrating legacy applications easier from start to finish without major restructuring of your applications.

Finance on AWS

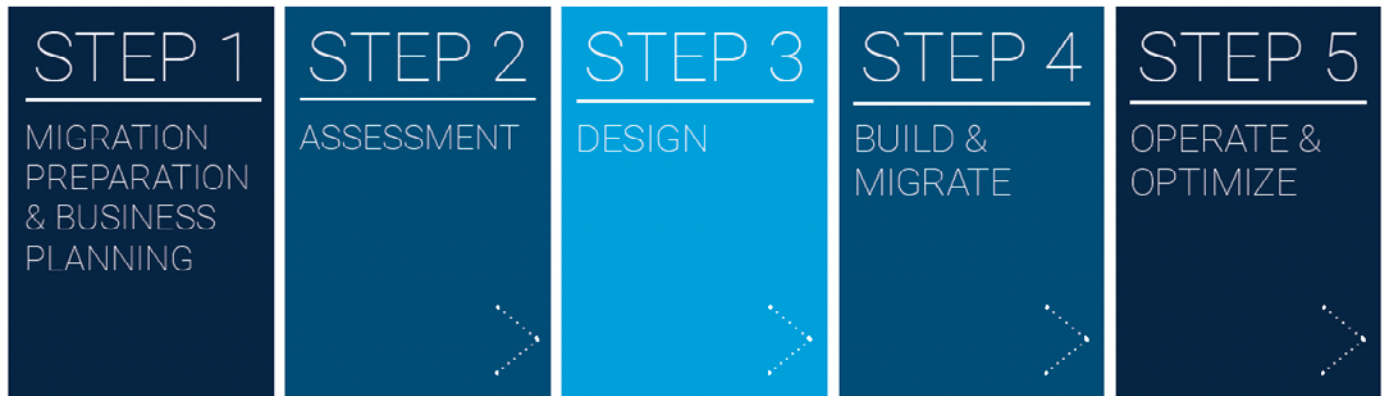
From large financial organizations to FinTech startups, most companies have made significant investments in cloud technology. In fact, [92.8%](#) of US finance executives say they are either using cloud-based solutions or plan to do so in the future. Many of them have already migrated workloads to AWS. AWS now counts Capital One, FINRA, Nasdaq, and Pacific Life among its customers. Gartner predicts that [85%](#) of companies now have a cloud-first strategy. What's the draw?

Agility and scalability are frequently cited as the top reasons for cloud migration. Long gone are the days when you build an application and run it unchanged for years, and "digital transformation", which often implies a mix of application modernization and cloud adoption, is now a mainstream concept. A cultural shift in favor of customer-obsession and pressure from nimble FinTech startups has pushed the entire finance industry to adopt cloud technologies relatively quickly, despite their risk-averse nature.

AWS has also actively courted financial institutions by strengthening security and governance controls that the industry needs. AWS has achieved nearly every compliance standard a finance organization could want, and there's reason to believe that they hold themselves to a higher standard than many corporate datacenters. Beyond basic encryption, firewall, and logging services, there are now new services like Amazon Macie, a tool that leverages machine-learning to detect anomalies, and Amazon Security Hub, a tool that gives you a high-level view of security alerts and compliance status across your AWS accounts.

The AWS Migration Process for Finance

Once a financial services company or bank decides that it wants to migrate to AWS, the normal process is as follows:



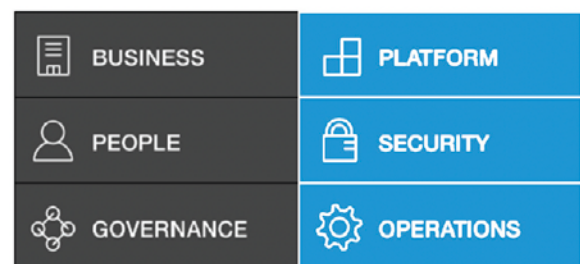
This process is more or less consistent for any application type. Let's dive into each step more deeply.

1. Discovery and Education

The first step in any migration project is to bring together key stakeholders to discuss and finalize your goals for moving to the cloud.

After helping thousands of organizations move to AWS, the AWS team created the AWS Cloud Adoption Framework (AWS CAF) to provide guidance for each unit in your organization. According to AWS, the CAF helps each business unit understand how to update skills, adapt existing processes, and introduce new processes to take maximum advantage of the services provided by cloud computing. The AWS CAF is organized into six focus areas to help organize your efforts:

AWS CAF Six Focus Areas



Source: AWS

By breaking down the process into focus areas, each business unit can better plan for the impact of cloud adoption. The AWS CAF is usually delivered in the format of a live, in-person workshop facilitated by an approved AWS CAF workshop partner like RapidScale.

The ultimate goal of the AWS Cloud Adoption Framework is to unify stakeholders and create an action plan designed to move your team from cloud goals to cloud implementation.

Sample AWS CAF Workshop Agenda

IDENTIFY & CLASSIFY CHALLENGES				
ACTION 1 IDENTIFY CHALLENGES		ACTION 2 GROUP BY STAKEHOLDER		ACTION 3 IDENTIFY THEMES
DETERMINE ACTIONS & BUILD CONSENSUS				BEGIN YOUR CLOUD JOURNEY
ACTION 4 CLASSIFY CHALLENGES	ACTION 5 CREATE ACTIONS	ACTION 6 ASSIGN PRIORITIES	ACTION 7 DETERMINE NEXT STEPS	
				ACTION 8 FINALIZE NEXT STEPS

Governance and the Shared Responsibility Model

For many finance organizations, the "Governance" portion of the Cloud Adoption Framework can be the most challenging area. Governance, Risk, and Compliance teams are unfamiliar with the responsibility model for operating on AWS and often skeptical about security controls they don't directly manage. The most important part of the Discovery and Education phase is educating compliance teams about the AWS Shared Responsibility Model.

By migrating to AWS, you have a shared security responsibility. This shared model means that AWS manages the infrastructure components from the host operating system (virtualization layer) down to the physical security of AWS' datacenters. It is your responsibility to configure and secure AWS-provided services. In other words, AWS controls physical components; you own and control everything else. As AWS states repeatedly, "AWS manages the security of the cloud; security in the cloud is the customer's responsibility."

The same line of demarcation applies to IT controls. Customers on AWS shift the management of some IT controls to AWS which results in a shared control environment. AWS manages controls associated with the physical and architectural infrastructure deployed in the AWS environment; the customer is responsible for network controls (Security Group configurations), access controls, encryption, and any control not directly managed by AWS.

In short running on AWS is very similar to running your applications in a rented datacenter. You are still responsible for common security operations tasks and for using AWS services in a secure manner.

Common Compliance Task	Insource AWS Management	Outsource AWS Management
Internal Risk Analysis (NIST, SOC2)	Customer	Customer
Internal Risk Analysis: Infrastructure Component	Customer	RapidScale
Attestation of PCI DSS, FFIEC Compliance	Customer	Customer
Attestation of PCI DSS Compliance: AWS Service Configuration Component	Customer	RapidScale
Network Design	Customer	RapidScale
Hardware Provisioning	AWS	AWS
Identity and Access Management	Customer	RapidScale
Image Hardening	Customer	RapidScale
Encryption at Rest	Customer	RapidScale
Logging	Customer	RapidScale
Change Management	Customer	RapidScale
Incident Management	Customer	RapidScale
Tier 1 Support	Customer	RapidScale

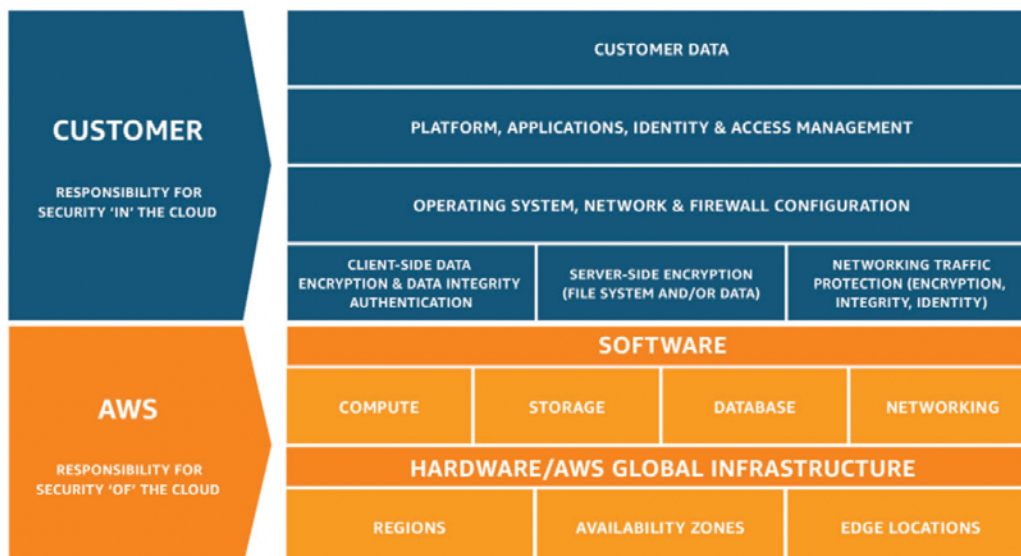
Physical Security and Environmental Controls

If you are concerned about the security of AWS' datacenters, any customer can access a copy of AWS' SOC 2 Type II report, which provides significant detail about physical security and environment controls. This report, ISO 27001, and dozens of others are available for review by audit and compliance teams if you visit AWS Artifact. If an auditor requests specifics regarding the physical controls of your system, they can reference the AWS SOC 2 Type II report. AWS does not allow datacenter tours, as independent reviews of datacenter security are also part of the SOC, ISO 27001, and other audits.

Data Privacy

AWS customers retain control and ownership of their data, and customers can move data on and off of AWS storage as required. AWS does not leverage any third-party providers to deliver services to customers and therefore does not provide any customer information or access to data to any other provider. Customers must control access to applications and data through the AWS Identity and Access Management service.

Client environments on AWS infrastructure are by default logically segregated from each other and have been designed to prevent customers from accessing instances not assigned to them. AWS has both instances that are dedicated to a single customer (Dedicated Instances) and instances hosted on shared infrastructure. AWS is responsible for patching the hypervisor and networking services, while customers patch their own guest operating systems, software, and applications.



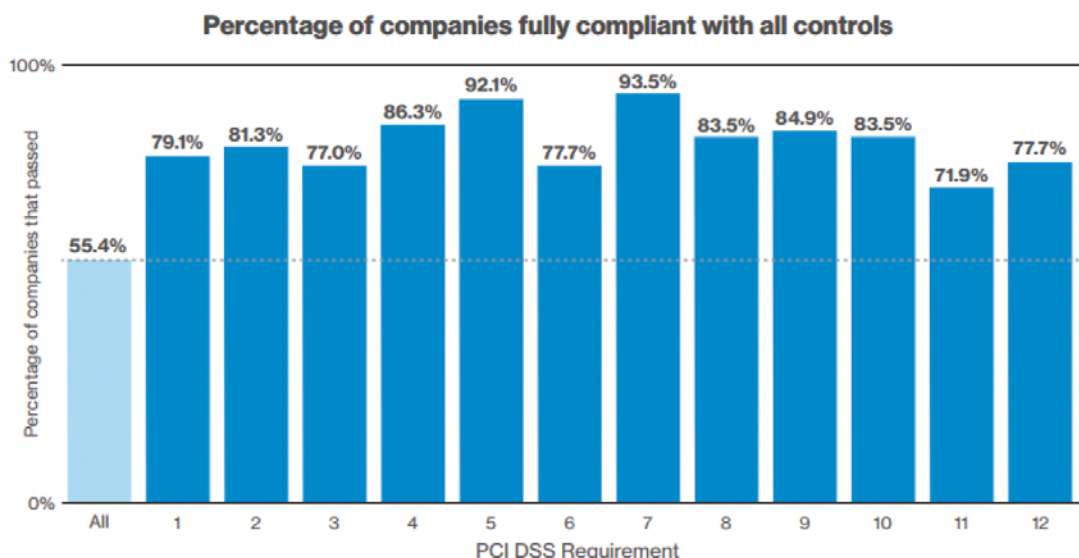
PCI Compliance on AWS

PCI-DSS is usually a baseline security requirement for most finance companies. New AWS customers often ask if AWS is compliant with PCI DSS. The answer is yes. AWS' physical datacenters are PCI DSS Level 1 Certified; however, that does not mean any application running on AWS is PCI compliant. AWS provides services that facilitate compliance, but all IT controls above the level of physical infrastructure are a customer's responsibility.

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that applies to all entities that store, process, or transmit cardholder data or sensitive authentication data. Although the standard was created to protect card payment data, PCI DSS is built on standard security principles, including topics like encryption and access controls that apply to many types of data.

Companies seeking PCI DSS compliance must manage their own compliance certification. If any system with cardholder data or sensitive authentication data is deployed on AWS, your auditor can rely on AWS' Attestation of Compliance for certain physical security controls, but only for services in scope for PCI DSS.

In 2020, only 27.9% of companies were able to maintain full PCI DSS compliance standards, and it's only getting worse.



Companies have the greatest difficulty meeting the following requirements, many of which are related to infrastructure compliance and policies:

- Requirement 3 – Protect stored cardholder data. Requirement 3 also saw the second highest use of compensating controls globally.
- Requirement 6 – Develop and maintain secure systems, covering the security of applications, and particularly change management.
- Requirement 11 – Test security systems and processes, including vulnerability scanning, penetration testing, file integrity monitoring, and intrusion detection.
- Requirement 12 – Maintain information security policies. Control 12.8 ("Manage service providers with whom cardholder data is shared") was the weakest of the Requirement 12 controls.

It is perhaps no great surprise that companies are struggling to meet PCI standards. The vast majority of companies are dramatically increasing their digital footprint at a time when 51% of compliance officers report a skills shortage in compliance.



Companies are expected to meet higher security standards across both legacy IT and cloud-based systems, at a time when IT departments are already stretched, trying to keep up with an accelerated pace of application development.

How to Accelerate the Discovery Phase

For many companies, the Discovery Phase is fairly brief. It can even take place in a single day workshop, or over the course of several weeks. The easiest way to accelerate this process is to get a Consulting Partner to educate each team prior to migration.

But a word of caution: no team should bypass the Discovery Phase. A lot of confusion and rework can be avoided if all members of your team share the same set of goals.

Assessment

When tackling a project of significant magnitude, the most challenging part is deciding where to get started. If you already have a project in mind for migration, this step is relatively simple. If your infrastructure is spread across multiple data centers or teams without a unified set of metrics for assessing applications, it can be very difficult to identify the set of applications best suited for the first wave of migration.

Selecting the right applications for migration is both art and science. A combination of the right data and expertise can help you make it through this phase.

Understand and Document Your Current Architecture

In order to identify the right applications for migration, you must have a common method for analyzing, documenting, and evaluating your current infrastructure.

This is where using an architecture assessment solution can help collect and analyze infrastructure performance, usage, and configuration from on-premises or virtualized servers. It funnels data into a single dashboard and can even make recommendations for the cost of running the application on the public cloud. Using a SaaS tool is far more efficient than asking individual data center teams to inventory application infrastructure, which can take many days or even weeks. Data collected from various teams may be in a different format, making comparisons difficult. A unified, SaaS-based assessment process helps business decision makers compare apples-to-apples in order to make the right migration decisions.

Assessment Category: Reliability		
3.1	How are services architected for high availability?	Score
Notes		
3.2	Are there any critical components of your services that are still single points of failure?	Score
Notes		
3.3	Do you monitor for any thresholds indicating availability issues?	Score
Notes		
3.4	Have you experienced any significant service downtime? If so, what was the cause of it and what improvements did you put in place to prevent it in the future?	Score
Notes		
3.5	Have there been performance bottlenecks in any area of your applications (databases, computer, user-interface)?	Score
Notes		
3.6	Are metrics available for traffic, server/app performance, etc?	Score

Example Assessment Workbook that RapidScale uses during initial assessment conversations.

Determine Which Applications to Include in the First Wave of Migration

Once you have collected data on your current systems, it is time to determine the best applications for migration.

There are many criteria to determine the "best" applications to migrate. In Step 1, you should have identified your business priorities and can decide whether you are simply looking for the applications with the greatest cost savings on public cloud or applications whose developers require greater agility.

If you haven't migrated to AWS yet, the best approach is to begin migrating the workloads with the fewest dependencies. This allows you to ramp up slowly, building expertise and confidence before tackling more complex workloads. Another approach is to start with the workloads with the most over-provisioned or idle resources. Industry research suggests that as many as 30% of on-premises servers, both physical and virtual servers, are zombies (showing no signs of useful compute activity for 6 months or more). On top of that, more than 35% of servers showed activity less than 5% of the time. As long as you rightsize your cloud deployment on AWS, these workloads will see the greatest price/performance improvements once migrated.

• • • • •

LOW-HANGING FRUIT WORKLOADS

- Fewest discrepancies
- Over-provisioned servers
- Applications on servers with full capacity

• • • • •

MORE CHALLENGING WORKLOADS

- Large, “temperamental” legacy applications
- Applications that require low-latency connectivity to local fire systems
- Purpose-built appliances like Oracle Exadata and IBM DataPower

Choose a Migration Strategy

Once you've determined your end state and which workloads you will begin with, you must decide on a migration strategy. You may have multiple different strategies depending on the workload, application, and business unit, but organizations typically pick one of the following options:

1. Lift and shift. This approach allows you to keep the application mostly as is while making any necessary adjustments to run on AWS. This is one of the fastest approaches, and there are many migration tools that can assist with the process.
2. Partial refactor. Some aspects of your applications can remain as is, but other parts may need to be rebuilt to operate properly on AWS. A partial refactor may also leave the existing application as is but build additional supporting services on top of it.
3. Full refactor. A full rebuild of your application is the most time-consuming approach, but it also represents the greatest opportunity to take advantage of the elasticity and availability of the AWS Cloud. This could also be a good opportunity to break an application down into microservices or build out a container-based architecture.

4. Transition to SaaS or PaaS. If the workload you are migrating is a commodity application (e.g., email, CRM), or has commodity components (e.g., a relational database), you can incorporate a SaaS or PaaS into the mix. This will help accelerate migration plans as well as reduce management overhead.

A lift and shift strategy is the simplest and fastest approach and is the most common method for companies migrating their first applications to AWS. However, be aware that you may not see significant cost savings on AWS. If you use this method, you may not be able to use some of the cost saving services of AWS, like horizontal scaling, managed databases, and more.

How to Accelerate the Assessment Phase

Use an AWS Consulting Partner to conduct the assessment and recommend the right cloud platform for you. Unfortunately, many companies get frozen in this step because different teams want different things.

Design

The last question to consider is tactical but complex: what will your infrastructure look like on AWS? Which instance types should you use, and in which configurations? How can you maximize your investments?

The ultimate goal of the design phase is to deliver a target reference architecture that is approved by all stakeholders identified in Step 1. This process usually involves the following steps:

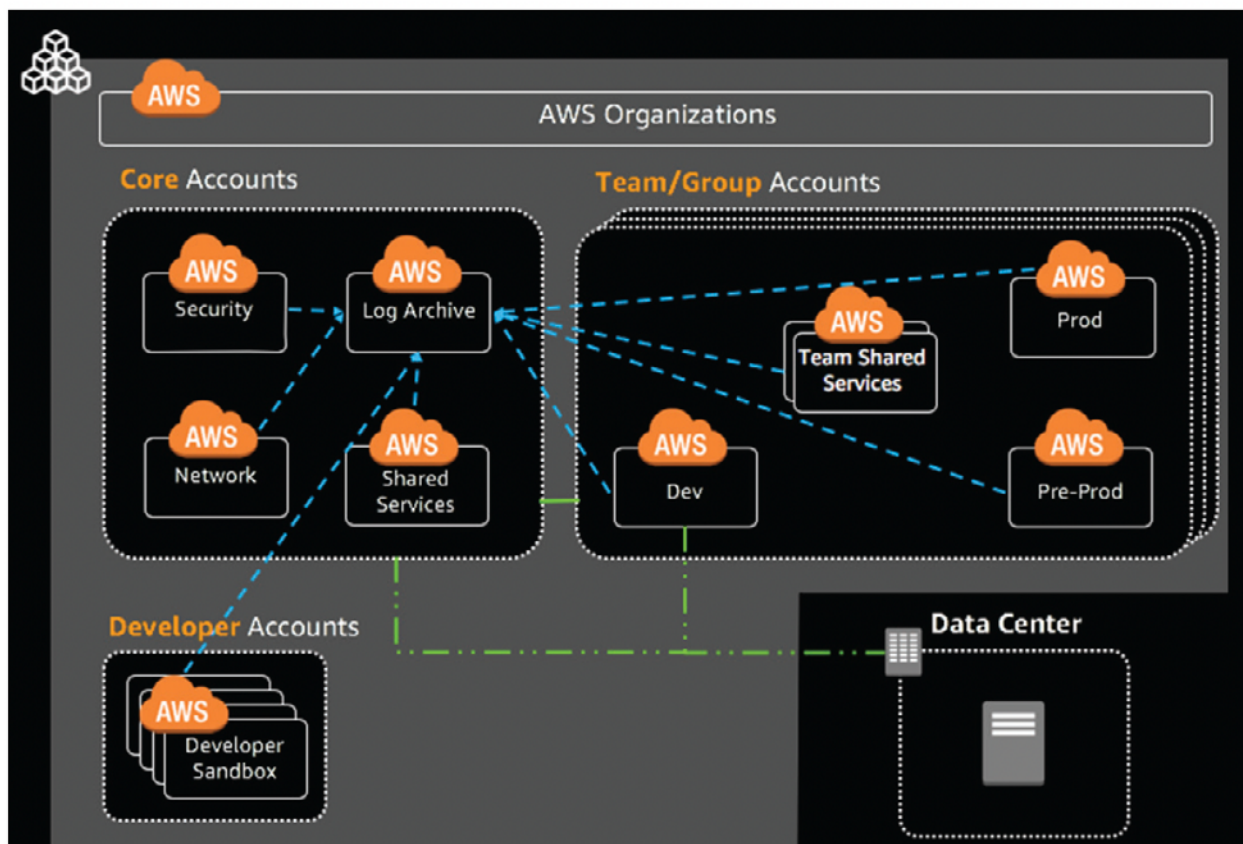
- Look at historical performance data across CPU, memory, network, and disk for servers, and across throughput, capacity, and IO for storage.
- Decide how much "headroom" you want to give each asset (typically 25%), and then look at the actual minimum, maximum, and average usage across these metrics to determine which instance type makes the most sense on AWS. A virtual machine is considered undersized when the amount of CPU demand peaks above 70% for more than 1% of any 1 hour. On the other hand, a virtual machine is considered oversized when the amount of CPU demand is below 30% for more than 1% of the time during a 7-day period. Looking at 30 days of history is sufficient because it is easy to scale up resources on the cloud if needed. When going through this process, it's critical to normalize for different generations of physical infrastructure.
- Design a strawman AWS architecture, both in the form of an architecture diagram and a list of proposed services including EC2 instances, EBS volumes, VPCs, etc. and associated costs.
- Share with key stakeholders identified in Step 1. If you involve security and compliance teams in the design stage, you will be much more likely to meet your project deadlines than if you involve them after the infrastructure is built out.

AWS Control Tower & Multi-Account Architectures

If you're migrating a large number of teams and applications to AWS, then you may not want to put everything into a single AWS account. For many companies, it is more efficient to create multiple AWS accounts for different departments, teams, or projects rather than a single large AWS account. Doing so makes it easier to separate critical data from sandbox environments, and helps limit the blast radius from a critical security event.

[AWS Control Tower](#) is a perfect solution to automate the process of setting up and configuring multiple accounts. Best practices for setting up multiple accounts are embedded in the solution, making AWS Control Tower a great idea for companies with complex workloads and larger teams that want to quickly migrate to AWS.

Control Tower is deeply tied into AWS Organizations, a service that allows you to enroll any number of "child" accounts under a parent account and apply policies across all accounts from a single location. This extends similar functions originally used for Consolidated Billing and provides additional capabilities like AWS CloudFormation "stacksets".



Source: AWS

Control Tower starts with a well-architected AWS Organizations implementation and adds centralized logging, a cross-account permissions structure, and an automated "Account Vending Machine" process to enroll new child accounts at will.

In order to get access to the AWS Control Tower toolset, you'll need to work with AWS Professional Services or an approved AWS partner like RapidScale. [RapidScale](#) evaluated Control Tower in tandem with AWS and other early adopters during the Preview period and now can offer it directly to our customers.

How to Accelerate the Design + Build Phase

Check out [AWS Quick Starts](#), which are infrastructure-as-code templates designed for specific use cases. With just a few clicks, you can launch infrastructure that AWS has vetted and audited for different compliance frameworks. Here are a few you might be interested in:

- [PCI-DSS compliant AWS architecture](#)
- [Standard VPC](#) with up to four Availability Zones
- [CIS Benchmark on AWS](#)
- [Standard cloud environment for NIST-based assurance frameworks](#)

If you're starting at square one and don't know how to implement a CloudFormation template, contact a cloud partner.

Build & Migrate

The next step is purely technical: your team must build the approved AWS architecture and migrate applications and data to the target architecture.

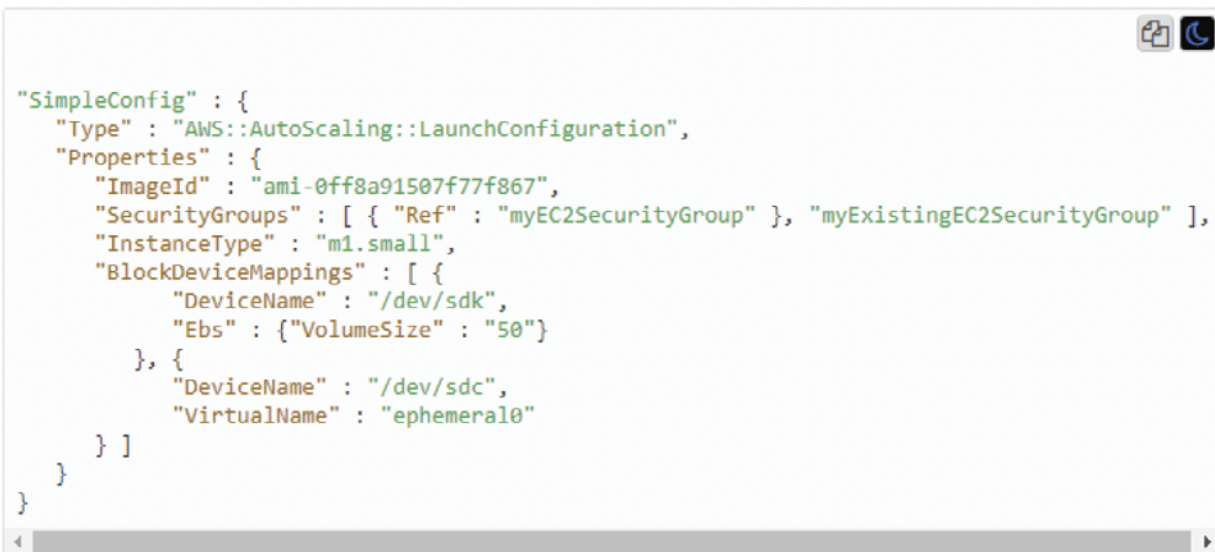
Build Target AWS Architecture

Ideally, the process follows this pattern:

1. Cloud engineers build the approved architecture in an infrastructure-as-code tool of choice (Terraform, AWS CloudFormation, an architecture templating tool that allows you to "build" once and spin out future environments instantly)
2. An AWS provided machine image (AMI) is used and further configured for each application using an automated configuration management tool like Puppet, Chef or AWS Systems Manager
3. Together, the templates and images are kept in a code repository (Git) and versioned and updated like a piece of software
4. Servers, databases, and data are migrated to AWS, either over the internet (which takes quite a bit of time), or through the AWS Migration Service, like those listed below
5. Other teams test and validate application performance, security, compliance, etc.

Many teams make the mistake of building AWS resources manually using the CLI or console. While this may be a quick, short-term solution, it makes the build-out of future test/dev environments complicated and causes long-term management issues, highlighted below.

When you automate infrastructure build-out from Day 1, you enable your team to build consistent, documented, easily-updated AWS environments. It is well worth your time to learn Terraform or AWS CloudFormation.



```
"SimpleConfig" : {
  "Type" : "AWS::AutoScaling::LaunchConfiguration",
  "Properties" : {
    "ImageId" : "ami-0ff8a91507f77f867",
    "SecurityGroups" : [ { "Ref" : "myEC2SecurityGroup" }, "myExistingEC2SecurityGroup" ],
    "InstanceType" : "m1.small",
    "BlockDeviceMappings" : [ {
      "DeviceName" : "/dev/sdk",
      "Ebs" : { "VolumeSize" : "50" }
    }, {
      "DeviceName" : "/dev/sdc",
      "VirtualName" : "ephemeral0"
    } ]
  }
}
```

Sample AWS CloudFormation script that sets up an Auto Scaling Group.

Configuration Management

The fundamental purpose of configuration management is to deploy environments prescriptively. By defining everything on the servers in a single location, there is a single source of truth about the state of the entire infrastructure. The value of configuration management is that when you want to change the OS, you can change the code on the servers without making major changes to the servers themselves. Configuration management is also used to install various security features on an instance, like Identity Detection System agents, log shipping, monitoring software, as well as requiring MFA and binding the instance to central authentication. Changes can be rolled out to many instances at once — and be rolled back. When you are done, each server is in a known, ideal state. When you build and maintain your environment manually, change is slow, cannot be rolled back, and has a higher risk of human error.

With AWS, there are many possible tools to control configurations. You can choose to use an AWS native tool like OpsWorks, which uses Chef. You can deploy your own server with Puppet, Chef, or another CM tool of your choice. Obviously, the latter provides greater control but requires that you provision and maintain your own Puppet/Chef server. You can also manage services in a more restricted (but more fully-managed) way through Amazon EC2 Systems Manager. This is essentially a collection of a la carte services to create system images, apply OS patches, track system configurations, etc.

Migrate Data

After you build your target environment, it is time to move your applications and data. AWS has nearly a dozen services to help you migrate to AWS. Here are just a few examples:

AWS Database Migration Service (DMS) helps you migrate databases to AWS easily and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The AWS Database Migration Service can migrate your data to and from most widely used commercial and open-source databases.

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for you to migrate thousands of on-premises workloads to AWS. AWS SMS allows you to automate, schedule, and track incremental replications of live server volumes, making it easier for you to coordinate large-scale server migrations.

AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. Using Snowball addresses common challenges with large-scale data transfers, including high network costs, long transfer times, and security concerns.

AWS VPN is the simplest and most popular option. You're limited by the speed of your internet connection, so most companies only use VPN for small amounts of data. If your application needs a high performing, persistent connection to your on-premises systems, you should invest in **AWS Direct Connect**.

How to Accelerate the Build & Migrate Process

During the migration process, there is a period of time where both your current and your AWS infrastructure will be up and running. This usually results in higher costs. You should anticipate and budget for this period. The planning done in Steps 1–3 will help minimize the length and impact of this "double" infrastructure period.

That said, this process can last for months or years. At RapidScale, we've seen a company's lack of internal organization translate into migration projects that never get off the ground. If your migration process is stalled, it could be that you're trying to accomplish too much at once. Go back to the drawing board and launch a POC for your most basic application. Or think about launching a multi-account architecture – where each team or project has a different account and teams' competing priorities won't prevent others from moving forward.

Operate & Optimize

While many of the key elements of a cost efficient migration are determined during the migration process, the key to long-term success on AWS is ongoing optimization.

By necessity, you will have some inefficiencies during the migration stage. As environments are tested and instances are changed to meet the demands of the application, there will be unexpected costs. After migration, you will have time to examine those inefficiencies and continually improve your infrastructure.

24X7 Ticket Support

During the Business Planning phase, you should have identified the key teams that will manage the AWS environment(s) on an ongoing basis. If you are managing internally, use the time after migration and before go-live to determine SLAs, establish roles and responsibilities, and prepare procedures for common tasks, such as instance rebooting, access management, etc. Relying on an external Managed Service Provider, like [RapidScale](#) can help reduce the burden of around-the-clock management on internal teams.

Cost Tracking and Analysis

One of the greatest benefits of using AWS cloud is that you can get real-time billing information and notifications of unusual or unexpected spending. In order to filter that information and turn data points into actionable information, use a cost analysis and cloud governance platform. Your cost tracking and analysis dashboard should be your "single pane of glass" over both on-premises and cloud-based environments. Ideally, it should also be as accessible by your cloud engineering team, who should be held accountable for maintaining their project budgets. Your team should schedule regular internal reviews related to the cost of the environment. AWS is continually adding new products and services, and these can impact the cost of an environment without the proper guardrails in place. For example, a new instance type that better fits your application may mean you can downsize and save.

Well-Architected Reviews

AWS recommends that every team conduct a Well-Architected Framework review every six months. The Well-Architected Framework is a structured approach for evaluating cloud environments based on these five pillars:

- Security
- Reliability
- Performance efficiency
- Cost optimization
- Operational excellence

Regular, formal assessments allow you to have a consistent approach for continuous improvement of your infrastructure and a common standard of excellence across all teams and AWS accounts. Whether you perform these internally or with the help of an approved Well-Architected Framework Review Partner, like [RapidScale](#), these reviews will help lower the ongoing risk of operations, improve cost-efficiency, and expose areas of potential weakness in your architecture.

While a formal review takes place every six months, your team should be constantly measuring your environment against the best practices outlined in the Well-Architected Framework. A SaaS-based governance solution can provide the data and recommendations to keep your team in line with best practices all year long.

Conclusion

Finance companies are increasingly migrating applications to AWS and want to be confident that security and compliance needs are addressed during the process. Compared to non-regulated workloads, regulated workloads will take longer to migrate, mostly due to the extra time required in the Assessment and Design phases. But you can still accelerate migration with the tips described in this eBook.

If you're ready to take the next steps in planning your migration, find out how RapidScale can help simplify the process of migrating assets from your data center to the AWS cloud. RapidScale's Migration Services enable you to efficiently assess and model workloads for migration. Then you can manage and optimize your infrastructure for cost, usage, performance, and security once they are running on the cloud. This helps reduce complexity and allows you to move faster in your migration process. Learn more about how RapidScale can help you plan, build, and manage your cloud environment by visiting rapidscale.net.

About RapidScale

RapidScale, the leader in compliant cloud solutions, provides end-to-end cloud strategy, RapidScale helps customers migrate, run, and operate mission-critical workloads on AWS with security, scalability, and efficiency baked in. RapidScale's Cloud Reliability Platform combines world-class engineering talent, policy-as-code, and integrated tooling to enable customers to confidently meet compliance regulations, security requirements, cost control, and high availability. Together with our team of dedicated certified engineers and decades of IT management experience, we ensure our customers' success across every stage of the Cloud Adoption Framework and governance.



- Solution Provider
- Managed Services Provider
- SaaS Services Competency
- DevOps Services Competency
- Security Services Competency
- L1 MSSP Services Competency
- Migration Services Competency
- Healthcare Services Competency
- Small & Medium Business Services Competency

SIMPLIFY IT. UNLEASH INNOVATION.

www.rapidscale.net ©RapidScale