



# HANDS-ON MULTI-CLOUD FOR DEVELOPERS

# Developers on the Cloud



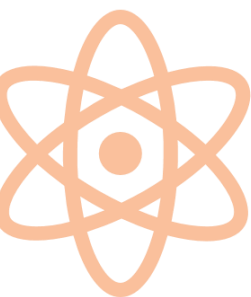
Source: Tomwang112/Dreamstime.com



# Multi-Cloud









## What is Multi-Cloud

- Less or no vendor lock-in
- Greater Reliability with multi cloud
- Location based cloud provision
- More Secure
- Performance
- Fault tolerance
- Cost efficiency



# Learning Objectives

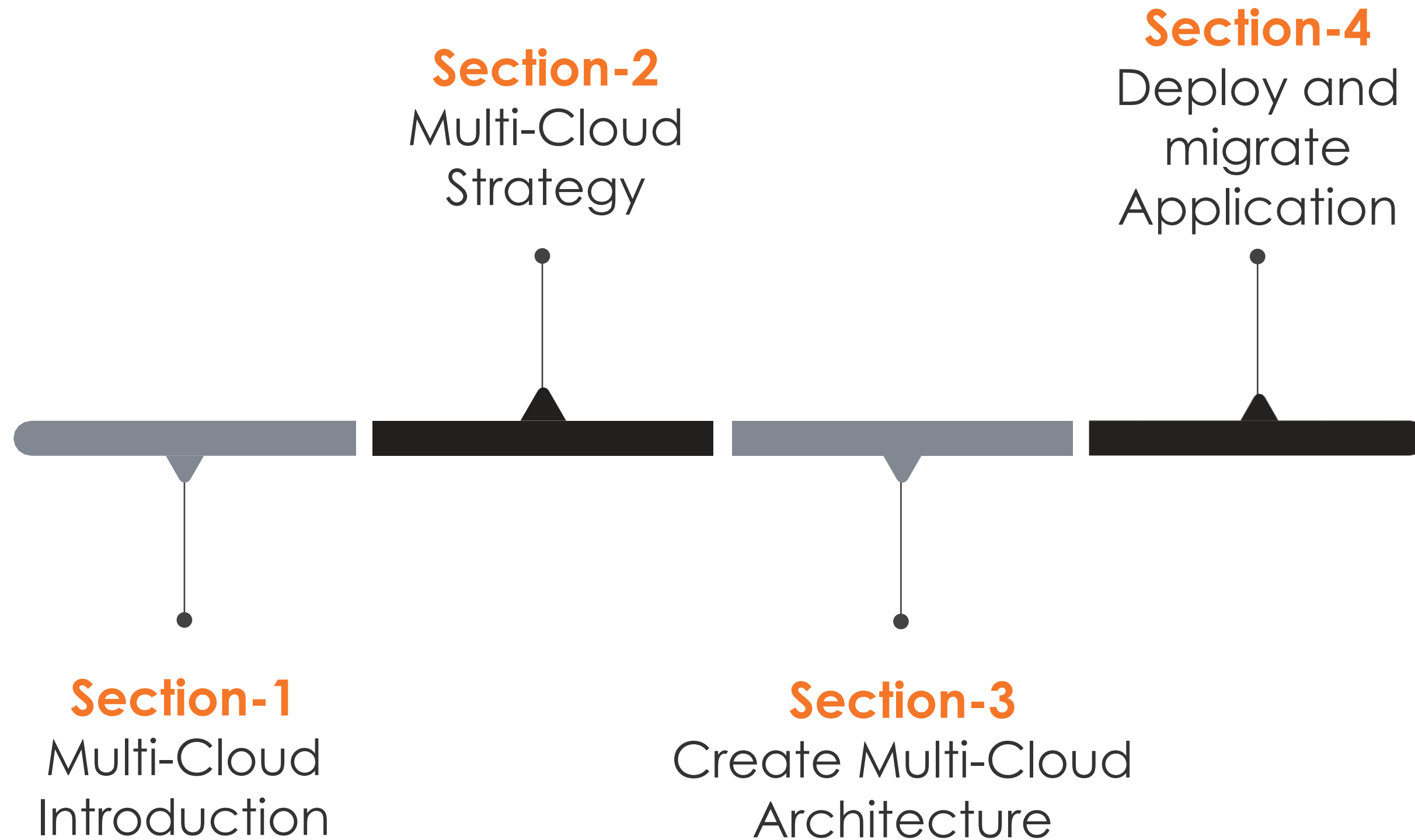
# In this session you will learn to

-  Develop cloud-native applications on the multi-cloud platform.
-  Practice and acquire an in-depth understanding and knowledge of multi-cloud platforms.
-  Extensive source code examples along with screenshots for Multi application development.
-  Deploy and migrate application in multi-cloud environment
-  Manage and troubleshoot Multi-Cloud application issues.
-  Understand the industry cloud-native application best practices.
-  Application security controls for the multi-cloud environment.
-  Real world examples to help to choose right cloud



# DAY 1

# Day-1



Section 1



# Introduction to Multi-Cloud for Developers

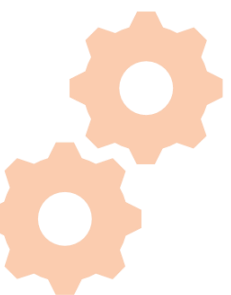


50 Min



# Goals

- ✓ Getting started with Multi-cloud
- ✓ *Myth: Multi-Cloud=Hybrid Cloud => all Hybrid clouds are Multi-cloud, but not all multi-clouds are hybrids*
- ✓ Create Cloud Trial Accounts
- ✓ Review the Application code from GitHub



# CLOUD AND HYBRID VS. MULTI-CLOUD

## CLOUD



Basic cloud use, using SaaS application, Public Cloud for test-dev or a specific use case.

## HYBRID-CLOUD



Run the same application seamlessly on premises and in a public cloud

## MULTI-CLOUD



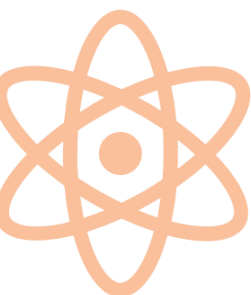
Ability to use the most appropriate cloud, whether on-premises or public, for each application



# Multi-Cloud vs. Hybrid Cloud

## What is the difference

- Hybrid Cloud is the combination of Private and Public Cloud
- Multi Cloud comprise of more than one Public Cloud
- The hybrid clouds are Multi-cloud, but not all Multi-clouds are Hybrid Cloud
- In Hybrid cloud, we use application services from a Public cloud and keep the database and storage private cloud.
- In Multi Cloud, the compute services(EC2) in AWS and use database services from Azure while storage from GCP.



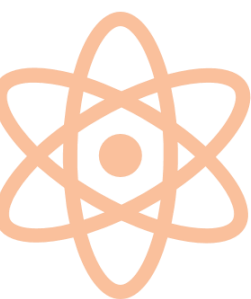


# Difference Between

Google vs. AWS vs. Azure



Source: <https://www.janbasktraining.com/blog/wp-content/uploads/2018/10/Difference-Between-Google-Cloud-vs.jpg>



# Compare key services among cloud vendors

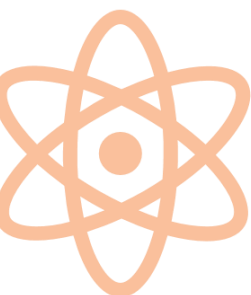
AWS	Azure	GCP
Amazon EC2	Azure Virtual Machine	Compute Engine
Amazon RDS	Azure SQL Database	Cloud SQL
Amazon Simple Storage Service (S3)	Azure Blob Storage	Cloud Storage
Amazon VPC	Azure VNet	Cloud Virtual Network
AWS Lambda	Azure Functions	Cloud Functions
Amazon VPN	Azure VPN Gateway	Cloud VPN
Amazon CloudFront	Azure CDN	Cloud CDN
Amazon Route 53	Azure DNS	Cloud DNS
AWS Direct Connect	Azure Express Route	Cloud InterConnect
Elastic Load Balancing	Azure Load Balancer	Cloud Load Balancing
AWS CloudFormation	Azure Resource Manager	Cloud Deployment Manager
Amazon CloudWatch	Azure Monitor	Google StackDriver
AWS Command Line Interface	Azure Command Line Interface	Cloud Shell
Amazon DynamoDB	Azure CosmosDB	Cloud Datastore
Amazon Redshift	Azure SQL Data Warehouse	Big Query

# Lab Activity

# AWS Account

Steps to register for free AWS trial account

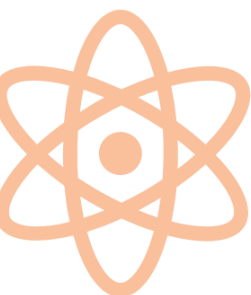
- Go to <https://aws.amazon.com/free/activate-your-free-tier-account/>
- 12 months of access to free products and services with AWS Basic Support features, including 24x7x365 customer service.
- Your credit card will not be charged unless your usage exceeds the free usage tier.
- Further details  
<https://aws.amazon.com/free/?awsf.Free%20Tier%20Types=categories%2312monthsfree&awsm.page=1>



# Azure Account

Steps to register for free Azure trial account

- Go to <https://azure.microsoft.com/en-us/offers/ms-azr-0044p/>
- \$200 in Azure credits to be used within the first 30 days of sign-up and 12 months of select free services.
- Your credit card will initially NOT be charged, except for a temporary authorization hold.
- Further details <https://azure.microsoft.com/en-us/free/free-account-faq/>

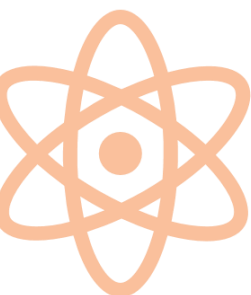




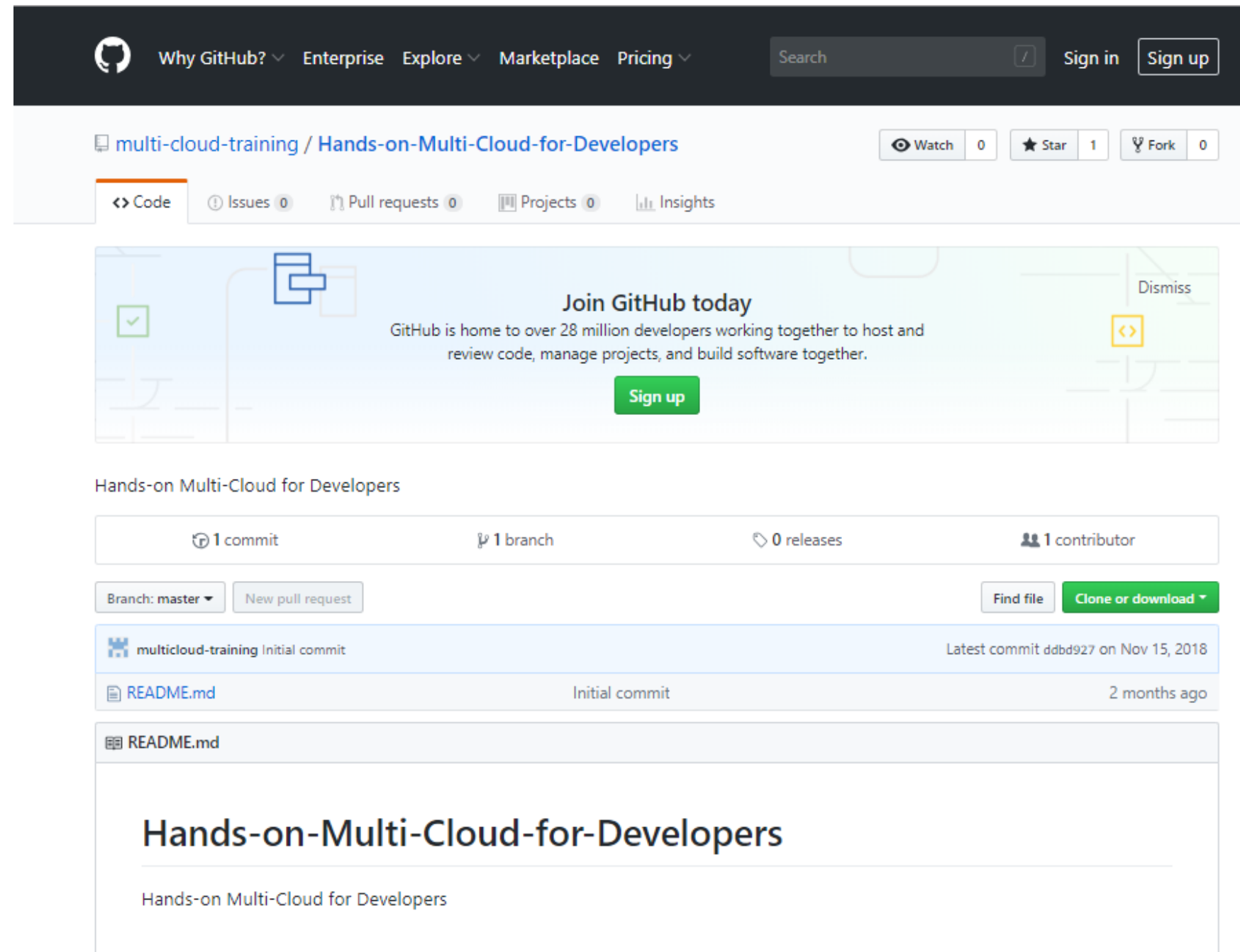
# GCP Account

Steps to register for free GCP trial account

- Go to <https://cloud.google.com/free/>
- 12 Months and offers \$300 free credit to get started with any GCP product.
- Also has some always Free products to keep you going.
- Google asks for your credit card information when you sign up for the free trial to verify your identity and to distinguish actual customers from robots.
- Further details <https://cloud.google.com/free/docs/gcp-free-tier>



# Scripts will be added soon



The screenshot shows the GitHub interface for the repository 'multi-cloud-training / Hands-on-Multi-Cloud-for-Developers'. The top navigation bar includes links for 'Why GitHub?', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing', along with a search bar and 'Sign in'/'Sign up' buttons. The repository header shows 'Watch' (0), 'Star' (1), and 'Fork' (0) buttons. Below the header, there are tabs for 'Code', 'Issues' (0), 'Pull requests' (0), 'Projects' (0), and 'Insights'. A prominent banner encourages users to 'Join GitHub today' with a 'Sign up' button. The repository details section shows '1 commit', '1 branch', '0 releases', and '1 contributor'. It also includes a 'Branch: master' dropdown, a 'New pull request' button, and a 'Clone or download' button. The file list shows 'multicloud-training Initial commit' and 'README.md Initial commit 2 months ago'. The README content is partially visible, showing the title 'Hands-on-Multi-Cloud-for-Developers' and the subtitle 'Hands-on Multi-Cloud for Developers'.

<https://github.com/multi-cloud-training/Hands-on-Multi-Cloud-for-Developers>



 **Break**

 **10 Min**

## Section 2



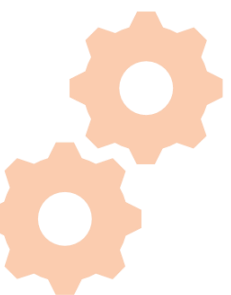
# Develop Multi-Cloud strategy



50 Min

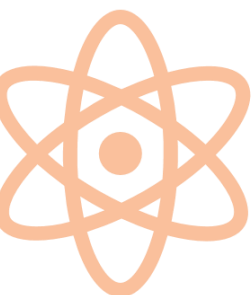
# Goals

- ✓ Multi-Cloud Strategy
- ✓ Split your infrastructure for multi-cloud platform
- ✓ Build scalable, flexible multi-cloud architecture using AWS, Azure and GCP
- ✓ Setup VPN connectivity between multi-cloud environments

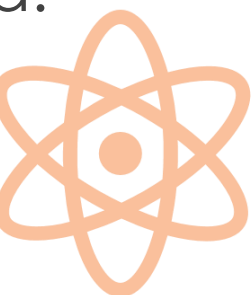
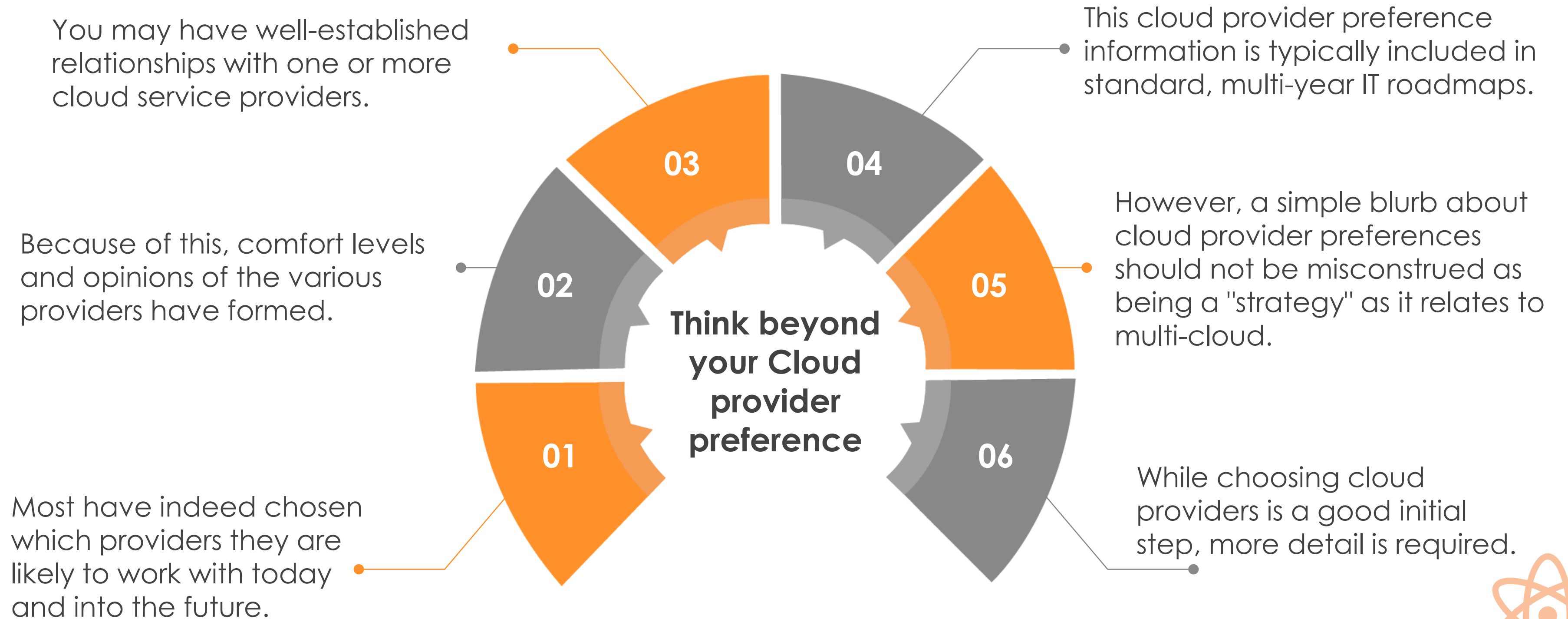


# Multi-Cloud Strategy

- A true multi-cloud strategy takes far more planning than you may think.
- It must include well thought-out and actionable steps regarding business need for multi-cloud.
- Details on how multi clouds can most efficiently be stitched together to create a singular network.
- The decision making strategy for multi-cloud based on
  - Cost
  - Performance
  - Reliability
  - Security
  - Compliance



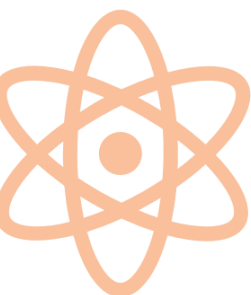
# Multi-Cloud Strategy



# Multi-Cloud Strategy

## Analyze in-house multi-cloud expertise

- When the number of public cloud providers increases as it likely will in a multi-cloud environment, IT leadership must consider how they plan to obtain and maintain in-house expertise.
- Depending on your current and future cloud plans, you may opt to train cloud administrators as generalists that can be proficient working in any cloud environment the business selects.
- A tipping point will inevitably be reached as the number of cloud providers grows.
- That's when it may make more sense to have certain administrators specialize in only a handful of cloud providers or certain cloud skills.
- Planning to identify this tipping point for your business is crucial -- especially if multi-cloud takes off faster than anticipated.

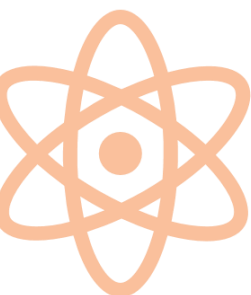




# Multi-Cloud Strategy

## Organize your applications

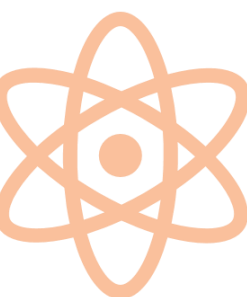
- Applications and data operate differently depending on which public/private cloud they run in.
- Cost savings, performance and redundancy must all be considered when planning where to spin up cloud services -- and where to store massive amounts of data.
- Other factors such as the cost of exporting data from the cloud, the level of elasticity required for specific apps and data, as well as what types of SLAs are required will also play heavily into this decision-making process.
- In terms of a strategy, it's best to be able to categorize various applications and data into groups as opposed to having to perform in-depth evaluations every time a new app or database project formalizes.
- That way, the decision time is shortened to avoid delays in rollout.



# Multi-Cloud Strategy

## Examine scalability and security

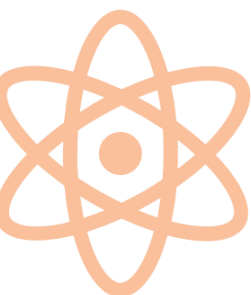
- While cloud scalability and security are vastly different topics from a technical sense, they must be discussed in tandem when looking at a multi-cloud strategy.
- It's likely that your cloud providers are not 100% compatible in terms of the setup and configuration of underlying infrastructure components for both the networking and security components.
- Thus, your multi-cloud strategy should detail how scalability and security will be initially set up and maintained.
- Some will opt for manual processes that require internal IT staff to duplicate networking and security across multiple cloud instances.
- Others will look to multi-cloud management platforms to help automate these processes.
- Either way, some serious thought must be put into this category to make sure that your multi-cloud network is both easily scaled and secure.



# Multi-Cloud Strategy

## Re-evaluate regularly

- Any multi-cloud strategy must detail when and how the current strategy should be re-evaluated to ensure it continues to meet business demands.
- Each of the topics listed above should be formally audited at set time intervals throughout the year to look for changes in need, new cloud provider opportunities and security/growth concerns.
- You'll likely find that decisions that were correct from a business strategy 12 or even 6 months prior may have dramatically changed.
- Thus, it's necessary to re-evaluate your strategy a minimum of once per year.

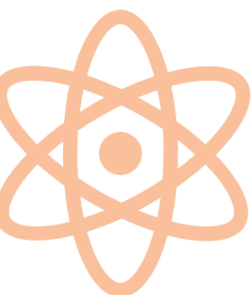


# Split your infrastructure for multi-cloud platform

In order to split the applications, databases, backups for the multi-cloud environment.

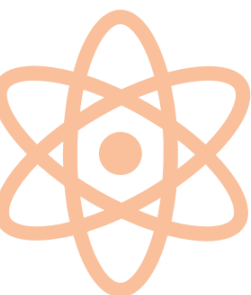
These are the most important questions to ask before split your infrastructure.

- What is the criticality of this application?
- How many users depend on it?
- What is the downtime sensitivity?
- Is it Tier 1 (highly important, 24x7 mission-critical)
- Is it Tier 2 (moderately important)
- Is it Tier 3 (low importance, dev/test)



# Split your infrastructure for multi-cloud platform

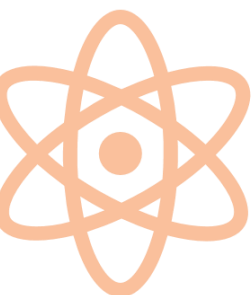
- **What is the production level of this application?**
  - Is it in production
  - Is it in staging
  - Is it in development
  - Is it in testing
- **What are the data considerations for this app?**
  - Is it Stateful data (stores data in some form)
  - Is it Stateless data (doesn't store data)
  - Other systems reliant on this data set



# Split your infrastructure for multi-cloud platform

- **How was this application developed?**
  - Third-party purchase from major vendor (still in business?)
  - Third-party purchase from minor vendor (still in business?)
  - Written in-house (author still at company?)
  - Written by a partner (still in business? still a partner?)
- **What are this application's operational standards?**
  - What organizational, business, or technological considerations exist?
  - Defined maintenance windows?
  - Defined SLAs?
  - Uptime-sensitive?
  - Latency-sensitive?
  - Accessed globally or regionally?
  - Deployed manually or via automation?

***Avoiding sensitive apps is often most desirable for a first multi-cloud migration.***



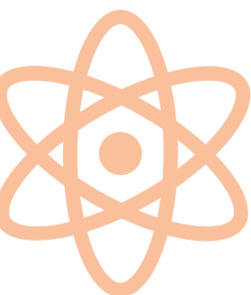
# Split your infrastructure for multi-cloud platform

- **What are the specific compliance or regulatory requirements?**
  - ISO 27000?
  - PCI/DSS?
  - HIPAA?
  - EU Personal Data Protection?
  - GDPR?

***The fewer compliance or regulatory requirements, the better for a first multi-cloud migration.***

- **What kind of documentation is readily available, and is it up-to-date?**
  - System diagram?
  - Network diagram?
  - Data flow diagram?
  - Build/deploy docs?
  - Ongoing maintenance docs?

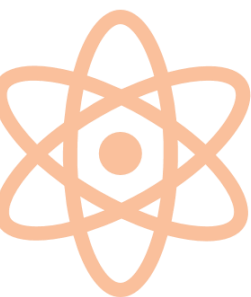
***The more docs that exist, the better!***



# Split your infrastructure for multi-cloud platform

- **What are the multi-cloud migration implications?**
  - Easy to lift-and-shift as-is into the cloud
  - May require some refactoring
  - Need to modernize before migrating
  - Can wait to modernize after migrating
  - Need to rewrite in the cloud from scratch
- **Any business considerations?**
  - Is this system used year-round or seasonally?
  - Is there a supportive line-of-business owner?
  - Does this app support an edge case or general use case?
  - Is this app managed by a central IT team or another team?
  - Would a downtime window be acceptable for this app?

***Having more supportive owners and stakeholders is always crucial to the success of initial multi-cloud migrations.***

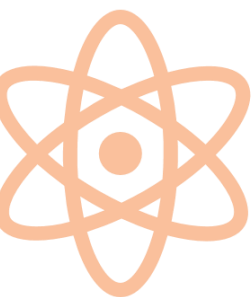




# Split your infrastructure for multi-cloud platform

- **What are the app integrations and dependencies?**
  - Look closely at how this application ties into all your other applications and workloads.
  - We can group applications into the same migration sprint if they're coupled together tightly through integrations or dependencies.
- **What are the interdependent applications?**
  - ERP (SAP)?
  - CRM ?
  - Legacy Mainframe?
  - Custom or in-house apps?

***Fewer dependencies are ideal.***



# Split your infrastructure for multi-cloud platform

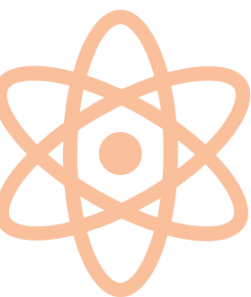
- **What are the interdependent workflows?**

- Messaging?
- Monitoring?
- Maintenance/management?
- Analytics?

***Fewer dependencies are ideal.***

- **Where is the database and storage located?**

- Separate servers?
- Co-located servers?
- Is storage block- or file-level?
- Any other services to analyze?

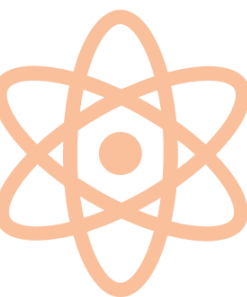


# Split your infrastructure for multi-cloud platform

- **Web services?**
  - RPC (Remote Procedure Call) used either inbound or outbound?
  - Backup services (and locations) in effect?
  - Unique dependencies?
  - Manual processes required?
  - Synchronized downtime/uptime (with other apps)?

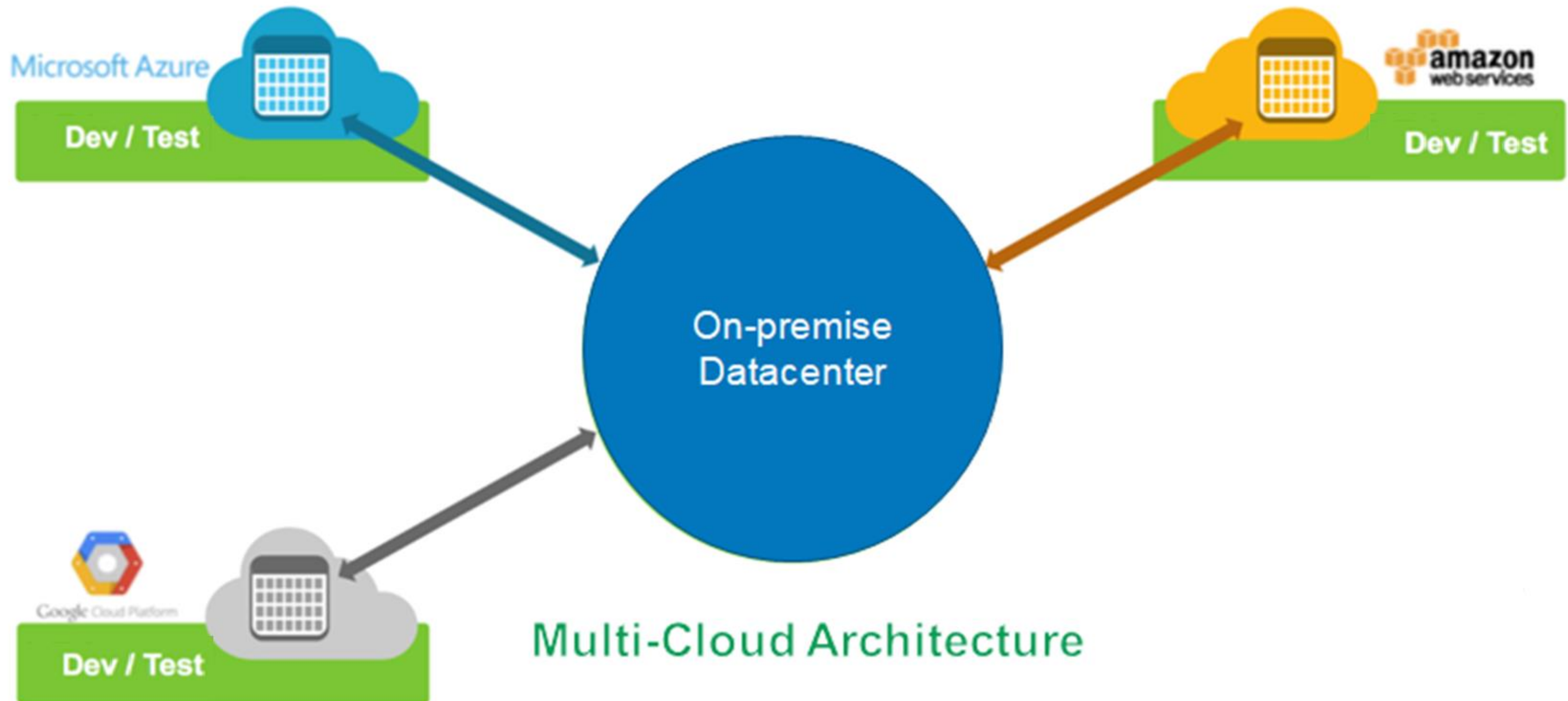
***The goal for first apps to migrate is to minimize complexity and labor.***

- Taking the time to truly understand your applications is a big part of success when migrating to the cloud.
- Picking the right applications to migrate first is key to building success and confidence within your organization in your cloud and migration strategy.
- Analyzing these details should help you to split your infrastructure for migrating to multi-cloud platform.



# Lab Activity

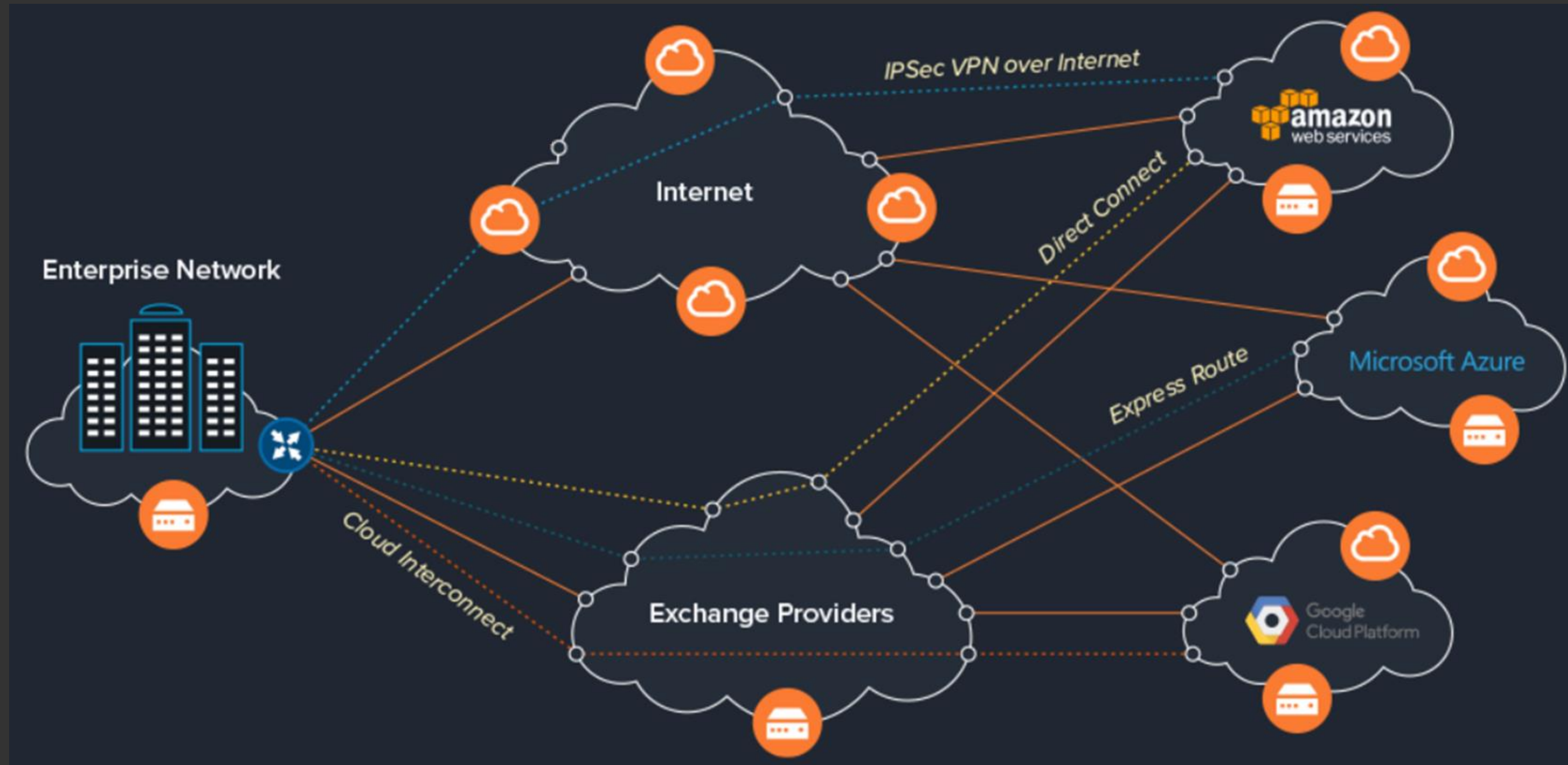
# Build scalable, flexible multi-cloud architecture using AWS, Azure and GCP



Source: <http://sdtimes.com/wp-content/uploads/2015/04/0413.sdt-hortonworks.png>



# Build scalable, flexible multi-cloud architecture using AWS, Azure and GCP

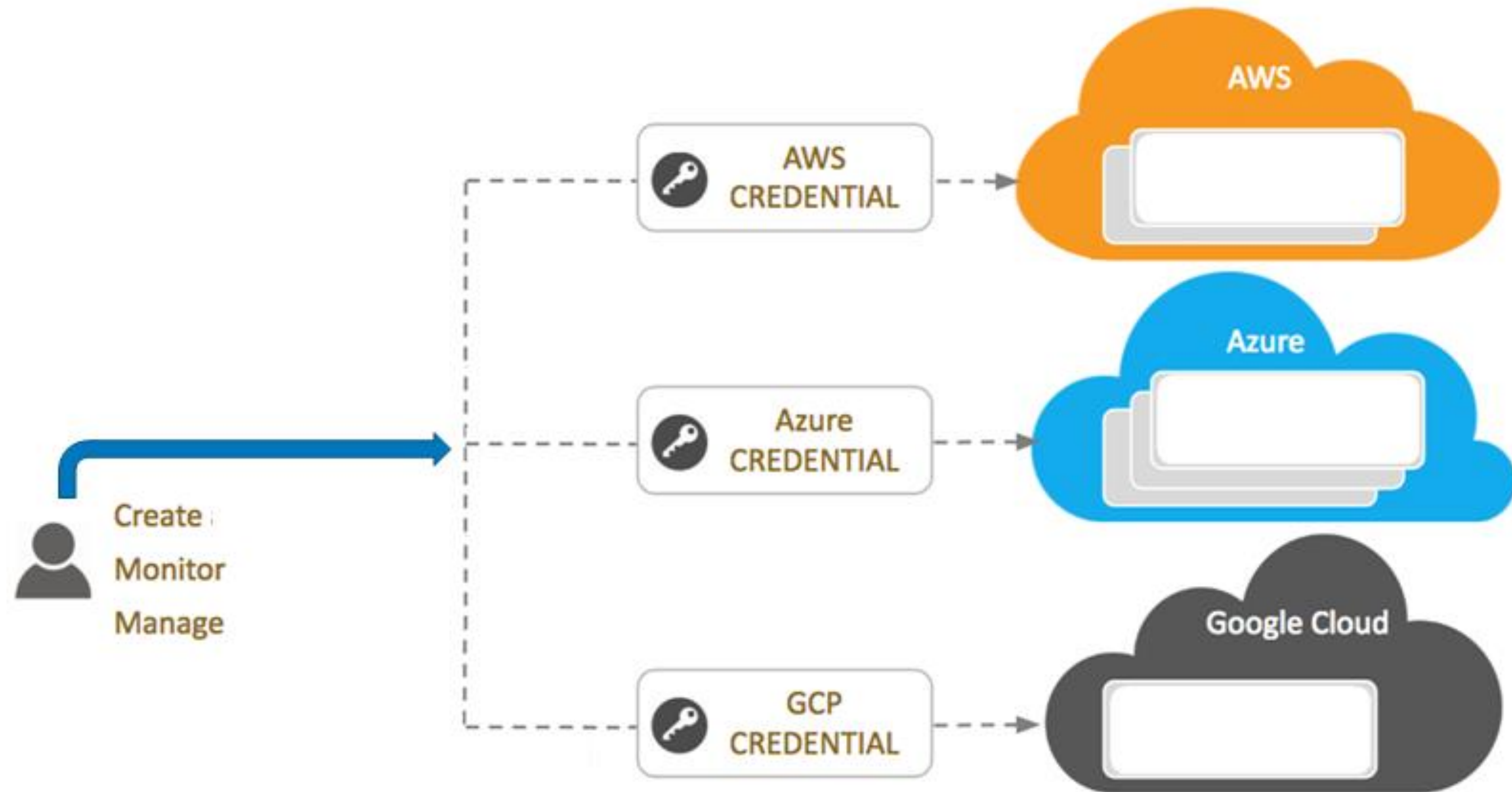


Source: [https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTW8bloTiMYfZ2Ta2mBub-qApIDUFJrTZCRgOV3UNgC7P6Owr85\\_g](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTW8bloTiMYfZ2Ta2mBub-qApIDUFJrTZCRgOV3UNgC7P6Owr85_g)





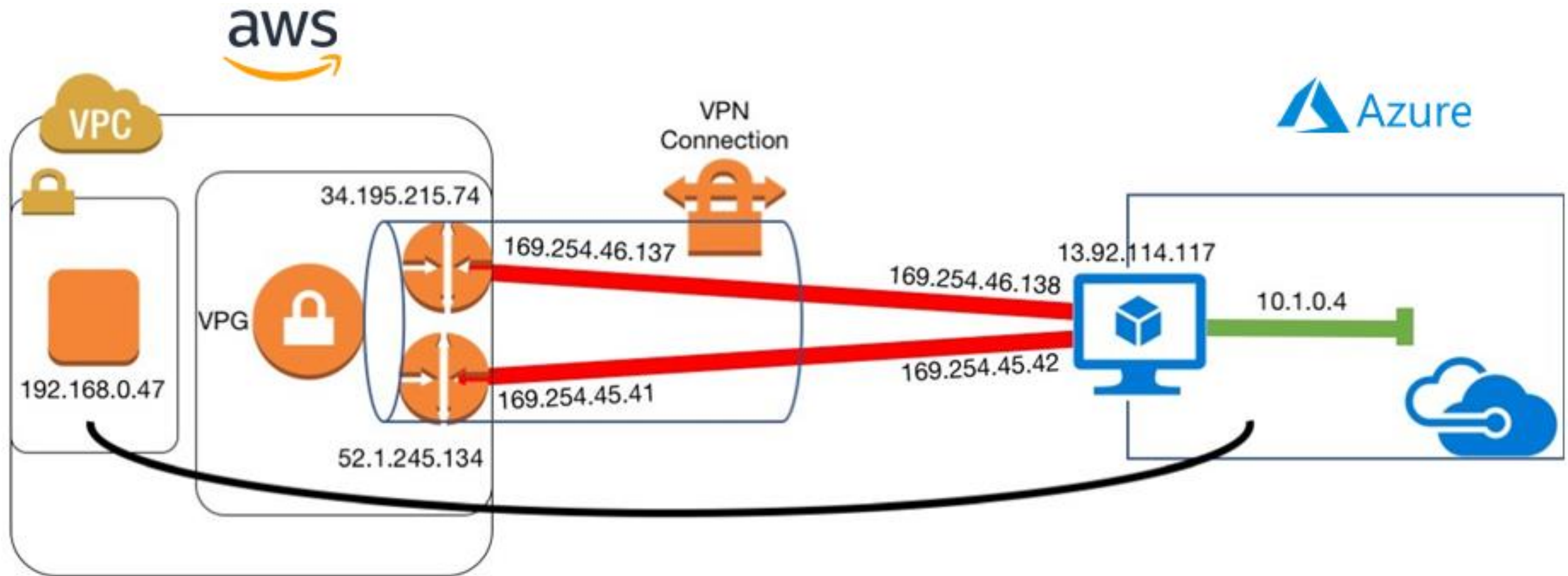
# Setup VPN connectivity between multi-cloud environments



Source: [https://hortonworks.github.io/cloudbreak-documentation/latest/images/cb\\_arch.png](https://hortonworks.github.io/cloudbreak-documentation/latest/images/cb_arch.png)



# Setup VPN connectivity between multi-cloud environments







 **Break**



**10 Min**

## Section 3



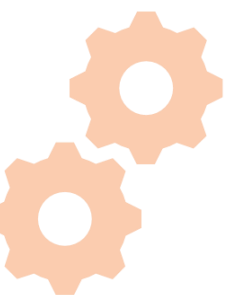
# Deploy Multi-Cloud environment



50 Min

# Goals

- ✓ Migrate your application and database to cloud
- ✓ Deploy your application from GitHub to AWS, Azure and GCP
- ✓ Build CI/CD pipeline in Azure
- ✓ Setup backup in another cloud



# Migrate your application and database to cloud

## Tier 1: Opportunistic (especially to maximize ROI)

The first tier is the strong candidates to migrate first because it revolves around current opportunities that could help you maximize ROI(Return of Investment).

Here are some questions to ask to identify the applications and databases to prioritize:

- Is this application significantly more expensive to run on-prem than it would be to migrate and run in the public cloud?
- Will this application require an upcoming hardware refresh, making it more attractive to move to the public cloud sooner rather than later?
- Are there services (or regions/instances, etc.) in the cloud that would make this application perform significantly better?

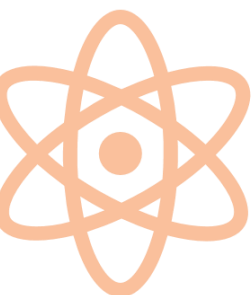
Identifying these options to migrate can create some quick wins that yield tangible, immediate benefits for users and the business.



# Migrate your application and database to cloud

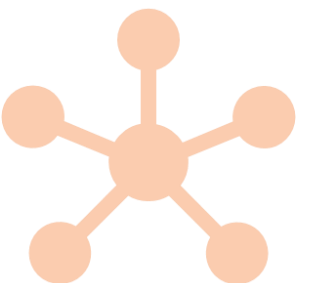
## Tier 2: Minimize your migration risk

- Where our first tier focuses on opportunity, our second tier focuses on risk.
- What applications can you move with relatively low risk to your greater IT operations?
- There are a number of questions you can ask to help evaluate which applications are the least risky to migrate, making them the most attractive to migrate in the early phases of a cloud migration project. For example:
  - What is the business criticality of this application?
  - Do large swaths of employees and/or customers depend on this application?
  - What is the production level of this application (development vs. production)?
  - How many dependencies and/or integrations does this application have?



## Migrate your application and database to cloud

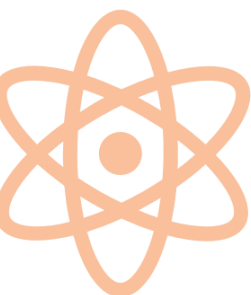
- What is my IT team's understanding of this application?
- Does my IT team have proper, up-to-date, thorough documentation for this application and its architecture?
- What are the operational requirements (SLAs) for this application?
- What are the legal or governmental compliance requirements for this application?
- What are the downtime and/or latency sensitivities for this application?
- Are there line-of-business owners eager and willing to migrate their apps early?
- Low-risk applications should be migrated first, and higher-risk applications should come later.



# Migrate your application and database to cloud

## Tier 3: Ease of migration to the multi cloud

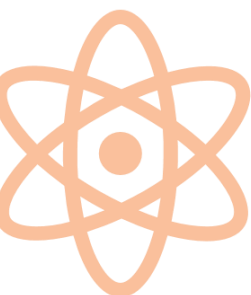
- The third tier in this framework revolves around the ease with which you can potentially migrate an application to the cloud.
- Unlike risk, which is all about that application's relative importance, ease of migration is about how frictionless the application's journey to the cloud will be. Some good questions to ask include:
  - How new is this application, and was it designed to run on-prem or in the public cloud?
  - Can this application be migrated using straightforward approaches like lift-and-shift?





# Migrate your application and database to cloud

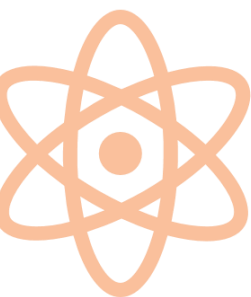
- Is this application standardized for one OS type, or does it have flexible requirements?
- Does this application (or its data) have regulatory, compliance, or SLA-based requirements to run on-premise?
- When plotting out which applications to migrate to the cloud, you may find that sometimes applications from Tier 3 may go before Tier 2 (or even Tier 1).
- Tier 2 and Tier 3 both involve a lot of variables, so it's common to have some mixing and matching along your migration path.



# Migrate your application and database to cloud

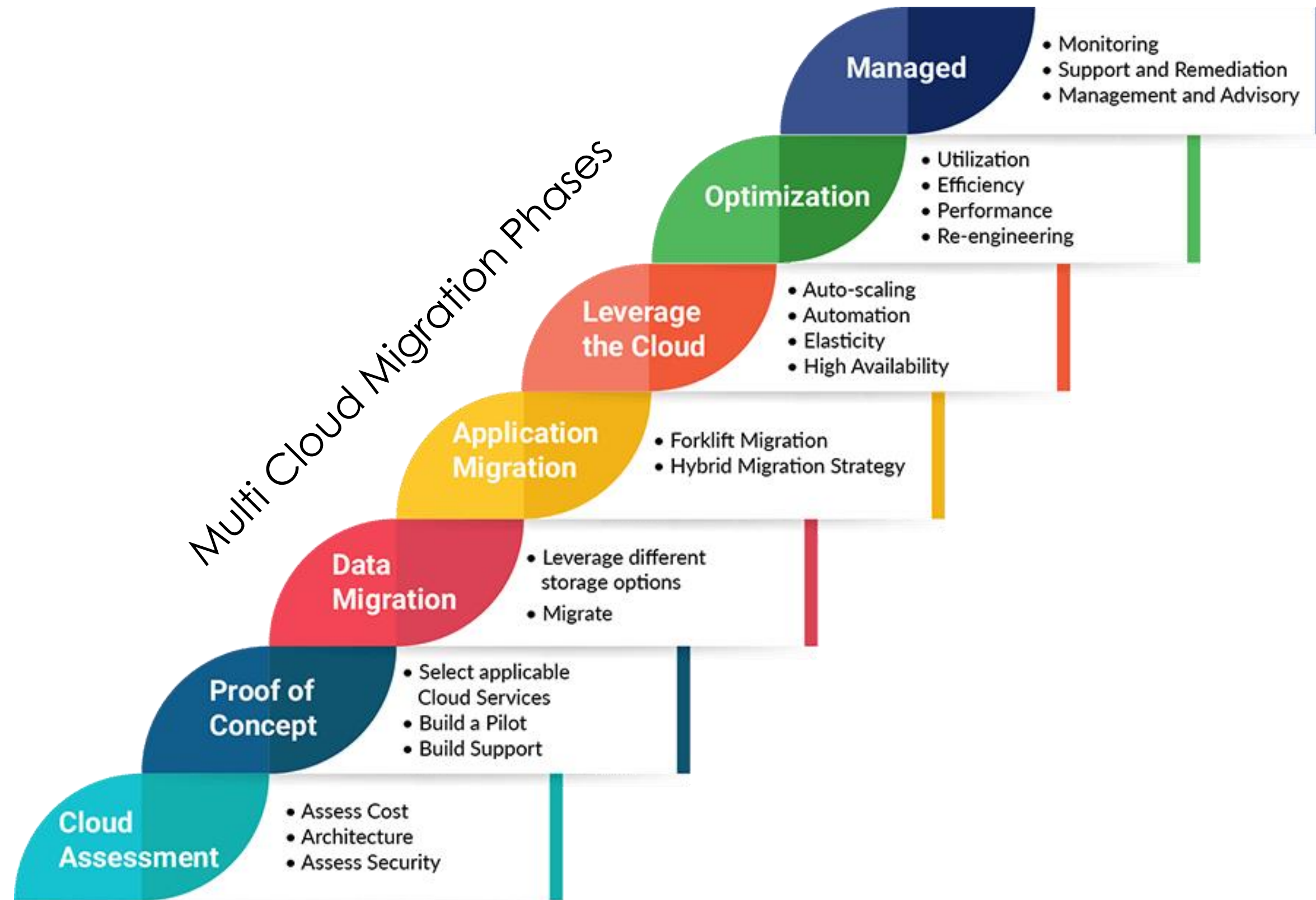
## Tier 4: Custom applications

- The fourth and final tier of this framework—representing the applications you should migrate last—are your custom applications.
- These are applications that were written in-house or by third parties, but which will pose some potentially unique migration questions, like:
  - Was this application built specifically for its current hardware? For on-premise?
  - Do we have proper comments in the code to help us re-architect for the cloud if needed?
  - How is this application intertwined within our total application landscape?
  - Do we have the in-house expertise to migrate this application to the cloud successfully?

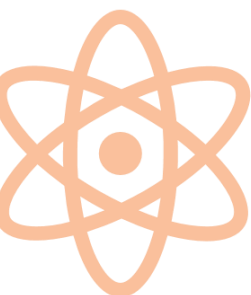


# Lab Activity

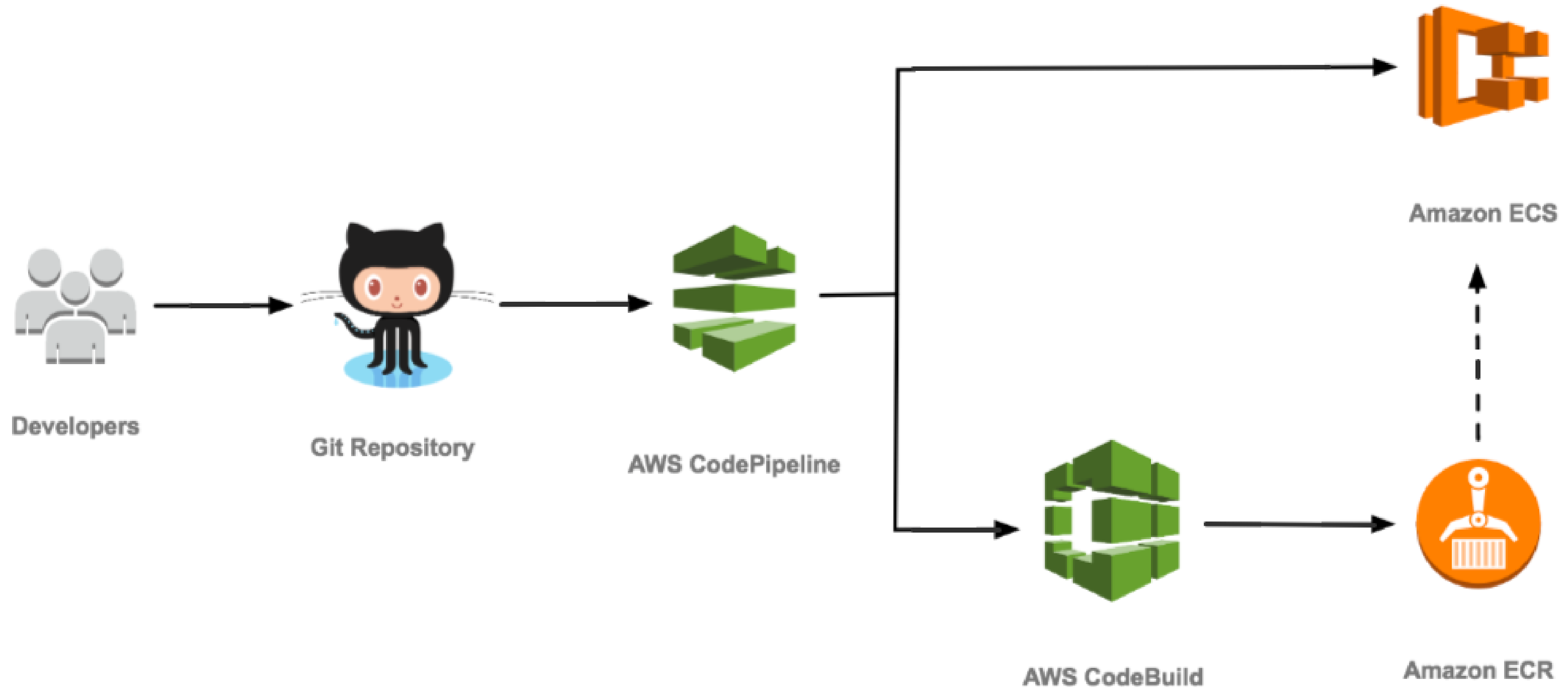
# Migrate your application and database to cloud



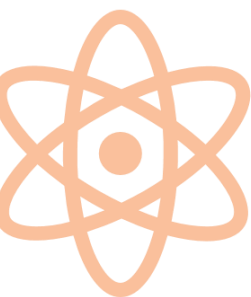
Source: <https://progressive.in/wp-content/uploads/2017/12/date-migration.png>



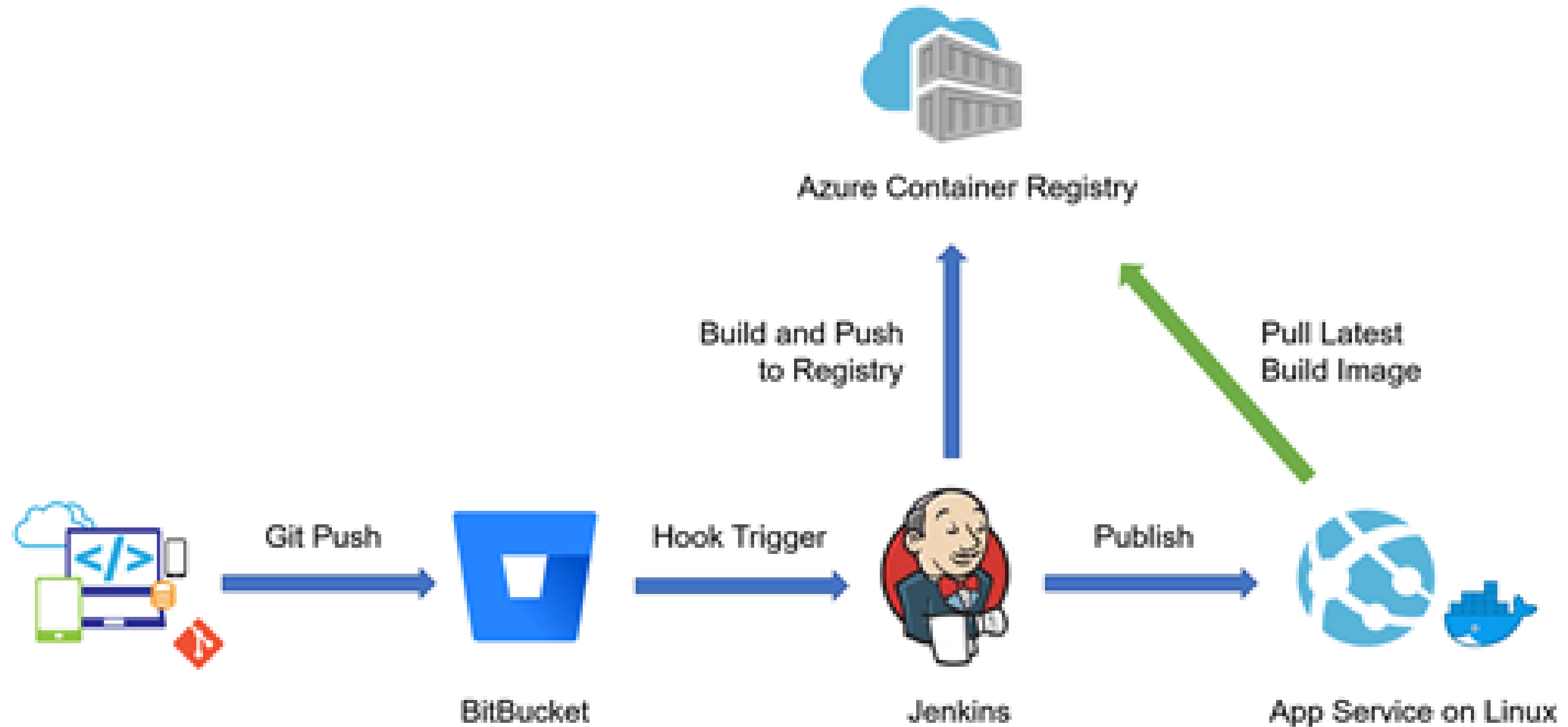
# Deploy your application from GitHub to AWS, Azure and GCP



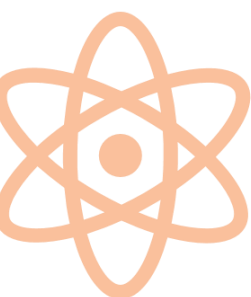
Source: [https://cdn-images-1.medium.com/max/1200/1\\*YycpUVzoFYnLi\\_OvIYVQtw.png](https://cdn-images-1.medium.com/max/1200/1*YycpUVzoFYnLi_OvIYVQtw.png)



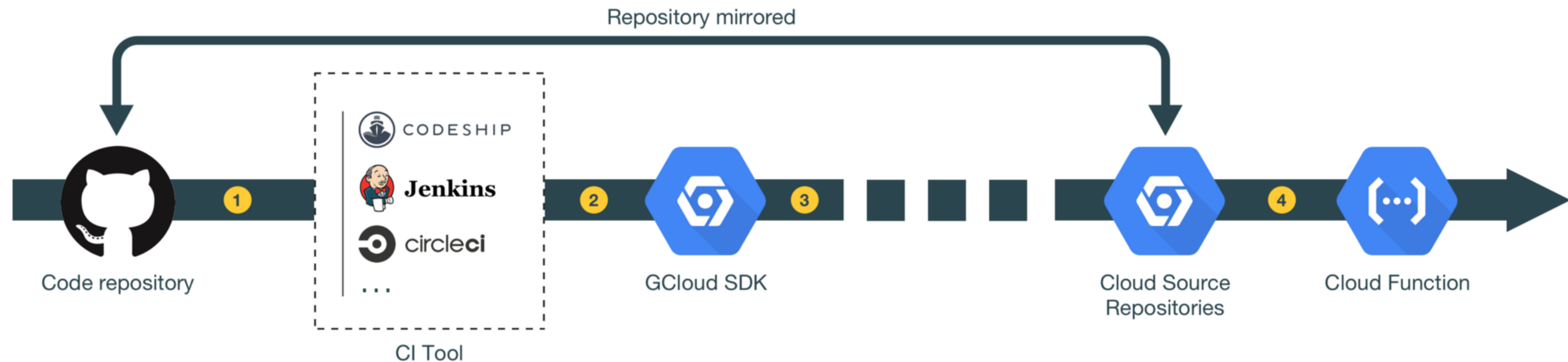
# Deploy your application from GitHub to AWS, Azure and GCP



Source: [https://cdn-images-1.medium.com/max/483/1\\*EavQgOE1U0i3kPQ3crbMIQ.png](https://cdn-images-1.medium.com/max/483/1*EavQgOE1U0i3kPQ3crbMIQ.png)

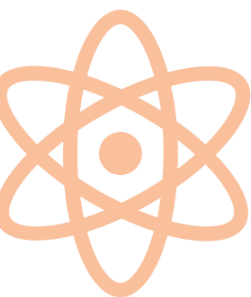


# Deploy your application from GitHub to AWS, Azure and GCP



- 1 Commit and optionally tag.
- 2 Run tests on every commit. On tag, deploy with GCloud SDK.
- 3 GCloud SDK triggers redeployment from mirrored source repo.
- 4 Cloud Function is redeployed from mirrored source repo.

Source: [https://cdn-images-1.medium.com/max/2000/1\\*zOP9Ch4v3\\_Phh3E32cgjA.png](https://cdn-images-1.medium.com/max/2000/1*zOP9Ch4v3_Phh3E32cgjA.png)

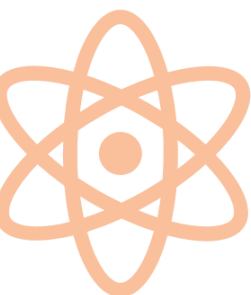


# Build CI/CD pipeline in Azure

Azure DevOps Projects presents a simplified experience where you can bring your existing code and Git repo or choose a sample application to create a continuous integration (CI) and continuous delivery (CD) pipeline to Azure.

You will:

- Use DevOps Projects to create a CI/CD pipeline
- Configure access to your GitHub repo and choose a framework
- Configure Azure DevOps and an Azure subscription
- Commit changes to GitHub and automatically deploy them to Azure
- Examine the Azure Pipelines CI/CD pipeline
- Configure Azure Application Insights monitoring
- Clean up resources

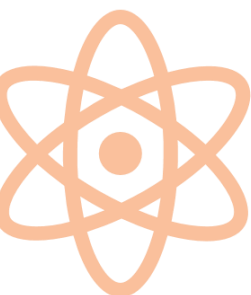




# Build CI/CD pipeline in Azure

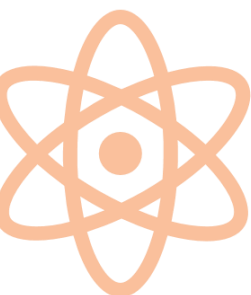
Azure DevOps Projects creates a CI/CD pipeline in Azure Pipelines. You can create a new Azure DevOps organization or use an existing organization. Azure DevOps Projects also creates Azure resources in the Azure subscription of your choice.

- Sign in to the [Azure portal](#).
- In the left pane, select **New**.
- In the search box, type **DevOps Projects**, and then select **Create**.
- Select Bring your own code, and then select Next.
- Configure access to your GitHub repo and choose a framework
- Select either GitHub or an external Git repo, and then select your repo and the branch that contains your application.
- Select your web framework, and then select Next.
- The application framework, which you chose previously, dictates the type of Azure service deployment target that's available here.
- Select the target service, and then select Next.



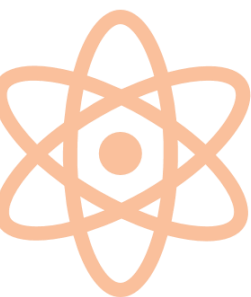
# Build CI/CD pipeline in Azure

- Configure Azure DevOps and an Azure subscription
- Create a new Azure DevOps organization or select an existing organization.
  - a. Enter a name for your project in Azure DevOps.
  - b. Select your Azure subscription and location, enter a name for your application, and then select Done.
- After a few minutes, the DevOps Projects dashboard is displayed in the Azure portal.
- A sample application is set up in a repo in your Azure DevOps organization, a build is executed, and your application is deployed to Azure.
- This dashboard provides visibility into your GitHub code repo, the CI/CD pipeline, and your application in Azure.
- Select Browse to view your running application.



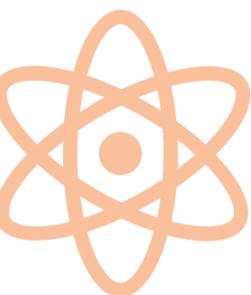
# Build CI/CD pipeline in Azure

- Azure DevOps Projects automatically configures a CI build and release trigger. Your code remains in your GitHub repo or another external repo.
- Commit changes to GitHub and automatically deploy them to Azure
- You're now ready to collaborate with a team on your app by using a CI/CD process that automatically deploys your latest work to your website.
- Each change to the GitHub repo starts a build in Azure DevOps, and a CD pipeline executes a deployment to Azure.
- Make a change to your application, and then commit the change to your GitHub repo.
- After a few moments, a build starts in Azure Pipelines.
- You can monitor the build status in the DevOps Projects dashboard, or you can monitor it in the browser with your Azure DevOps organization.
- After the build is completed, refresh your application to verify your changes.



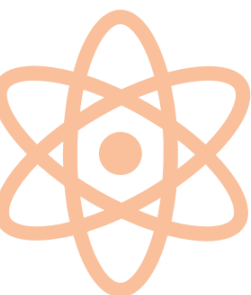
# Build CI/CD pipeline in Azure

- Examine the Azure Pipelines CI/CD pipeline
- Azure DevOps Projects automatically configures a CI/CD pipeline in Azure Pipelines.
- Explore and customize the pipeline as needed. To familiarize yourself with the build and release pipelines, do the following:
  - At the top of the DevOps Projects dashboard, select Build pipelines.
  - A browser tab displays the build pipeline for your new project.
  - Point to the Status field, and then select the ellipsis (...).
  - A menu displays several options, such as queueing a new build, pausing a build, and editing the build pipeline.
  - Select Edit.
  - In this pane, you can examine the various tasks for your build pipeline.



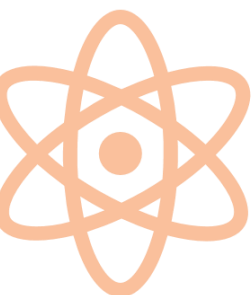
# Build CI/CD pipeline in Azure

- The build performs various tasks, such as fetching sources from the Git repo, restoring dependencies, and publishing outputs used for deployments.
- At the top of the build pipeline, select the build pipeline name.
- Change the name of your build pipeline to something more descriptive, select Save & queue, and then select Save.
- Under your build pipeline name, select History.
- You see an audit trail of your recent changes for the build.
- Azure DevOps keeps track of any changes made to the build pipeline, and it allows you to compare versions.
- Select Triggers.
- Azure DevOps Projects automatically creates a CI trigger, and every commit to the repo starts a new build.
- Optionally, you can choose to include or exclude branches from the CI process.



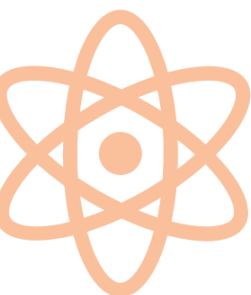
# Build CI/CD pipeline in Azure

- Select Retention.
- Depending on your scenario, you can specify policies to keep or remove a certain number of builds.
- Select Build and Release, and then select Releases.
- Azure DevOps Projects creates a release pipeline to manage deployments to Azure.
- Select the ellipsis (...) next to your release pipeline, and then select Edit.
- The release pipeline contains a pipeline, which defines the release process.
- Under Artifacts, select Drop.
- The build pipeline you examined in the previous steps produces the output that's used for the artifact.
- Next to the Drop icon, select Continuous deployment trigger.



# Build CI/CD pipeline in Azure

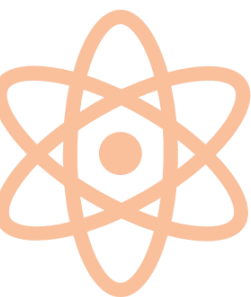
- This release pipeline has an enabled CD trigger, which executes a deployment every time there is a new build artifact available.
- Optionally, you can disable the trigger so that your deployments require manual execution.
- At the left, select Tasks.
- Tasks are the activities that your deployment process executes.
- A task was created to deploy to the Azure App service.
- At the right, select View releases to display a history of releases.
- Select the ellipsis (...) next to a release, and then select Open.
- There are several menus to explore, such as a release summary, associated work items, and tests.





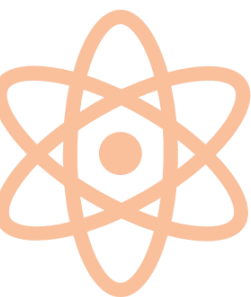
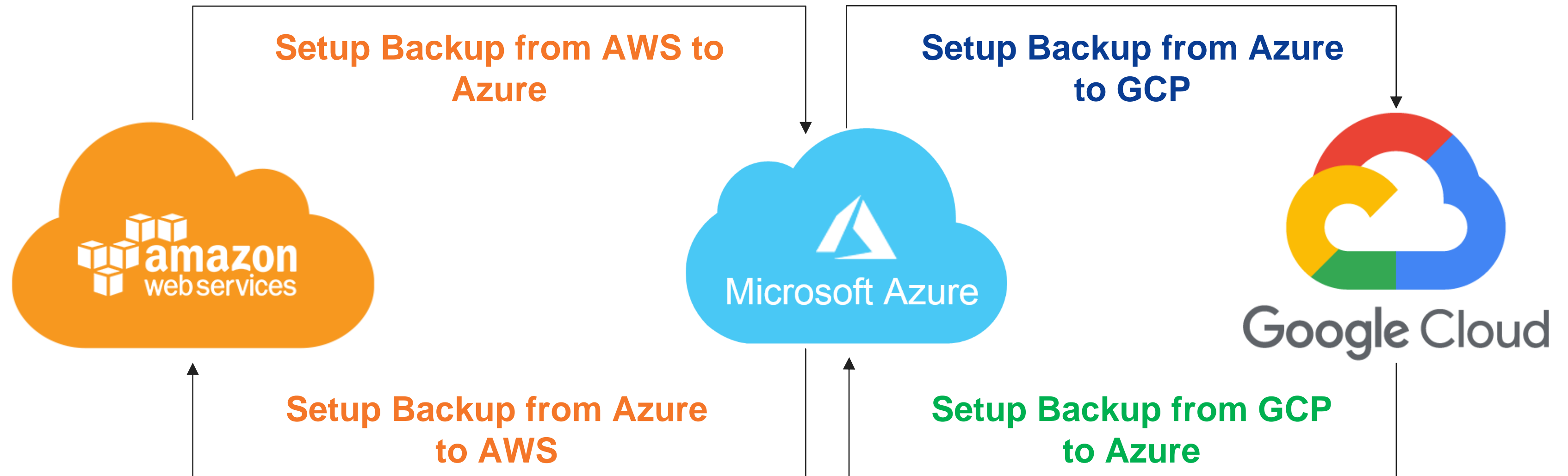
# Build CI/CD pipeline in Azure

- Select Commits.
- This view shows code commits that are associated with this deployment.
- Select Logs.
- The logs contain useful information about the deployment process.
- You can view them both during and after deployments.
- With Azure Application insights, you can easily monitor your application's performance and usage.
- In the Azure portal, go to the DevOps Projects dashboard.
- At the lower right, select the Application Insights link for your app.
- The Application Insights pane opens.
- This view contains usage, performance, and availability monitoring information for your app.





# Setup backup in another cloud



 **Break**



**10 Min**

Section 4



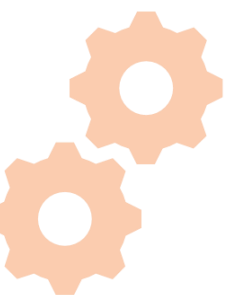
# Deploy and Migrate your Application



50 Min

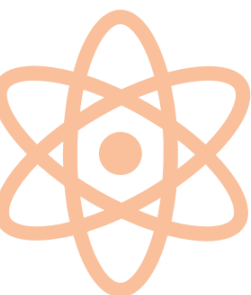
# Goals

- ✓ Deploy microservices application into more than one cloud
- ✓ Load Balance the workload using global load balancer
- ✓ Migrate Dockers application from AWS to Azure to GCP
- ✓ Lab Activity



# Deploy microservices application into more than one cloud

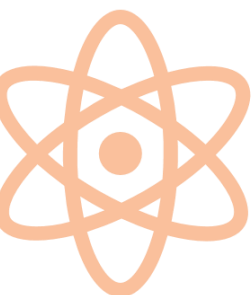
- Microservices or small, functional elements that are often shared among applications -- can magnify these benefits considerably.
- First, we have to plan, develop and deploy microservices properly.
- To begin microservices planning, we need to understand what makes microservices different than application components or elements of a service-oriented architecture.
- Microservices are not complete application pieces;
  - They are designed to be shared, as services, among applications
  - Multiple apps can invoke a single instance of a microservice at the same time.
- Microservices are also designed to use web-like RESTful interfaces.
- If microservices don't fit the model above, they aren't likely to deliver as many benefits.
- When microservices do match the characteristics above, you need to sustain each of them in a multicloud deployment.



# Deploy microservices application into more than one cloud

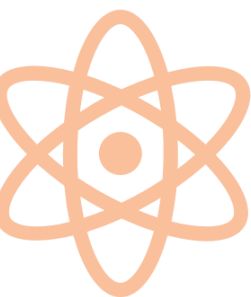
## Microservices' impact on multicloud networks

- The easiest way to approach microservice access is to assume that you have a VPN network that joins all your clouds and data centers.
- Because microservices are small pieces of functionality, they can divide applications into many successive requests for an external service.
- This service is accessed over a network that can introduce propagation delay and other network performance issues.
- It is critical that the network connection that links microservices to the applications that use them delivers the quality of service (QoS) needed to support users' experience.
- Before you deploy microservices, test their performance in all of the hosting variations across your multicloud environment.
- If your QoS falls below acceptable levels, change your network connectivity to correct it.
- Alternatively, you could design your application deployment process so that services aren't moved to dead spots in your network.



# Deploy microservices application into more than one cloud

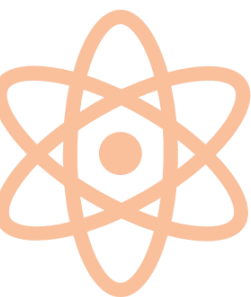
- Network performance issues in multicloud applications are usually related to the way traffic passes through the multicloud or single cloud and data center boundary points.
- Talk to your cloud providers, your VPN provider and your data center networking team to optimize connectivity.
- Be especially wary with multicloud applications, because many public cloud providers won't connect directly with other providers; they will expect to connect back through your VPN or data center network.
- If an application in one cloud uses a microservice in another, there could be a long potential propagation delay.
- If you can't reduce it, avoid crossing cloud provider boundaries with microservice access.
- You may need to deploy a duplicate of the service in each cloud to avoid such network performance issues.





# Deploy microservices application into more than one cloud

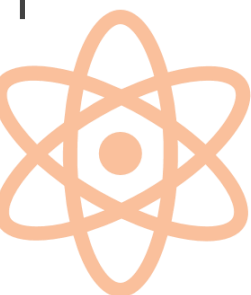
- The need for multiple applications to access a microservice may also require network accommodations.
- That way, you can deploy microservices anywhere, and applications can reach them using standard IP mechanisms, such as URLs and Domain Name Services (DNS), or other service cataloging methods.
- Another challenge occurs when a microservice moves from one cloud provider to another, or between a cloud provider and a data center.
- Normally, this kind of movement requires a change in the IP address, which means the logical name of the service will have to be associated with a different address after the move.
- Make sure your tools and practices for replacing a failed component make the necessary change to DNS or service catalog entries so your applications can find the microservice in its new location.
- Compared to monolithic architectures, microservices create a more seamless process for developers
- Compare monolithic and microservices architectures



# Deploy microservices application into more than one cloud

## Deploy microservices securely

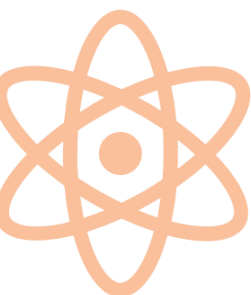
- The fact that multiple applications often share a single microservice can create two other challenges in hybrid and multcloud environments: security and compliance, and stateful vs. stateless behavior.
- Any time applications share functionality, there's a risk that an application with rigorous compliance requirements will be contaminated.
- This is because a shared service might provide outsiders with a portal for entry.
- Since moving microservices, or duplicating them under load, requires fairly open addressing, you need to secure each microservice with respect to its access.
- Avoid microservices that mix features demanding security and compliance monitoring with other features open to a larger community make them two different microservices.



# Deploy microservices application into more than one cloud

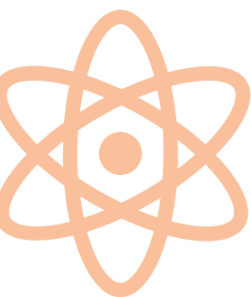
## Explore the stateful vs. stateless issue

- Avoid microservices that mix features demanding security and compliance monitoring with other features open to a larger community.
- The stateful vs. stateless issue is complex, even for software architects and developers.
- Applications typically support transactional activity that involves multiple steps or states.
- For example, imagine we have a service called "add two numbers."
  - If we present the first number on one request and the second on another, other users could inadvertently introduce their own number between our two, and we'd get the wrong answer.



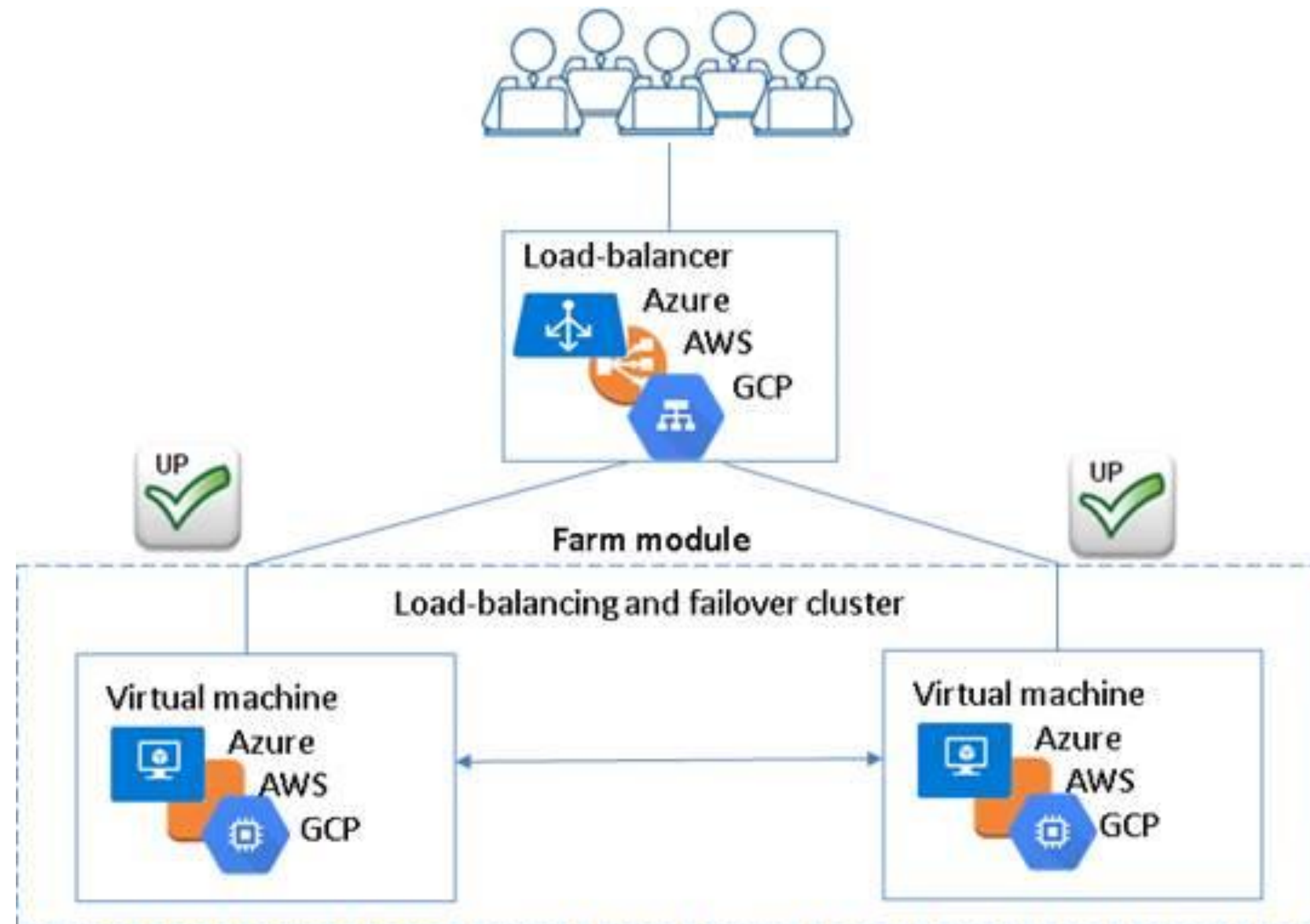
# Deploy microservices application into more than one cloud

- If microservices cannot save data between requests made to it, then make the requests stateless or ensure they can somehow convey the state, if needed.
- It's also possible to have the request include a user ID that the microservice would associate, through a back-end database, with the state.
- When a first number is presented, the microservice would record that number in the database.
- Then, when the second is presented, it could add them and return the answer.
- There's always a price to be paid for versatility, agility and flexibility and combining microservices with multiclouds.
- Plan carefully to minimize that price and deploy microservices that extend easily into a complex multi-cloud future.

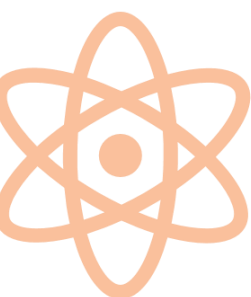


# Lab Activity

# Load Balance the workload using global load balancer

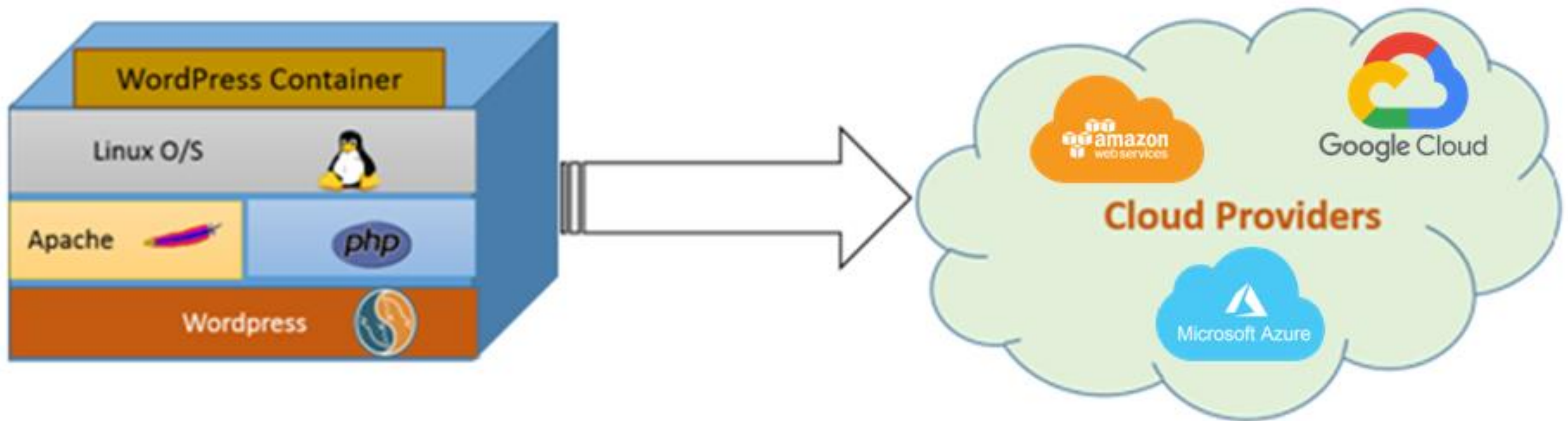


Source: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRRcpYIPeFBqCWOOCfJ4dxd-BVeKcsvrktFWc09MT98mZ01jr6H>

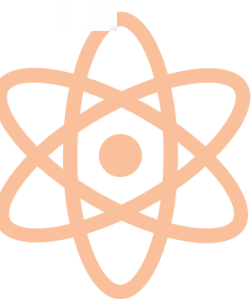




# Migrate Dockers application from AWS to Azure to GCP



Source: [https://www.corestack.io/wp-content/uploads/2014/10/070814\\_1103\\_migratingap2.png](https://www.corestack.io/wp-content/uploads/2014/10/070814_1103_migratingap2.png)





# End of Day 1

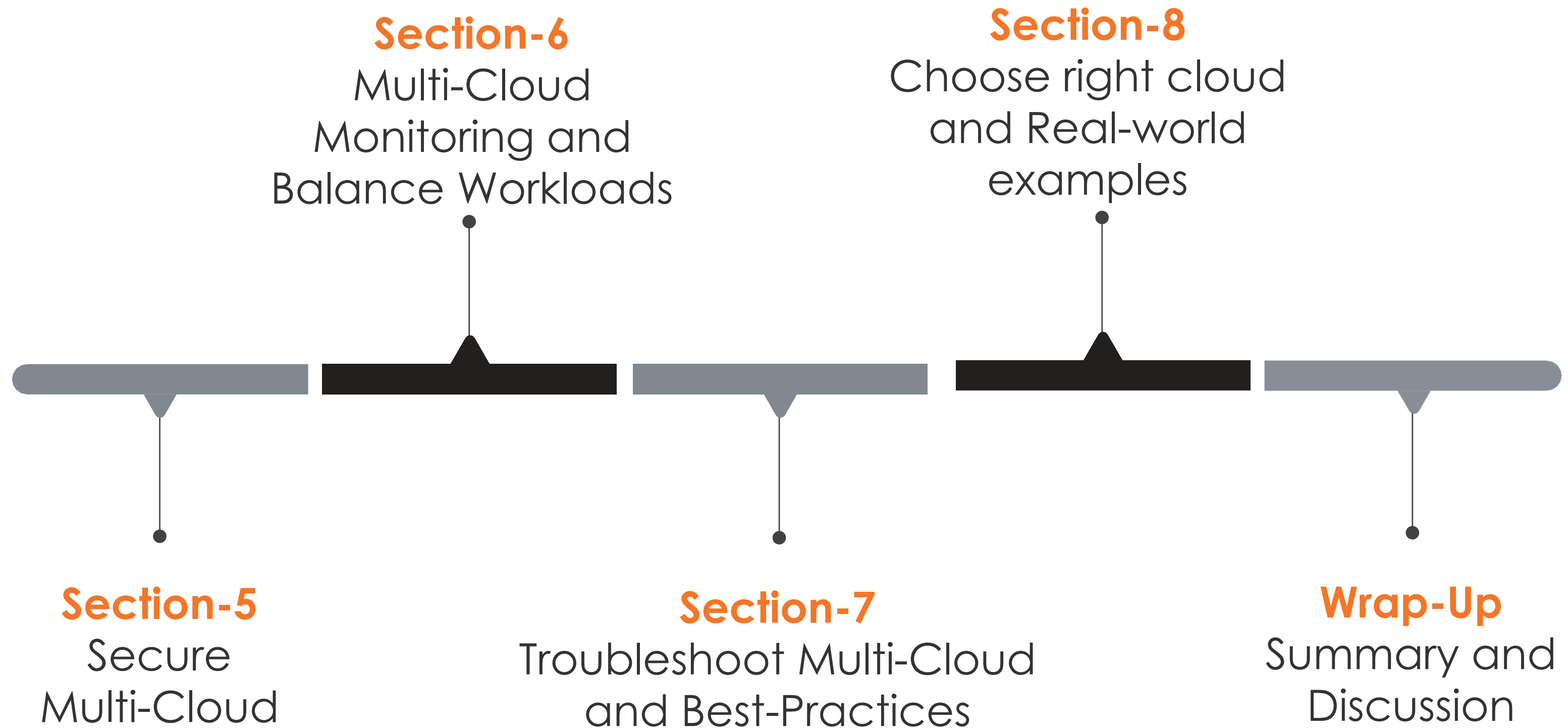




**THANKS EVERYONE !**  
**WILL RESUME TOMORROW !**

# DAY 2

# Day-2



Section 5



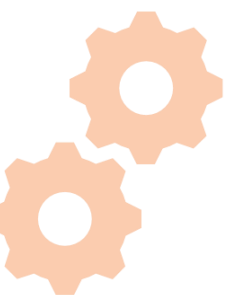
# Secure your Multi-Cloud environment



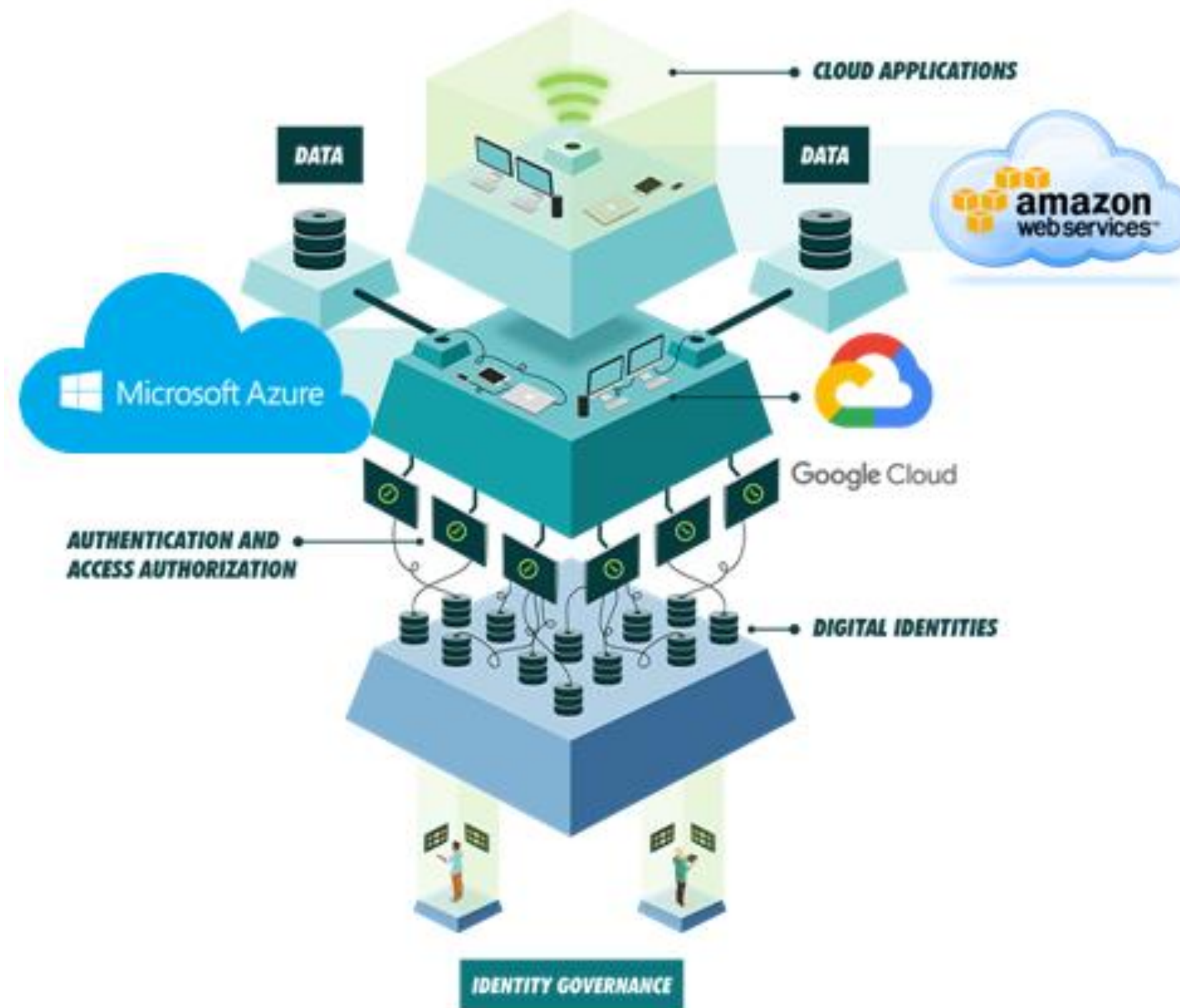
50 Min

# Goals

- ✓ Build security aware multi-cloud platform
- ✓ Explore right tools/services for boosting security
- ✓ Make Multi Cloud more resilient against DDoS attacks
- ✓ Deploy mandatory security controls



# Build security aware multi-cloud platform



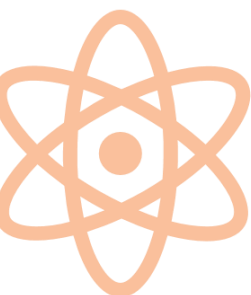
Source: <https://silasg.com/application/files/8215/4083/9571/zero-trust-iga-diagram.png>





# Build security aware multi-cloud platform

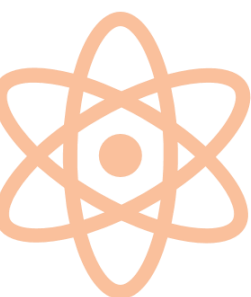
- In the traditional data center, primary security came from securing the perimeter. We typically used security middleware, such as IP firewalls, web application firewalls (WAF), and intrusion detection systems (IDS). The idea was to create a zone of trust inside the data center.
- A typical refinement to this model was to subdivide the high-trust zone, using virtual LANs or software-defined networking—often segmenting it by line-of-business.
- But when we move some of our workloads to a public cloud, things become more challenging. This becomes even more challenging when you introduce multiple cloud services or cloud zones.



# Build security aware multi-cloud platform

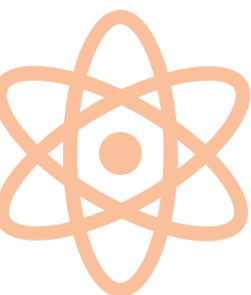


Source: <https://www.hytrust.com/uploads/Asset-71-1.png>



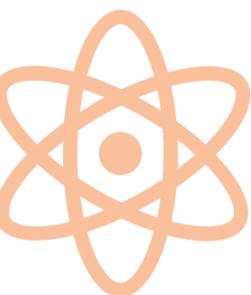
# Build security aware multi-cloud platform

- Multi-Cloud secure to enable secure communications "from any host, to any host, anywhere" with application-level DTLS encrypted micro-tunnels and Public Key Authentication. Scales across environments to build a secure hybrid/multi-cloud distributed application infrastructure. No cloud vendor lock-in.
- **Micro-Perimeters** – Application-level micro-tunnels give network admins the ability to deep segment by application, not by network. Limits remote users to fine-grained access to specific services. No ACLs or FW policies to manage. Eliminates lateral network attacks.
- **Discreet Invisibility** – Randomly generated non-standard UDP ports for dynamic on-demand micro-tunnel communications. Servers are cloaked and secured with no open ports. Virtually eliminates network attack surfaces.



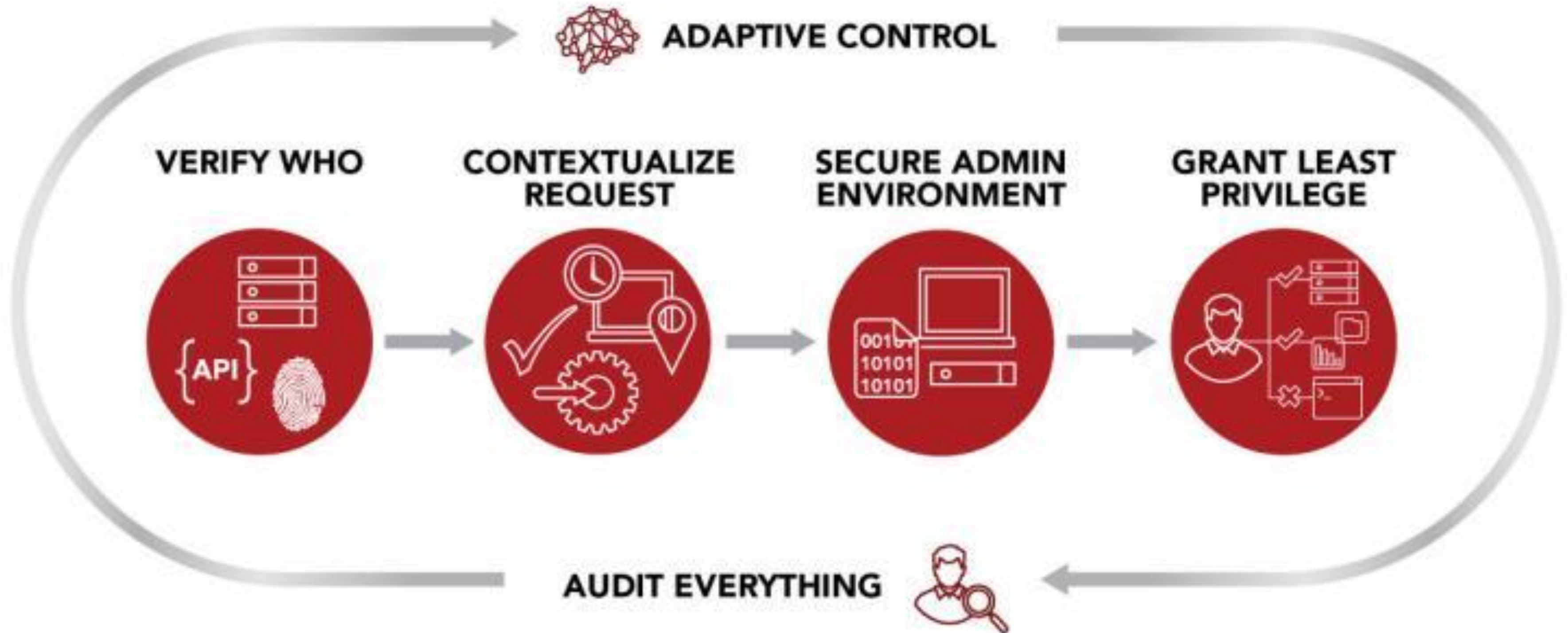
# Build security aware multi-cloud platform

- **Smart Availability** – Dynamic movement of micro-tunnel gateways and application workloads with self-healing automatic fault detection and failover.
- The perimeter can be orchestrated to change dynamically so that micro-tunnels and workloads always find their **best execution venue** (BEV). The entire application infrastructure is "always-secure and always-on."
- **Lightweight Software** – Software-Defined-Perimeter solution. Just install on any host and connect. Integrates into existing network infrastructure. No network reconfiguration. No appliances to deploy, configure or maintain.





# Build security aware multi-cloud platform

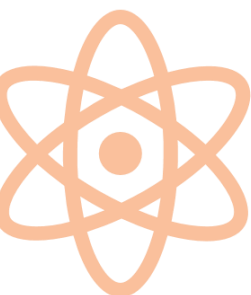


Source: [https://www.centrixy.com/sites/default/files/styles/inline\\_sm/public/2018-12/Zero-Trust-approach.jpg?itok=9OhVQHpd](https://www.centrixy.com/sites/default/files/styles/inline_sm/public/2018-12/Zero-Trust-approach.jpg?itok=9OhVQHpd)



# Build security aware multi-cloud platform

- In modern environments, it's better to assume that there is no perimeter—or at least it's better to not depend on one. This is also a good way to counter insider threats.
- In this new world of zero-trust networks, Armon suggests three important aspects for success:
  - **Good secrets management:** don't hard-code service passwords
  - **Segmentation:** don't segment by network, but do it by service
  - **Data protection:** encrypt data at rest



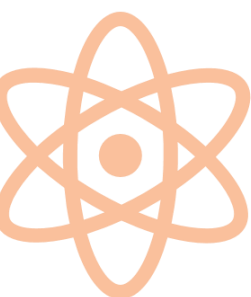
# Explore right tools/services for boosting security

## Clouds are the New Silos

Different teams, with different expertise, using different environments and tools



Source: <https://zdnet2.cbsstatic.com/hub/i/r/2017/08/25/a8549ee6-bb34-4693-bb7c-496ec0445140/resize/770xauto/93c790c2a9c0bf43bb0d5edb64921918/vmware-clouds.png>

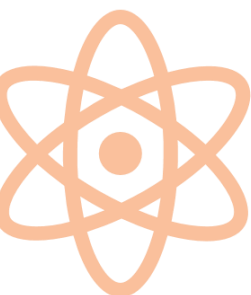




# Explore right tools/services for boosting security

## Establish actionable, compliance-based policies.

- Considering the speed of development and deployment common in today's multi-cloud environments, organizations need to embrace policies that embed compliance and security testing into both the service delivery process and software development lifecycle.
- The most effective route is to embrace cloud-based offerings capable of providing continuous verification, analytics, and governance throughout your software delivery and cloud operations processes.



# Explore right tools/services for boosting security

## IOT/ IIOT SECURITY



## MOBILE SECURITY



## CLOUD SECURITY



## THREAT INTELLIGENCE



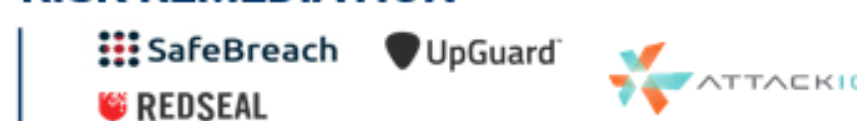
## BEHAVIORAL DETECTION



## DECEPTION SECURITY



## RISK REMEDIATION



## NETWORK & ENDPOINT SECURITY



## CONTINUOUS NETWORK VISIBILITY



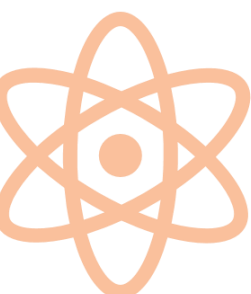
## QUANTUM ENCRYPTION



## WEBSITE SECURITY

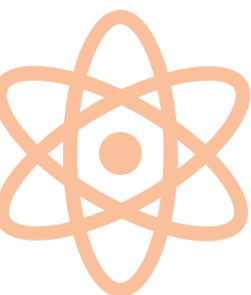


Source: <https://cbi-blog.s3.amazonaws.com/blog/wp-content/uploads/2016/08/THE-ONE-IN-THE-POST-9-30-16.png>



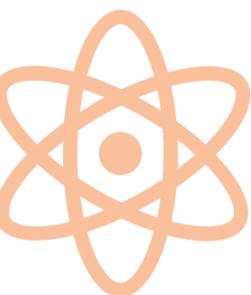
# Explore right tools/services for boosting security

- Successful multi-cloud security requires checking and enforcing critical configurations of cloud services as well as vulnerabilities in application libraries and web application components.
- The security of any multi-cloud infrastructure depends on the proper configuration of numerous services across an entire array of resources.
- When a multi-cloud deployment is coupled with a well-managed strategy, organizations have access to actionable data including cross functional visibility.
- This information is crucial as an organization works to prioritize and remediate risks based on the potential impact to the business.



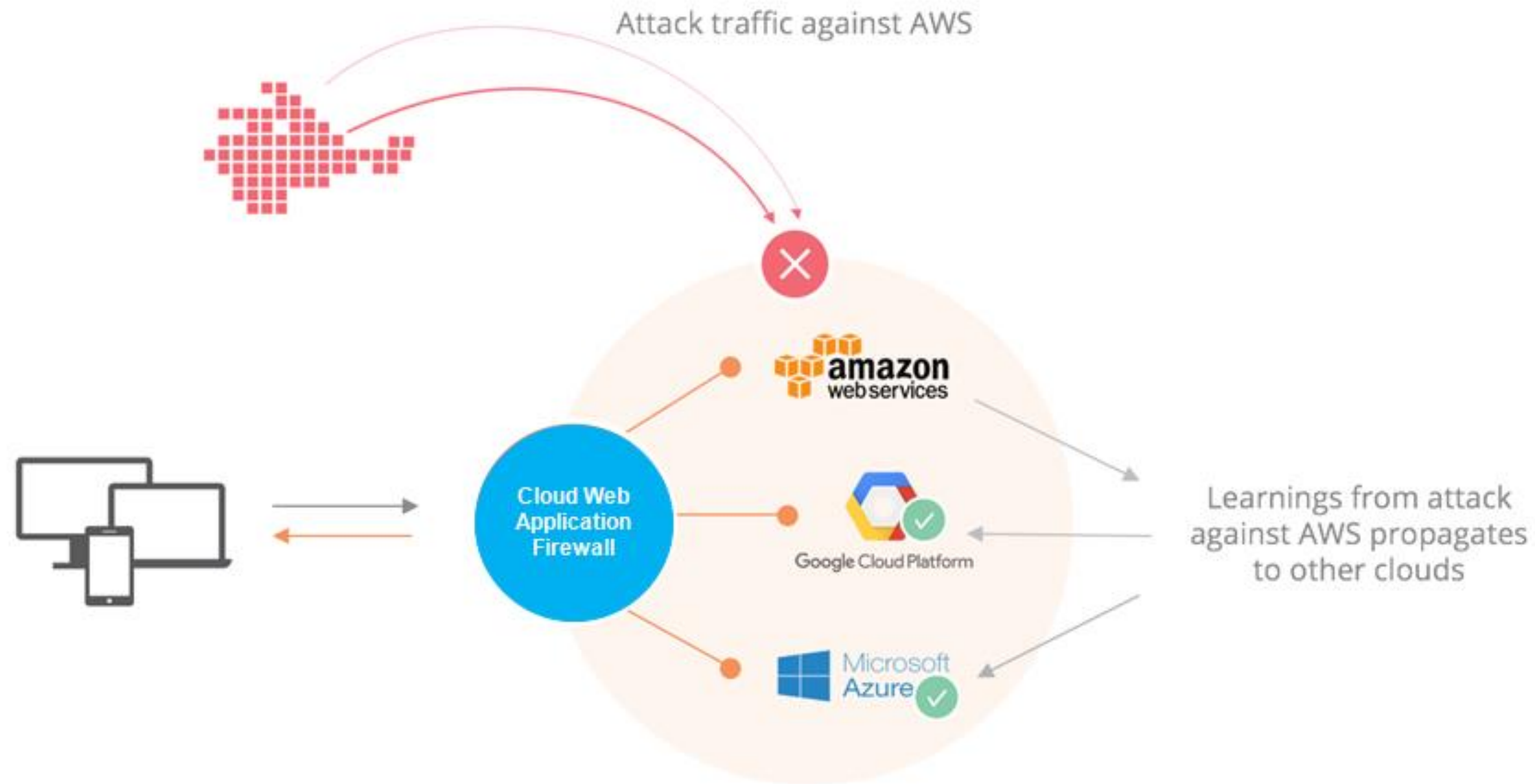
# Make Multi Cloud more resilient against DDoS attacks

- Modern attackers are now combining traditional volumetric attacks designed to overwhelm network bandwidth with stealthy application-layer attacks designed to slowly exhaust network resources over time.
- This blended approach to DDoS is growing in popularity because it is highly effective and difficult to defend.
- To combat today's full spectrum of DDoS attacks, security experts recommend a hybrid solution that integrates cloud-based mitigation and on-premise protection.
- We need to build a scalable, multi-layer DDoS defense solution by combining powerful on-premise protection for infrastructure and application-layer attacks with an on-demand cloud-based scrubbing service for volumetric attacks that otherwise overwhelm the network.





# Make Multi Cloud more resilient against DDoS attacks



Source: <https://riskemy.com/wp-content/uploads/2018/05/5-min.png>

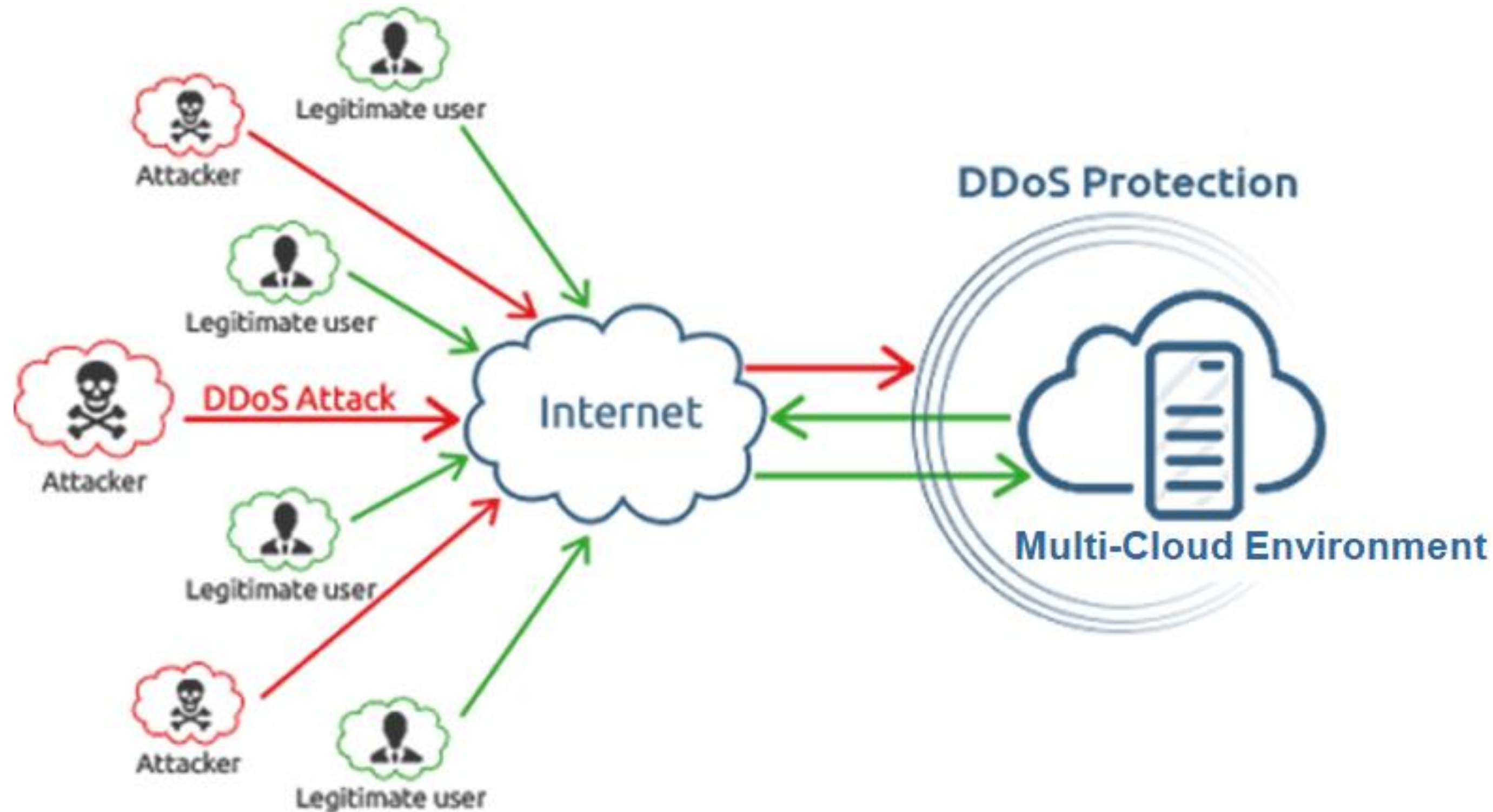


# Make Multi Cloud more resilient against DDoS attacks

- Build a comprehensive solution at the networks edge for “always on” protection against DDoS attacks. It needs to quickly and automatically detects and mitigates attack traffic.
- In the case of a high volumetric attack will traffic be rerouted to cloud-based scrubbing center before it reaches your network.
- At the scrubbing center, attack traffic is mitigated and legitimate traffic is redirected back to your network.
- When the DDoS attack has subsided, mitigation operations will revert back.
- Monitoring management and reporting system should provides browser-based management for all multi-cloud protection.



# Make Multi Cloud more resilient against DDoS attacks



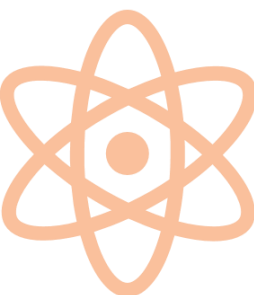
Source: <https://www.hostingfuze.net/wp-content/uploads/2018/01/ddos-protection-left-bg.png>





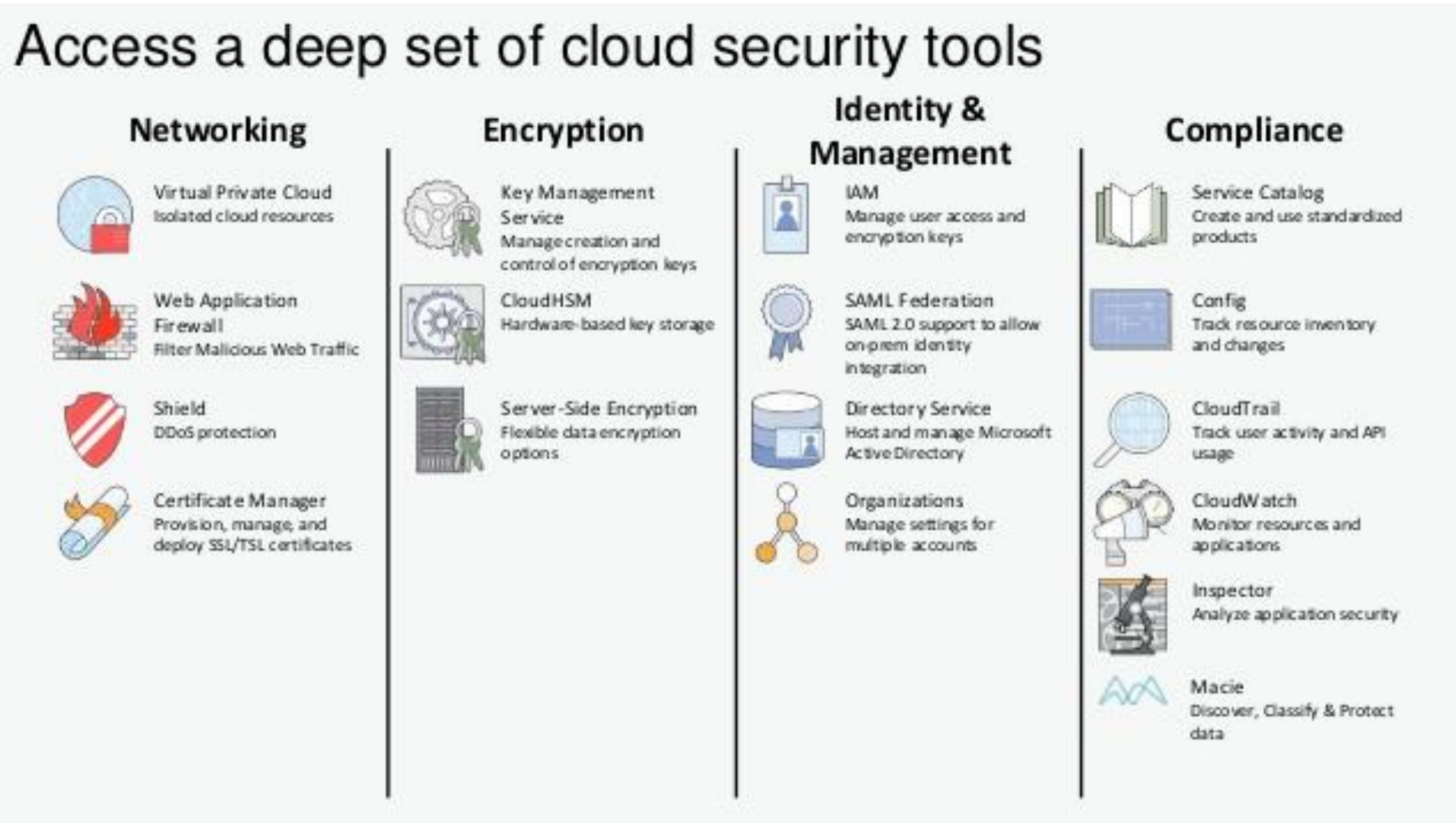
# Make Multi Cloud more resilient against DDoS attacks

- In addition, the management and reporting capabilities provided by the customer portal at the scrubbing center will be consistent with the operator's experience.
- It should give network operators complete visibility into the traffic passing through their network and a comprehensive range of tools to quickly analyze attack traffic.
- This makes the decision-making process of transferring traffic between on-premise and cloud-based scrubbing straightforward.
- In addition, a robust API that makes all functions available for integration into external systems and provides almost unlimited reporting flexibility.
- Build a layered approach to DDoS attacks enables businesses to deploy and manage best-practices defense with a single solution that integrates multi-cloud DDoS protection.



# Lab Activity

# Deploy mandatory security controls



Source: <https://image.slidesharecdn.com/magnoliaawswebinarv0-180312073152/95/how-to-get-the-most-out-of-your-cms-deployment-on-aws-17-638.jpg?cb=1520839945>



# Deploy mandatory security controls



Source: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/35243/10\\_steps\\_portrait\\_red\\_headings.png](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/35243/10_steps_portrait_red_headings.png)



 **Break**

 **10 Min**

Section 6



# Monitoring Multi-Cloud environment

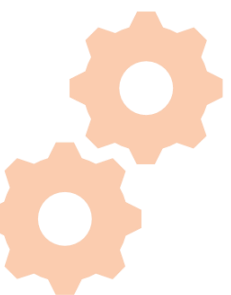


50 Min



# Goals

- ✓ Build robust multi cloud monitoring solution
- ✓ Balance your workload between various cloud vendor
- ✓ Move workloads to appropriate cloud providers
- ✓ Migrate storage from AWS and GCP to Azure

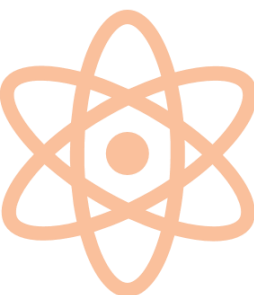




# Build robust multi cloud monitoring solution

## Get Network Monitoring Visibility Across All Your Cloud Deployments

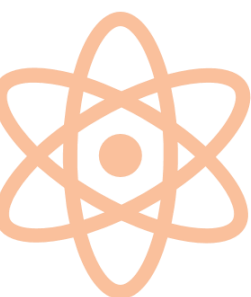
- Enterprises are adopting multi-cloud strategies to reduce vendor lock-in and access best of breed services from cloud providers like Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).
- The proliferation of modular application architectures has resulted in a complex matrix of inter-service communication across infrastructures and networks that enterprises do not own or control.
- Much of this communication traverses the Internet, which has evolved into a mission-critical transport for enterprises.
- Traditional monitoring tools rely on packet capture, flow and SNMP flatline outside the perimeter of an enterprise and can't provide insight into connectivity to, from and within public cloud services, thereby creating a visibility blind spot in multi-cloud deployments.



# Build robust multi cloud monitoring solution

## Cloud Monitoring for AWS, Azure and GCP

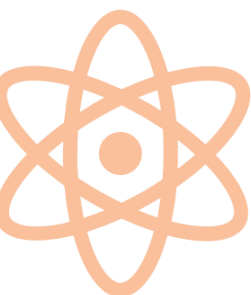
Application-aware cloud monitoring solutions for your Amazon Web Services (AWS), Microsoft Azure and Google Cloud (GCP) multi-cloud deployments.



# Build robust multi cloud monitoring solution

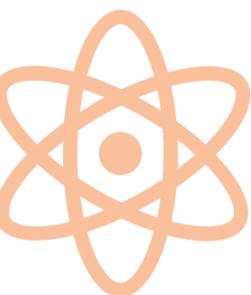
## Get Network Monitoring Visibility Across All Your Cloud Deployments

- This lack of visibility puts enterprises at risk of delivering poor digital experiences that adversely impact revenue, brand reputation and employee productivity.
- Build Network Intelligence that gives enterprises a modern answer to cloud monitoring, including the ability to measure and visualize application and network-layer performance between their hybrid cloud, private cloud and public cloud services.
- In addition to the pre-provisioned Cloud Agents, enterprises can also deploy lightweight Enterprise Agents in their own VPCs, data centers and branches for insights into hybrid cloud and private cloud environments.



# Build robust multi cloud monitoring solution

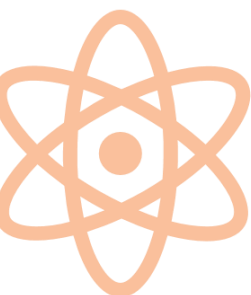
- This enables a data-driven approach from planning to deployment and operations stages of your cloud adoption journey.
- Monitoring should provide immediate visibility into application delivery, network behavior and inter-service dependencies, and their impact on digital experience.
- With multi cloud based monitoring, companies gain immediate and comprehensive visibility into every service delivery path in a multi-cloud environment, allowing them to overcome the complex operational challenges of cloud computing, accelerate cloud adoption and deliver superior digital experiences.





# Balance your workload between various cloud vendor

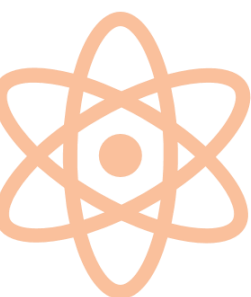
- Multi-cloud, by its very definition, means that applications and supporting services need to be agnostic to the underlying infrastructure.
- Any application should receive any service in any cloud. But that's not how most load balancers work. Most load balancers are opinionated about how and where they work.
- Software-defined architecture: centralized control and distributed data plane with elastic auto-scaling.
- Built-in analytics: actionable insights based on performance monitoring, logs and security events in a single dashboard with end-to-end visibility.
- Extensible application services: load balancing, application security, service mesh and beyond



# Balance your workload between various cloud vendor



Source: [https://blog.cloudflare.com/content/images/2018/02/Single\\_Pane\\_of\\_glass\\_Cloudflare.png](https://blog.cloudflare.com/content/images/2018/02/Single_Pane_of_glass_Cloudflare.png)



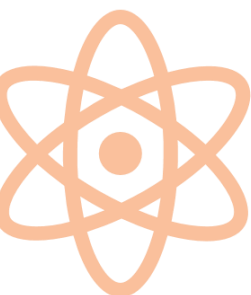
# Lab Activity



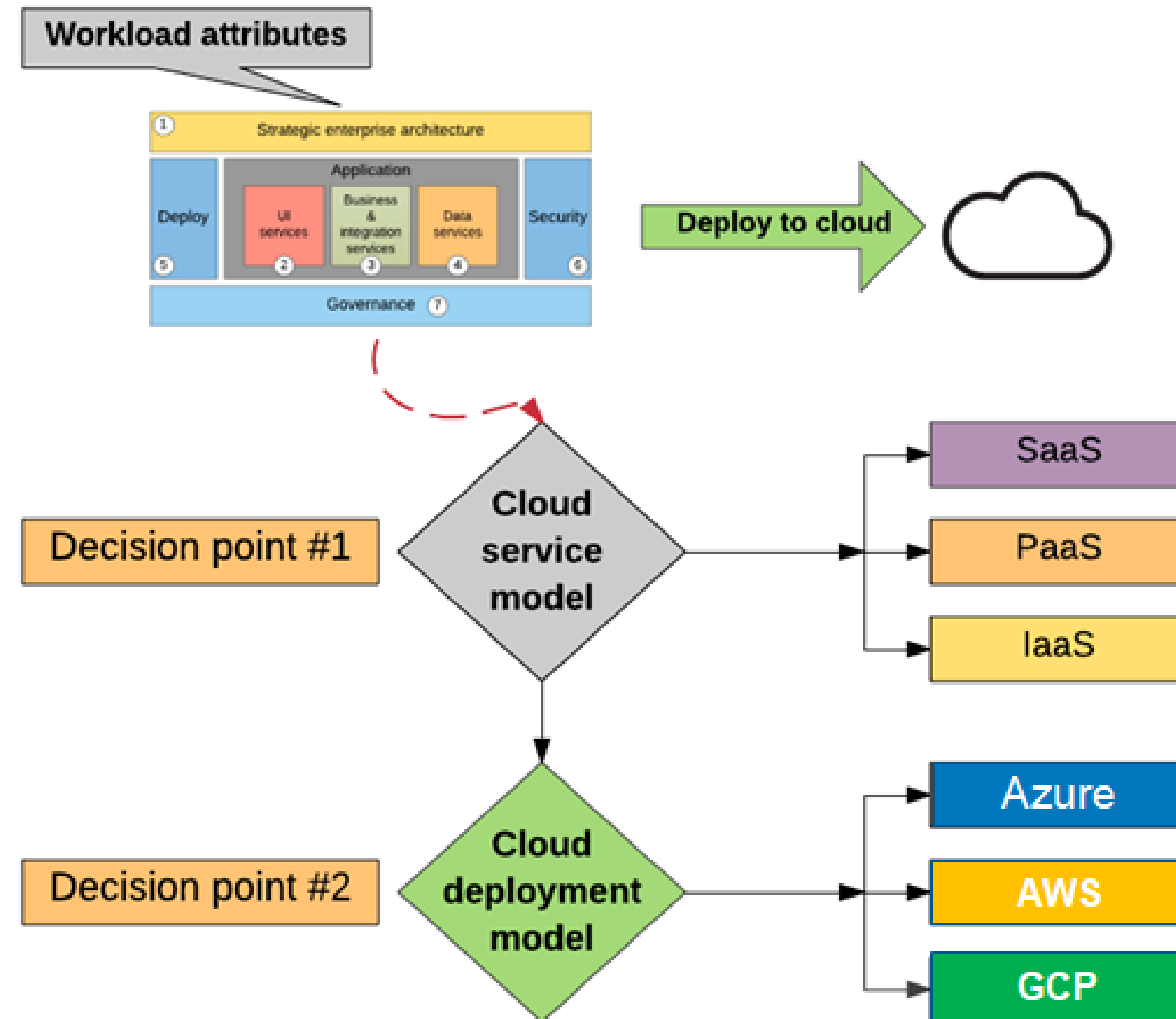
# Move workloads to appropriate cloud providers

## Prepare Resources

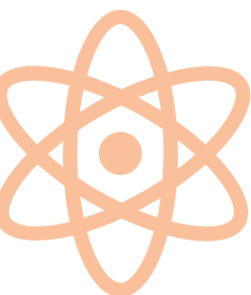
- In order to prepare for your applications to be migrated into Azure, you need to set up infrastructure components on Azure.
- You'll begin with a Site Recovery vault, as this will be the starting point for all of your ASR experiences.
- You need to deploy two IaaS VMs viz., configuration server and master target server in Azure.
- You can setup protection between on-premises physical servers and Azure to deploy these components on Azure.



# Move workloads to appropriate cloud providers

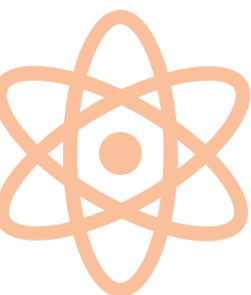


Source: <https://www.ibm.com/developerworks/library/mw-1609-fernandes-trs/figure10.png>

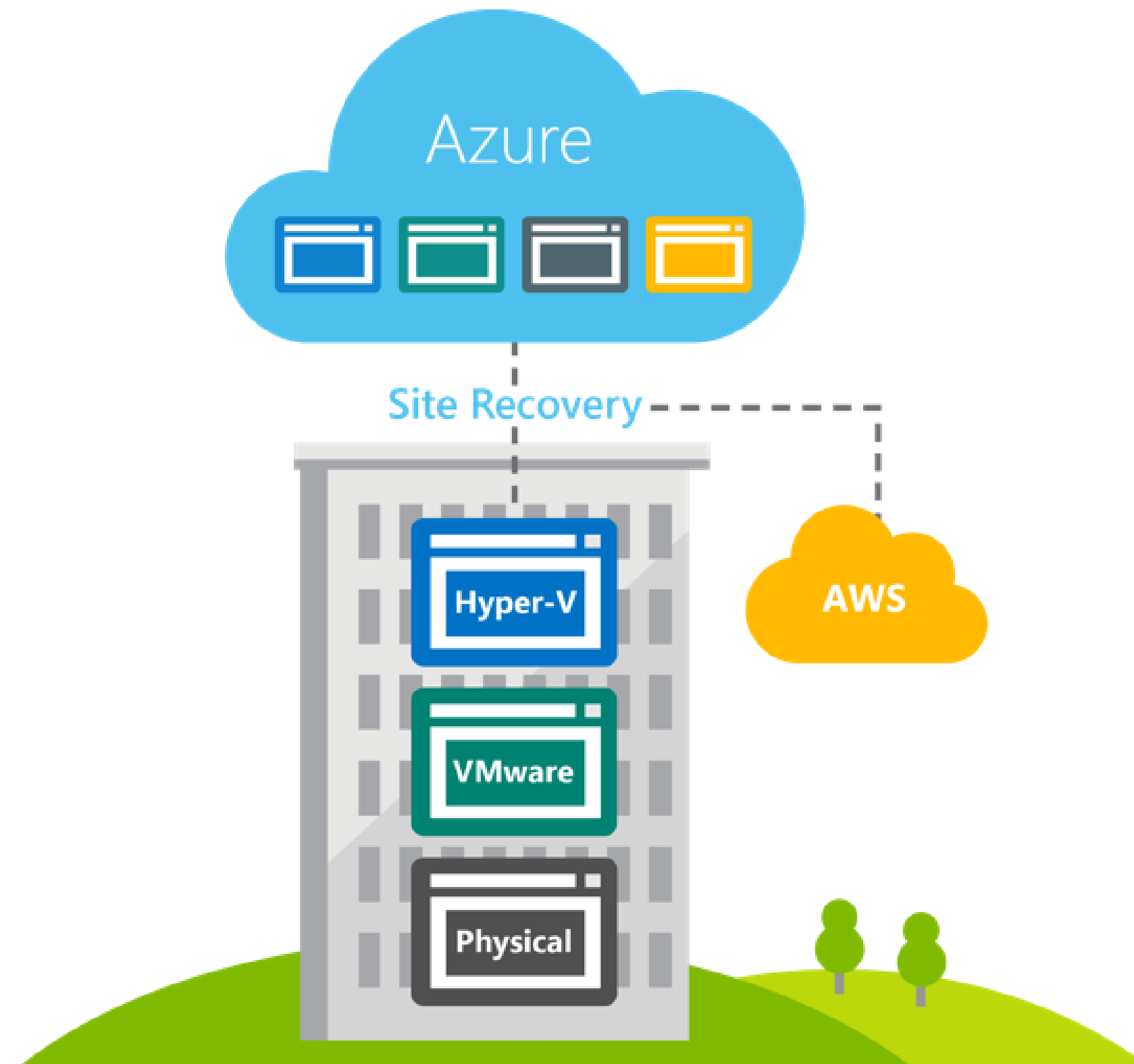


# Move workloads to appropriate cloud providers

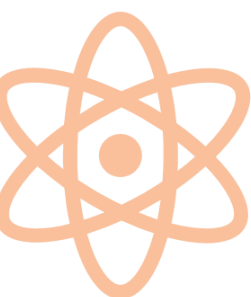
- You need to deploy an EC2 instance running the process server component. Keep the guidelines on sizing of the process server in mind when you deploy the process server.
- The process server needs access to the VMs running your application on AWS which is why it's recommended that the process server be in the same subnet as the VMs you are migrating.
- The VMs you are migrating will also need to have security group configuration that allows inbound connections on TCP and UDP ports 135-139, 445 and 1024-65535 to enable communication with the process server.
- Once you've completed this step and registered your process server with the configurations server, you are ready to move to the next step.



# Move workloads to appropriate cloud providers

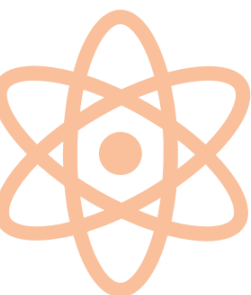


Source: [http://acom.azurecomcdn.net/80C57D/blogmedia/blogmedia/2015/07/16/ASR\\_Migration.png](http://acom.azurecomcdn.net/80C57D/blogmedia/blogmedia/2015/07/16/ASR_Migration.png)



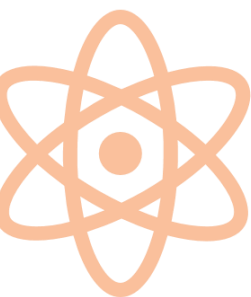
# Move workloads to appropriate cloud providers

- At this point, you can begin discovering your VMs on AWS. Start by creating a protection group and use the “add physical machine” workflow to identify all the EC2 instances that you wish to migrate to Azure.
- You can use the private IP address of the EC2 instance to discover them, you are also afforded the convenience of having a friendly name that you can refer to later.
- After this step is complete, all the VMs you identified in the previous step will begin to replicate to Azure.
- This can be a long running operation depending on the size of the virtual machines, the network capacity and the process server. Once this initial replication is successful you are ready for migration.
- Now you perform an failover action with one-click and migrate your application to Azure. Be sure to delete your EC2 instances and disable protection on ASR since these resources are no longer needed.



# Migrate storage from AWS and GCP to Azure

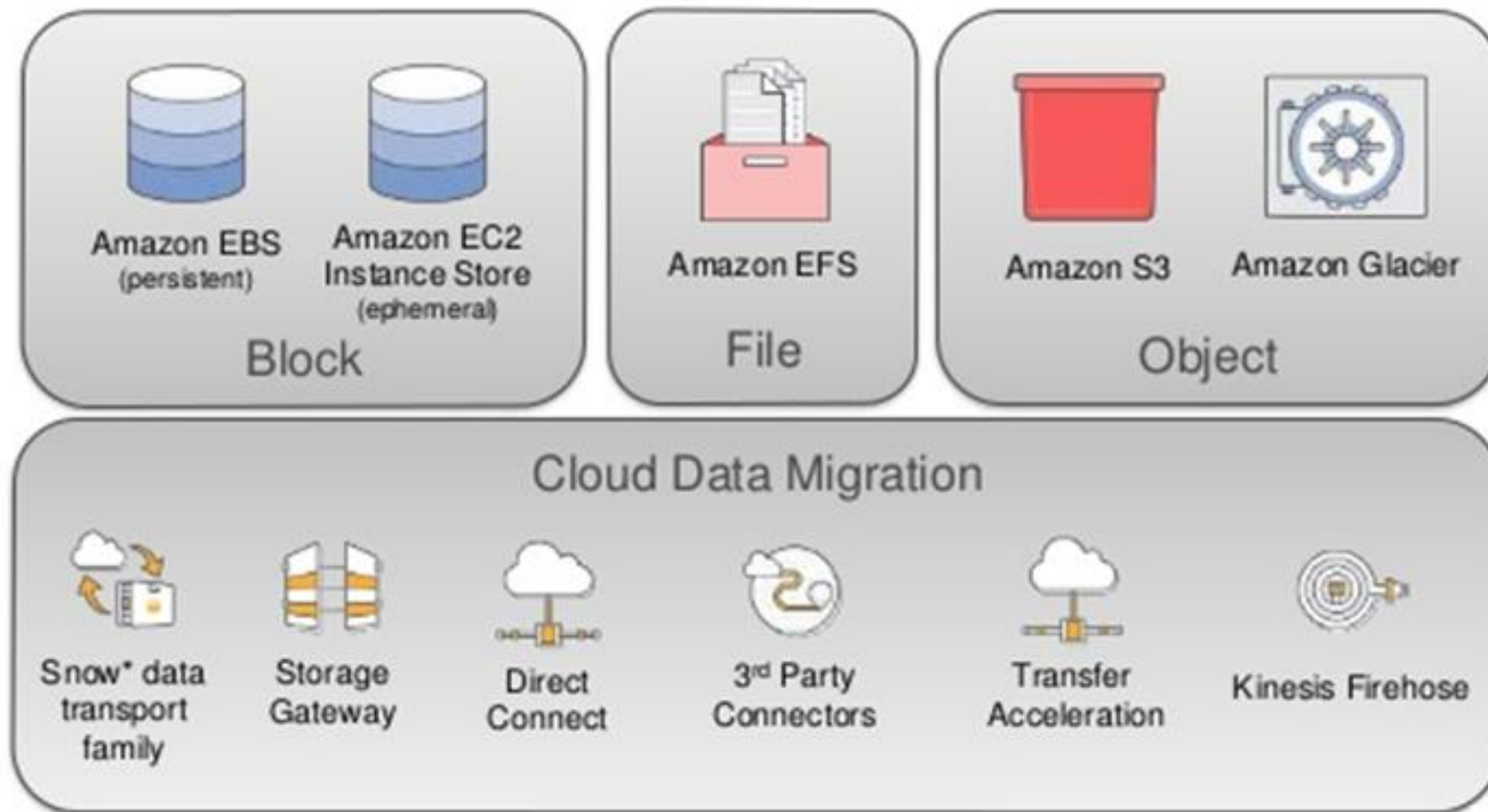
- AWS' primary offline data migration services are Snowball and Snowmobile.
- With Snowball, admins create a job in the AWS Management Console, and then AWS sends a physical disk, called a Snowball, to them.
- Users load the Snowball appliance with the data they want to migrate to the AWS public cloud. The data volumes are electronically labeled, so when the appliance arrives at AWS' facility, the vendor can load the data onto the cloud.
- AWS charges a service fee for each data transfer job with Snowball; a 50 terabyte (TB) Snowball appliance costs \$200, and an 80 TB appliance costs \$250.
- For larger data-transfer needs, AWS offers Snowmobile, an exabyte-scale data transfer service that allows users to ship up to 100 petabytes of data to an AWS facility using a 45-foot shipping container that's pulled by a truck. AWS charges for the Snowmobile service based on the amount of data stored per month in the truck.





# Migrate storage from AWS and GCP to Azure

## The AWS Storage Portfolio



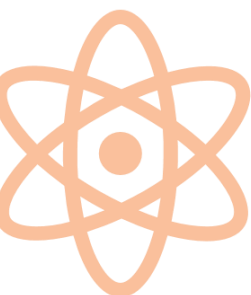
Source: <https://image.slidesharecdn.com/09262017-storage-revolutionizi-7ba9fc84-3b43-49dd-ade0-ea400d3c91c8-1417073046-170926220001/95/revolutionizing-backup-recovery-using-amazon-s3-aws-online-tech-talks-11-638.jpg?cb=1506463212>



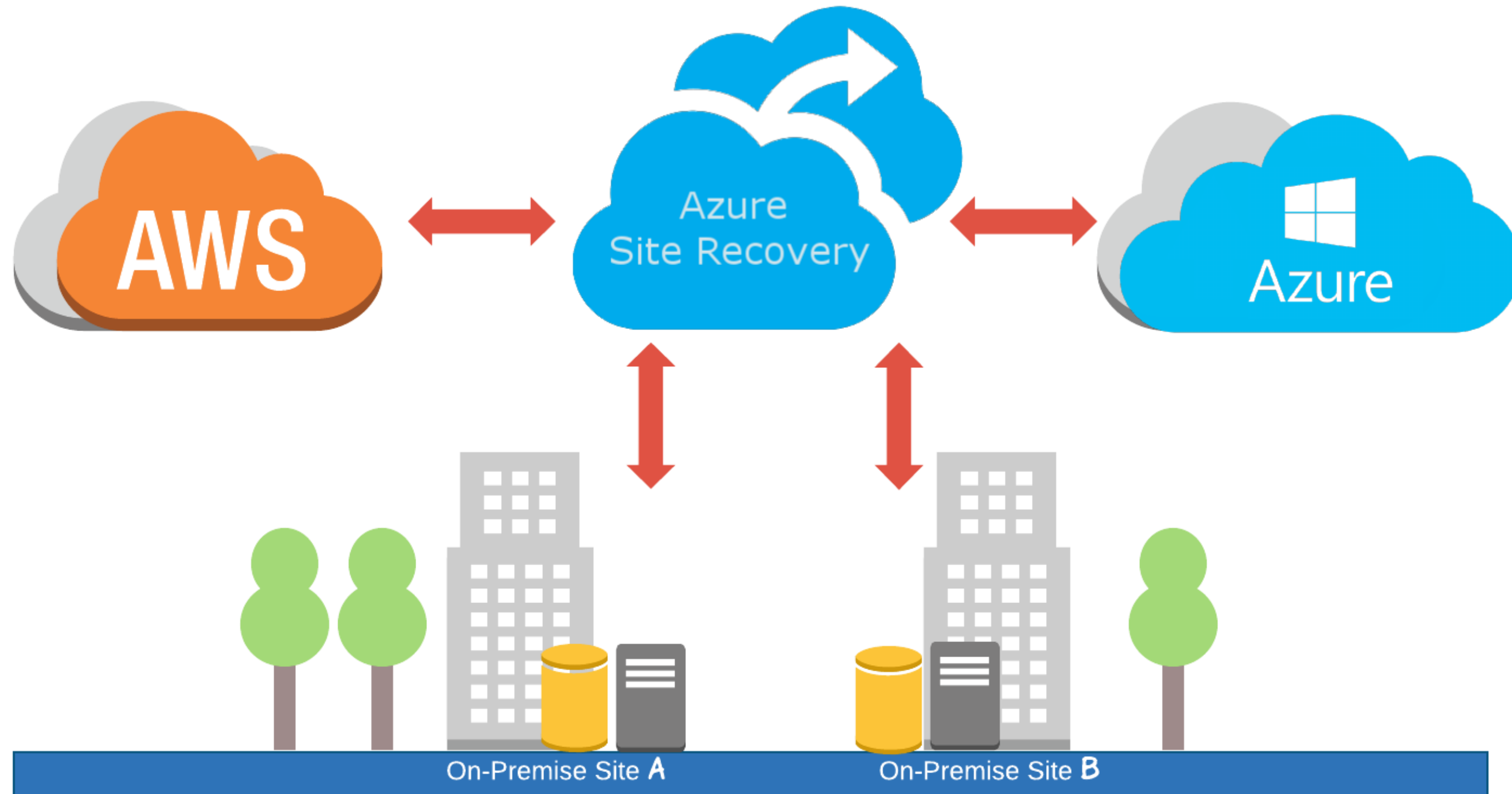


# Migrate storage from AWS and GCP to Azure

- Microsoft Azure provides a service similar to AWS Snowball, called Import/Export service, but doesn't provide users with the physical disks.
- Instead they must supply their own, and follow these requirements:
- Use 2.5-inch solid-state drives (SSDs) or 2.5-inch or 3.5-inch SATA II or SATA III internal hard drives.
- When copying data to the hard drive, attach it directly using a 2.5-inch SSD or 2.5-inch or 3.5-inch SATA II or SATA III connector, or attach it externally using an external 2.5-inch SSD or 2.5-inch or 3.5-inch SATA II or III USB adaptor.
- Hard drives can be up to 10 TB.
- For import jobs, Microsoft will only process the first data volume on the drive.
- Users must format their data volume with the NT file system.
- Microsoft charges an \$80 fee for each storage device, and recommends users download the latest version of the WAImportExport tool. This tool copies your data volumes to the physical drives you purchase.



# Migrate storage from AWS and GCP to Azure

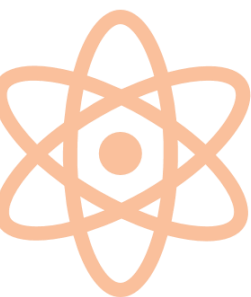


Source: [https://cdn-images-1.medium.com/max/1600/0\\*UjzkCwBiUpqKYPLT](https://cdn-images-1.medium.com/max/1600/0*UjzkCwBiUpqKYPLT).

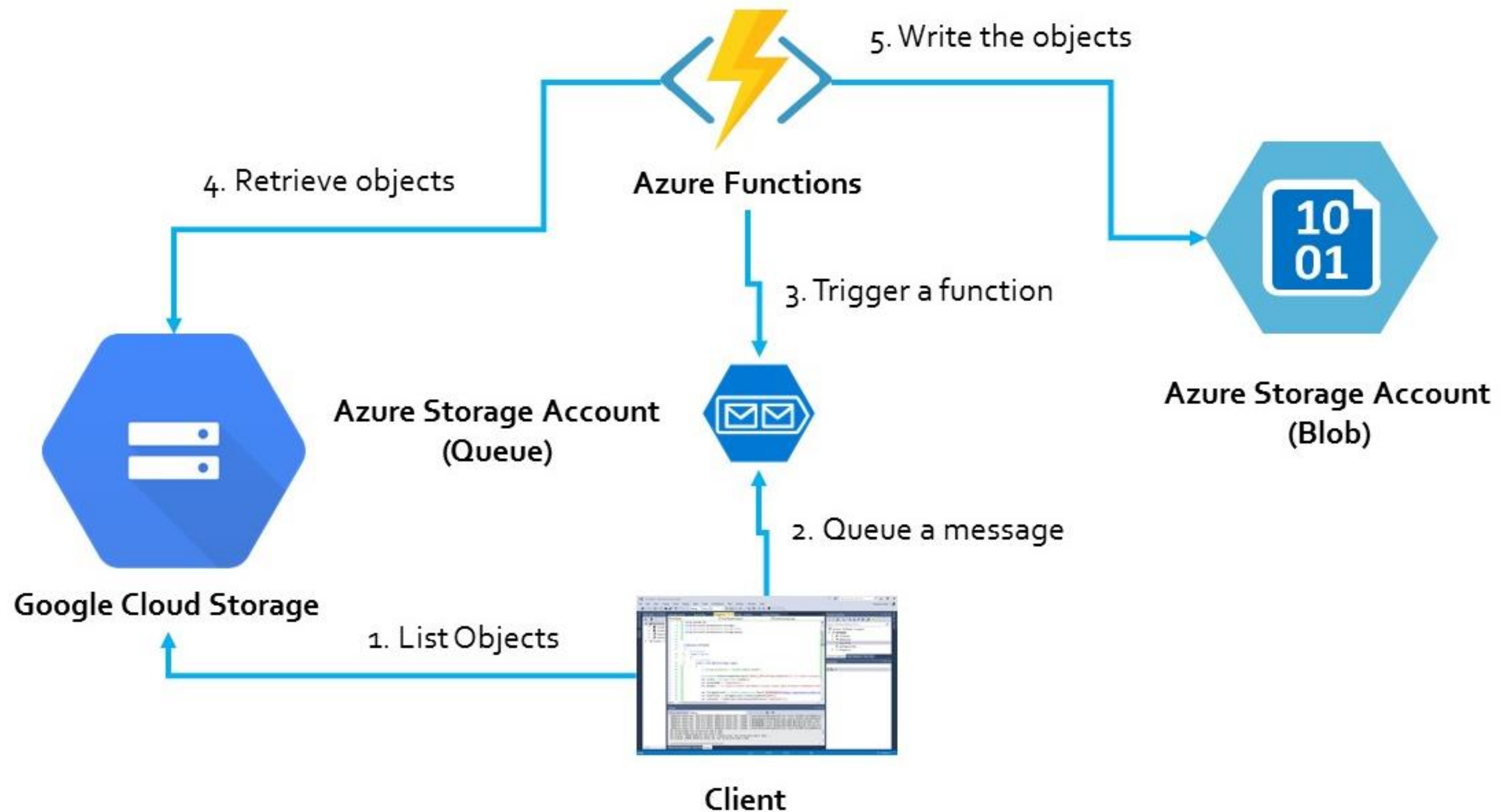


# Migrate storage from AWS and GCP to Azure

- Google's Offline Media Import/Export involves a third-party vendor, but functions similar to the offline data migration services from AWS and Microsoft.
- In this case, enterprises send their storage appliance to a third-party service provider, who then uploads the data to Google's cloud.
- Enterprises are required to make their own arrangements for Offline Media Import/Export with the third-party provider they select, rather than do so through Google.
- These providers include Iron Mountain for North America, and Prime Focus Technologies for Europe, the Middle East and Africa, as well as Asia Pacific regions.



# Migrate storage from AWS and GCP to Azure



Source: <https://msdnshared.blob.core.windows.net/media/2017/01/Hackfestxenodataarchitecture.jpg>



 **Break**

 **10 Min**

Section 7



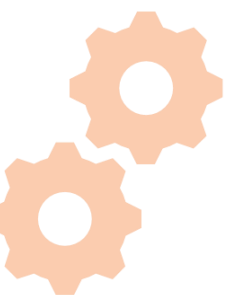
# Troubleshooting Multi-Cloud platform



50 Min

# Goals

- ✓ Troubleshooting multi cloud environment
- ✓ Setup alerting in multi cloud environment
- ✓ Industry best practices for multi cloud platform
- ✓ Sample multi cloud deployment architectures





# Troubleshooting multi cloud environment

## Troubleshooting connectivity

**Symptom:-** An attempt to connect to a server fails. An attempt to connect between Cloud Servers and another cloud service fails.

Test 1	Diagnosis 1
Try reaching the same server from different network locations, devices, and directions.	If any method succeeds in connecting to the server, the problem is not in the server itself but in some aspect of the network.
Test 2	Diagnosis 2
Try to access the server by its IP address (for example, 192.0.2.0) instead of its DNS entry (for example, <a href="http://www.example.com">www.example.com</a> ).	If the server is accessible by its IP address but not by its DNS entry, the problem relates to the DNS rather than to the server itself.
Test 3	Diagnosis 3
Try to confirm basic TCP/IP connectivity by using telnet.	If you cannot telnet to a target IP through a target port, a firewall may be blocking your access.

# Troubleshooting multi cloud environment

## Troubleshooting server builds

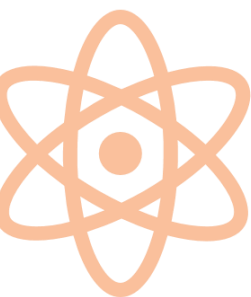
**Symptom:-** A cloud server build takes an unusually long time to complete.

Test	Diagnosis
<ul style="list-style-type: none"><li>• Windows servers take longer to build than servers running other operating systems.</li><li>• Servers built with backup enabled take longer to build than normal servers.</li><li>• Servers built from customer-saved images take longer to build than servers built from images.</li></ul>	<ul style="list-style-type: none"><li>• If any of these known causes of slower builds are true of the server that you are attempting to build, wait at least thirty minutes before rechecking for success or failure. Although build times vary, all server builds eventually either succeed or fail.</li><li>• If a slow server build eventually succeeds, use the new server normally. A slow build does not predict any operational problems.</li><li>• If a slow server build eventually fails, investigate the failure just as you would if it had failed quickly.</li></ul>

# Industry best practices for multi cloud platform

## 1. Prepare with realistic goals

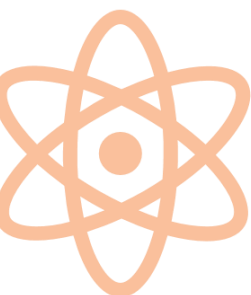
- Preparation is key to being in a position from which you can take advantage of multicloud benefits.
- Be sure to understand which platform works best for each application and prioritize your requirements when there is no exact match.
- You will need to have the right people with the right skill sets to migrate to a multi cloud environment successfully, and have goals for 12 months, 24 months, and 36 months down the line.
- These goals should be flexible in order to account for the evolving cloud landscape.



# Industry best practices for multi cloud platform

## 2. Secure the network

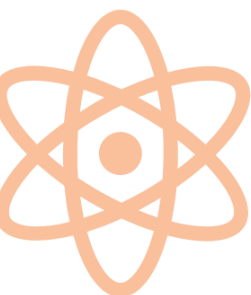
- Many companies operating in a single cloud environment adopt the “castle and moat” approach to network security by securing the perimeters of their networks and then assuming traffic within the network is acceptable.
- With a multicloud strategy you cannot do that because you no longer control the network perimeter, so you have to secure the inside of the network as well.
- Companies that have re-thought their approaches to network security have found their whole IT environments have become more secure.



# Industry best practices for multi cloud platform

## 3. Collect and consolidate data

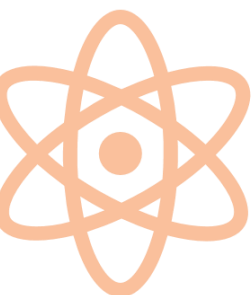
- In order to collect and consolidate data across multiple clouds, you need to have a cloud management platform capable of accessing data from all sources and consolidating the data so you can view it across a single pane display.
- Companies that struggle with multi cloud adoption often rely on cloud provider supplied management tools and reporting systems—creating disparate data sets that make it difficult to gain clear visibility into your cloud ecosystem.



# Industry best practices for multi cloud platform

## 4. Evaluate environments as one

- Multicloud management platforms not only give you a clear picture of your cloud ecosystem, they also enable you to evaluate multiple cloud environments as if they were one.
- This helps you better identify inefficiencies and security concerns, and define governance.
- A further advantage of having all your data in one place is that trend analyses are more accurate, leading to more accurate forecasting, planning and budgeting.
- Reporting is also simplified to help you quickly answer questions about usage, performance, security, and cost.

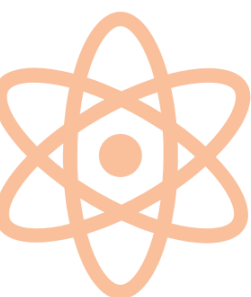




# Industry best practices for multi cloud platform

## 5. Rightsize and optimize

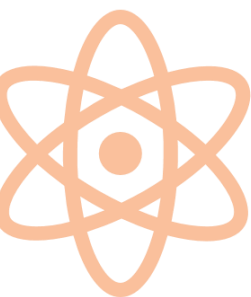
- This is an important best practice in any type of cloud environment, and is much harder without a complete set of metrics giving your total visibility of your multicloud environment.
- Without total visibility, it is harder to identify zombie assets and over-provisioned resources.
- However, optimizing is not only about reducing costs.
- You also need to optimize performance as well—a task made more difficult if different components of the same application are hosted on different clouds.
- A multicloud management platform can help you better understand your assets.



# Industry best practices for multi cloud platform

## 6. Schedule tasks when you can

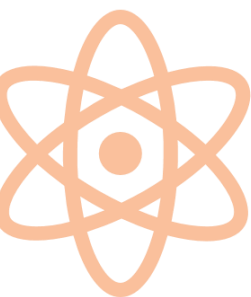
- Scheduling scripts is a standard best practice across companies with a presence in the cloud, as it creates a regular pattern for analyzing resource usage and investigating non-critical security events.
- Scheduling start-stop times for non-production resources can also significantly reduce cloud costs.
- Leaving non-production resources running when they are not required is one of the biggest contributors to cloud waste, and whereas writing scheduling scripts is one solution to this issue, scheduling start-stop times via a cloud management platform is more cost-efficient and flexible.



# Industry best practices for multi cloud platform

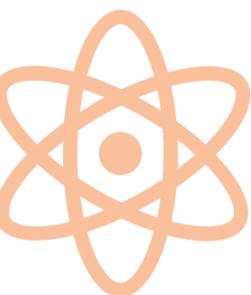
## 7. Automate wherever possible

- Managing a multicloud environment is not easy, therefore it is in your best interest to take advantage of policy-driven automation wherever possible.
- By creating policies that alert you to increasing costs, over/underutilized resources and asset misconfiguration, the management role is simplified.
- Policy-driven automation can also resolve concerns about employees failing to comply with cloud security policies.



# Sample multi cloud deployment architecture

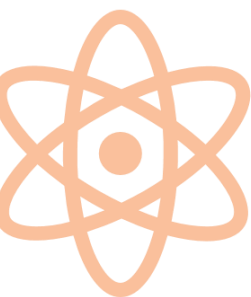
- Multi-cloud strategy is the concomitant use of two or more cloud services such as AWS, Azure, Google Cloud and more.
- This means you can use Google cloud to serve your US users and Microsoft Azure for your customers in Europe.
- Or you might use Azure SQL for your databases and Cognito for user management while using AWS EC2 instances and Load Balancing, all for a single application.
- In addition, you can run your app primarily on Digital Ocean but is completely replicated and backed up on AWS.
- You can run different app on different clouds. You can have your development and test environments on one cloud, and your production environment on another.



# Sample multi cloud deployment architecture

## Cloudification

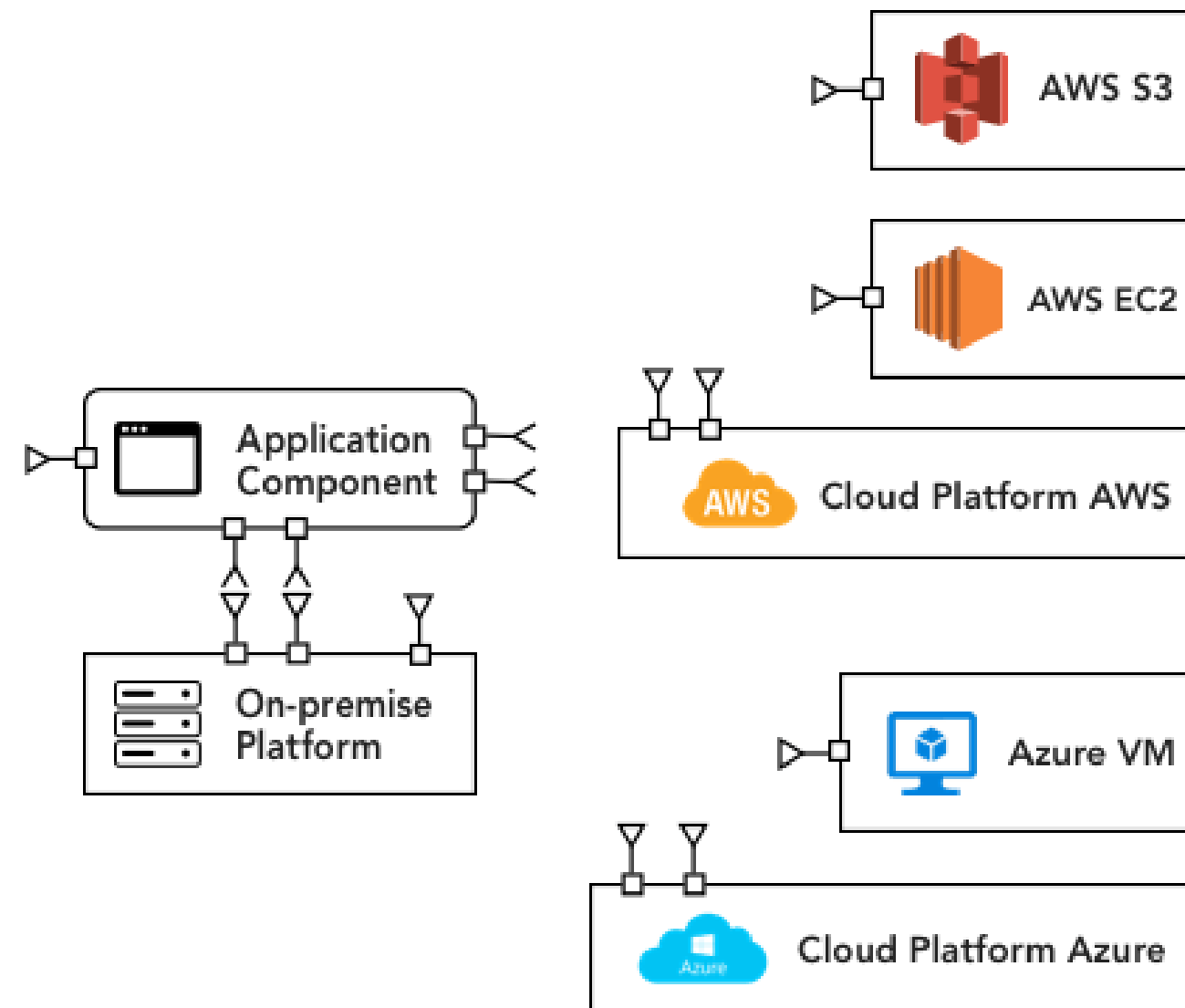
- In this architecture application component is hosted on-premise and after migration, it can use different cloud services of other cloud platforms to improve performance.
- Here application component C1 is been hosted on-premise but after adopting multi-cloud, it uses AWS storage service AWS S3 and for compute it uses Azure virtual machines.
- **Benefits:** Improves availability as application re-hosting in multiple cloud platforms and avoid vendor lock-in.



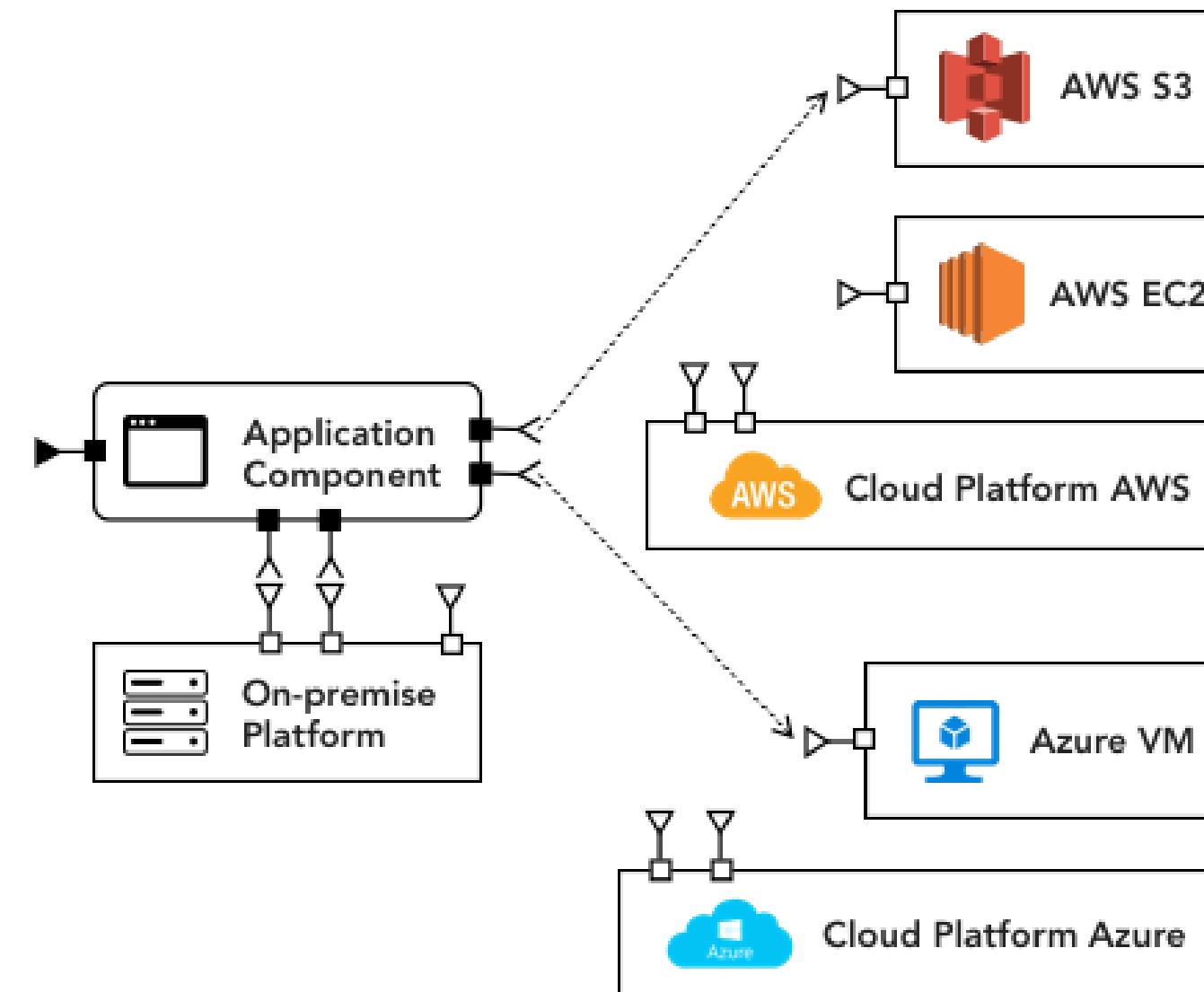
# Sample multi cloud deployment architecture

## Cloudification

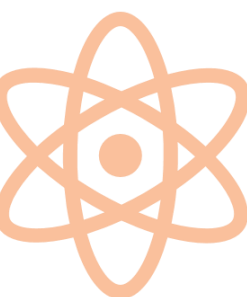
### Before Migration



### After Migration



Source: <https://www.simform.com/wp-content/uploads/2017/11/Cloudification-2.png>

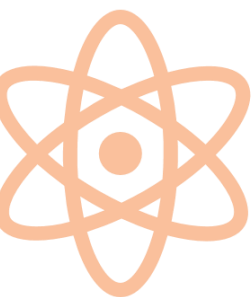




# Sample multi cloud deployment architecture

## Multi-Cloud Relocation

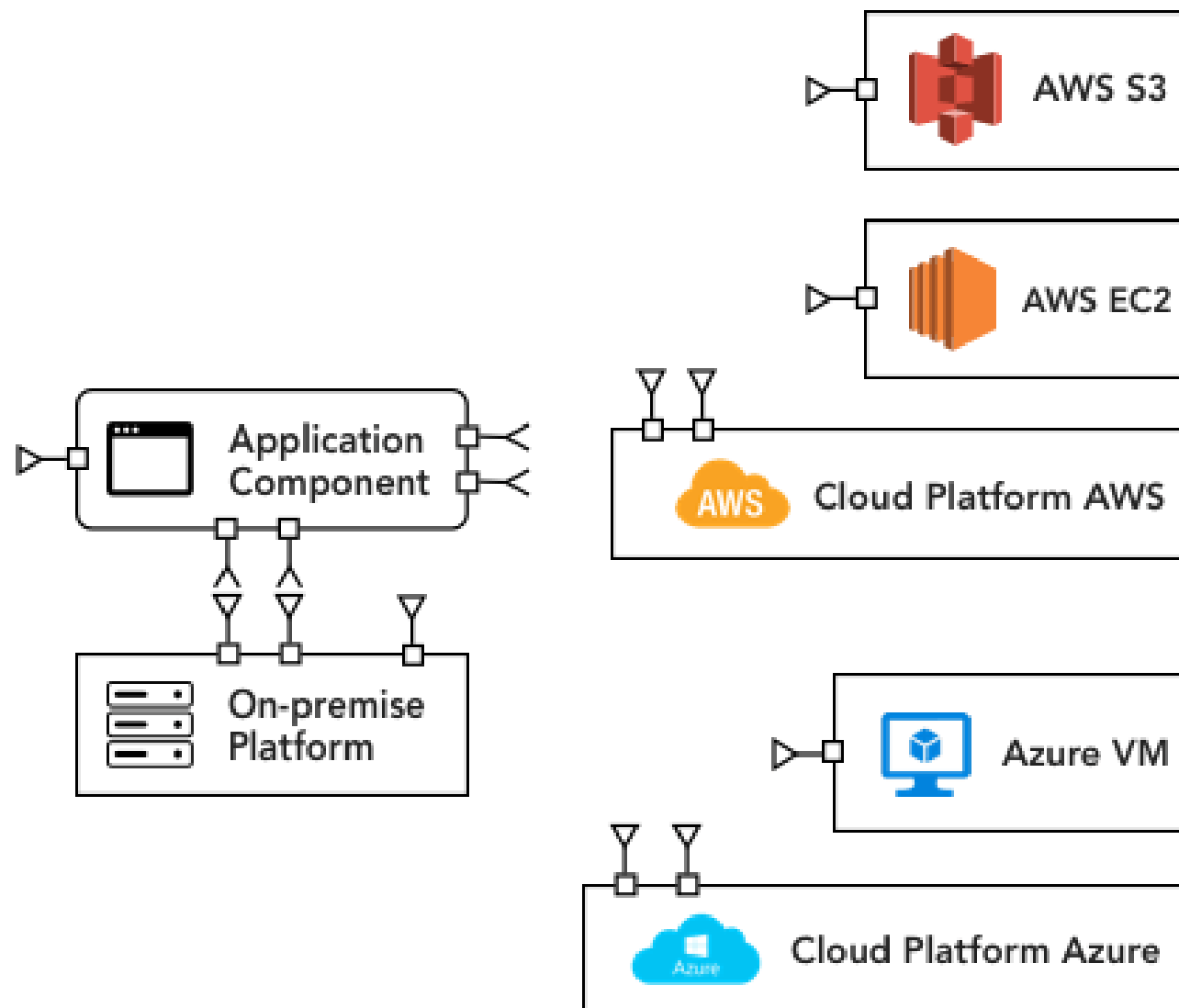
- In this architecture application component is re-hosted on cloud platform and use other cloud services of multiple cloud platform to enhance capabilities.
- Here application component C1 is re-hosted on AWS platform after migration and open to use environmental services of Azure. It is using AWS S3 for storage and has option available for compute either AWS or Azure.
- **Benefits:** Improves availability as application re-hosting in multiple cloud platforms and avoid vendor lock-in.



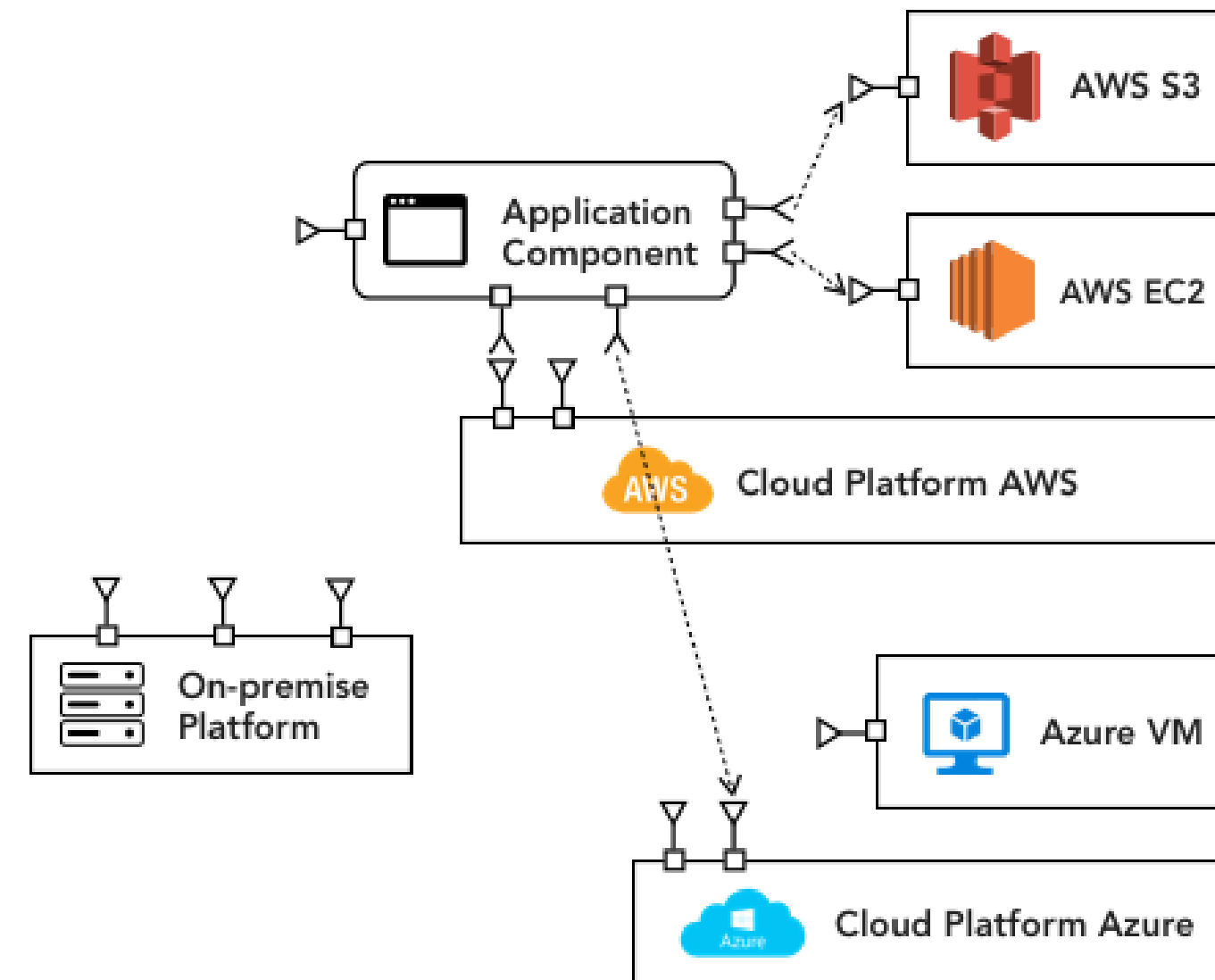
# Sample multi cloud deployment architecture

## Multi-Cloud Relocation

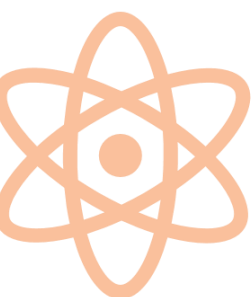
Before Migration



After Migration



Source: <https://www.simform.com/wp-content/uploads/2017/11/Cloudification-4.png>



# Sample multi cloud deployment architecture

## Multi-Cloud Refactor

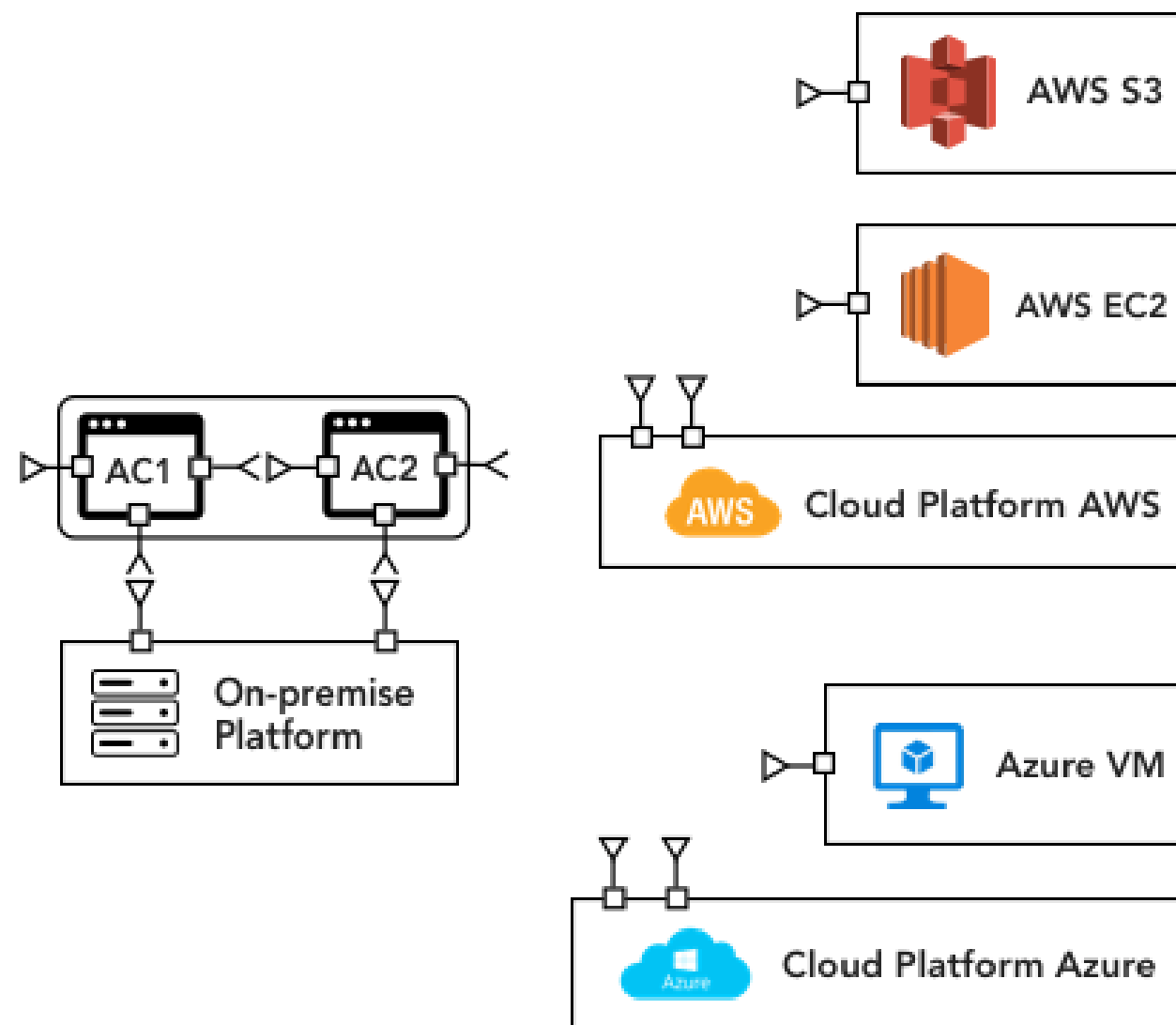
- To provide better QoS, An on-premise application is re-architected for deployment on multiple cloud platforms.
- Here application needs to re-architected as fine-grained components so that deployment of high-usage components can be optimized independently.
- Here deployment of high-usage components is optimized independently of low-usage ones. The parallel design enables better throughput to multi cloud platforms.
- Here AC1 and AC2 are two application components hosted on-premise before migration. As both the components are independent integrity units, AC1 is deployed on AWS using AWS S3. On the other hand, AC2 is deployed on Azure and it can use any Azure's cloud service as per requirements.
- **Benefits:** Optimal scalability/performance, range of multi-cloud deployment options, agility to respond to business/IT change.



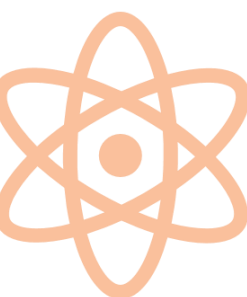
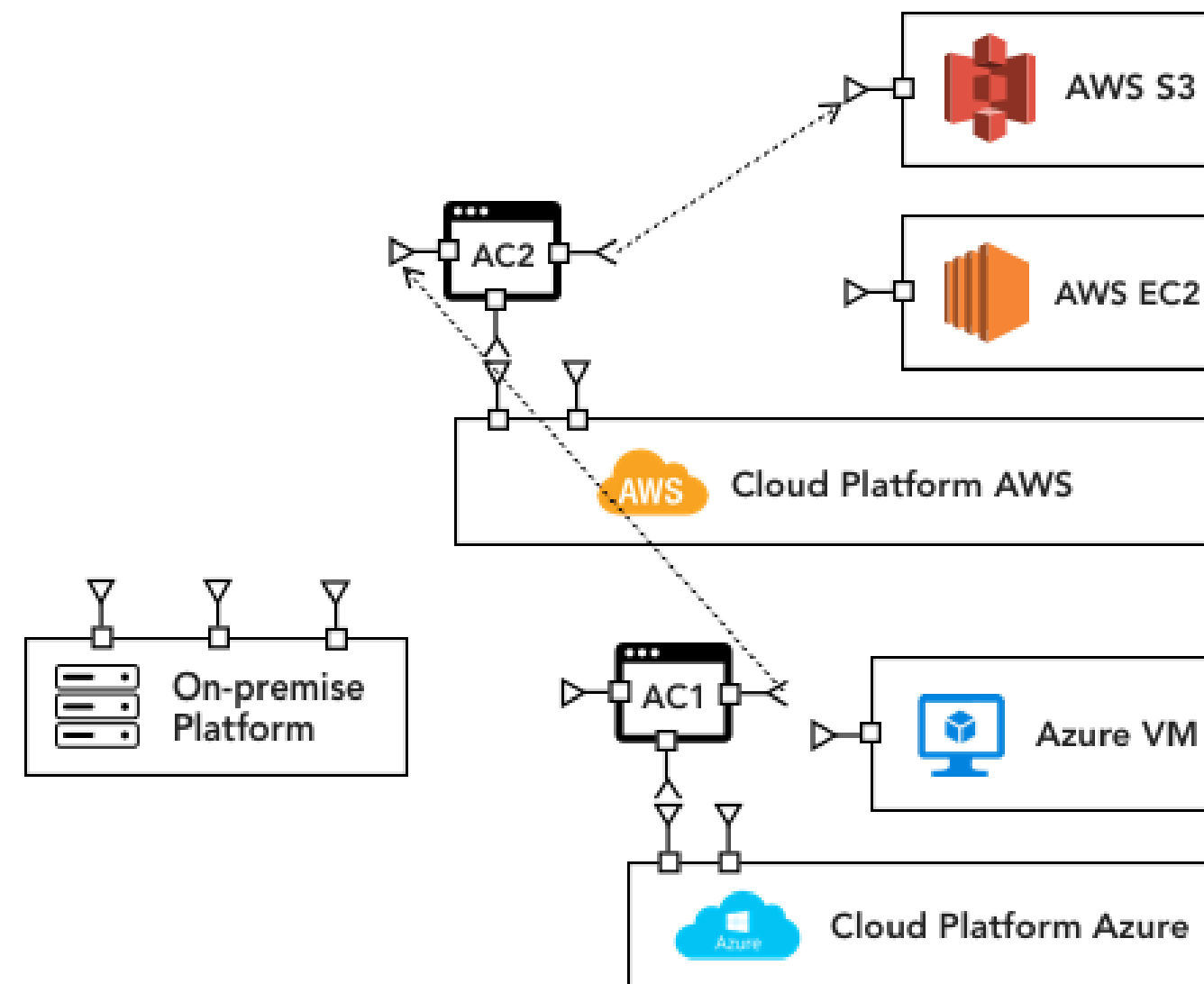
# Sample multi cloud deployment architecture

## Multi-Cloud Refactor

Before Migration



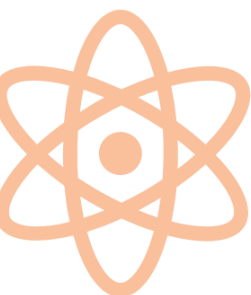
After Migration



# Sample multi cloud deployment architecture

## Multi-Cloud Rebinding

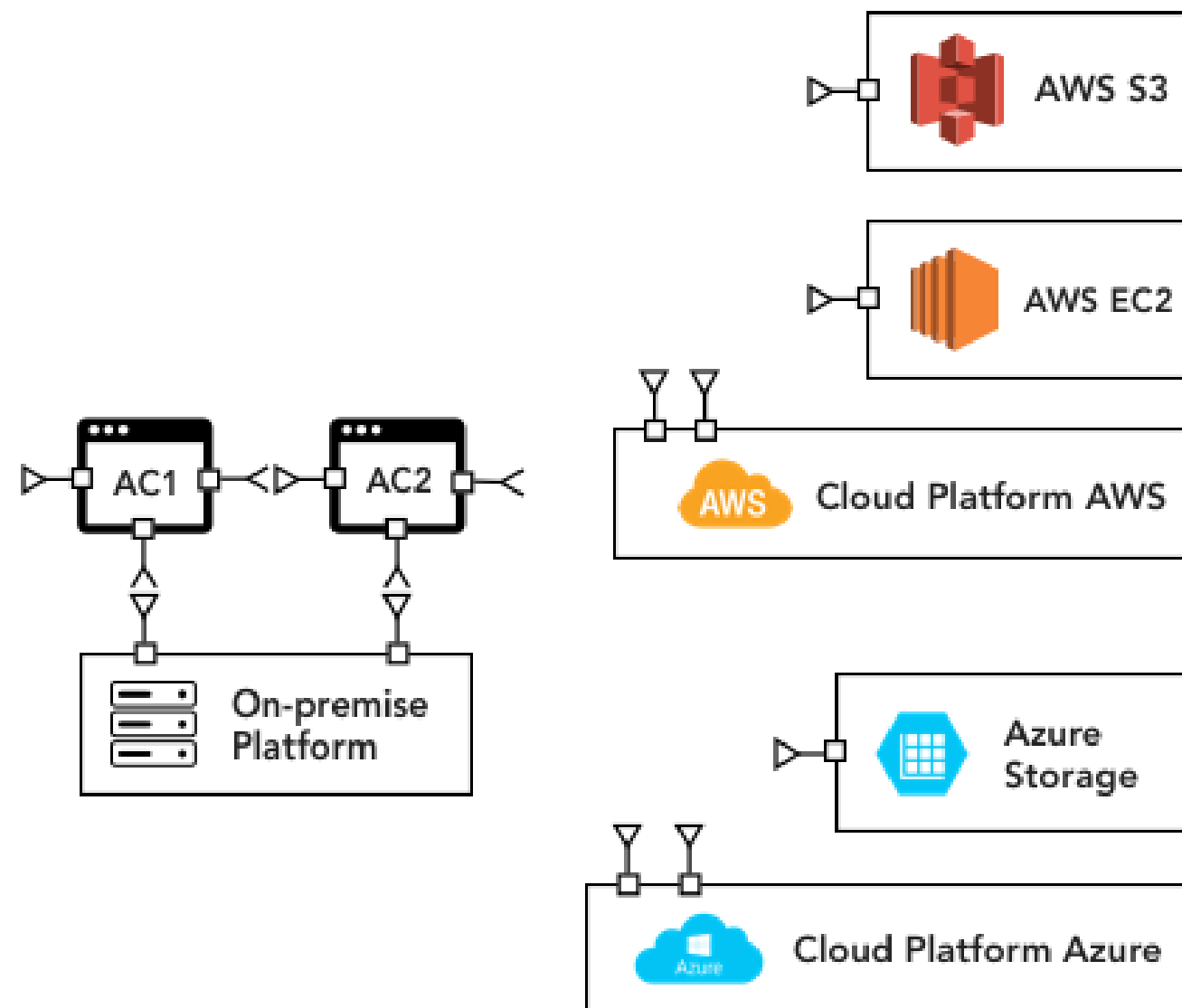
- A re-architected application is deployed partially on multiple cloud environments and enables the application to continue to function using secondary deployment when there is a failure with the primary platform.
- Here AC1 and AC2 are two application components hosted on-premise before migration. As both the components are independent integrity units, AC1 remains on-premise while two AC2 are deployed on AWS and Azure for disaster recovery. AC1 and two AC2 components are connected via EBS or Service bus.
- **Benefits:** As unhealthy services become healthy again, traffic can be delivered, returning system responsiveness to maximum.



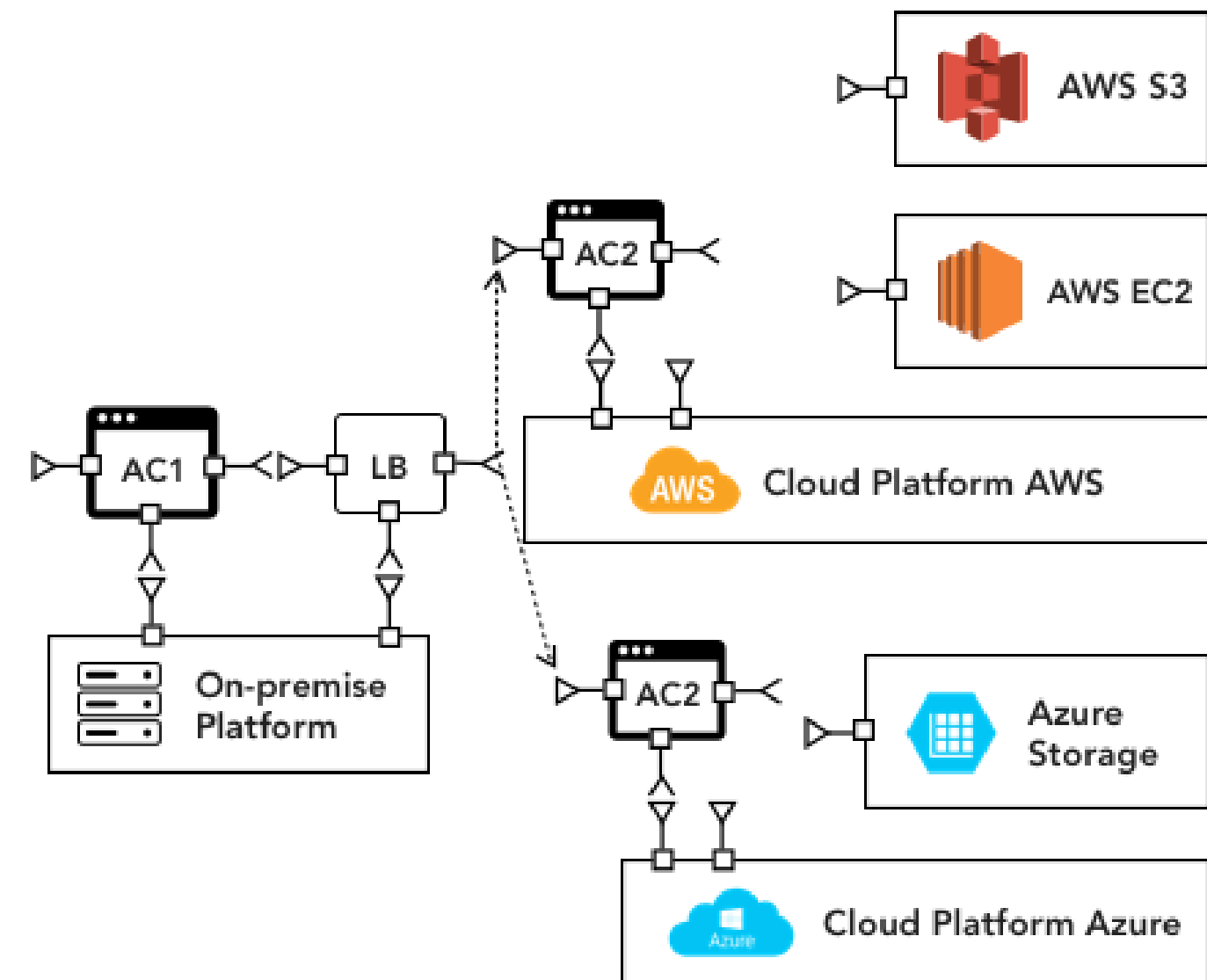
# Sample multi cloud deployment architecture

## Multi-Cloud Rebinding

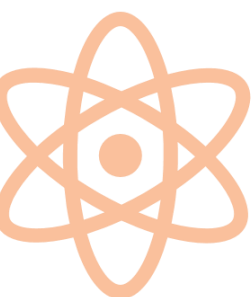
Before Migration



After Migration



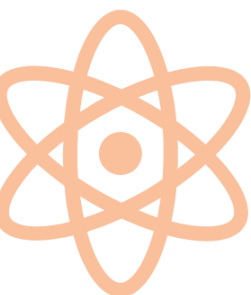
Source: <https://www.simform.com/wp-content/uploads/2017/11/Cloudification-10.png>



# Sample multi cloud deployment architecture

## Multi-Cloud Rebinding with Cloud Brokerage

- A re-architected application is deployed partially on multiple cloud environments. This enables the application to continue to function using secondary deployment when there is a failure with the primary platform using cloud brokerage services.
- In this architecture AC1 has been deployed on-premise and two re-architected AC2 are deployed on two cloud platforms AWS and Azure. Here Cloud broker services integrates all three components and provides flexibility to choose services from multiple providers (Cloud platforms AWS and Azure).
- **Benefits:** As unhealthy services become healthy again, traffic can be delivered, returning system responsiveness to maximum.

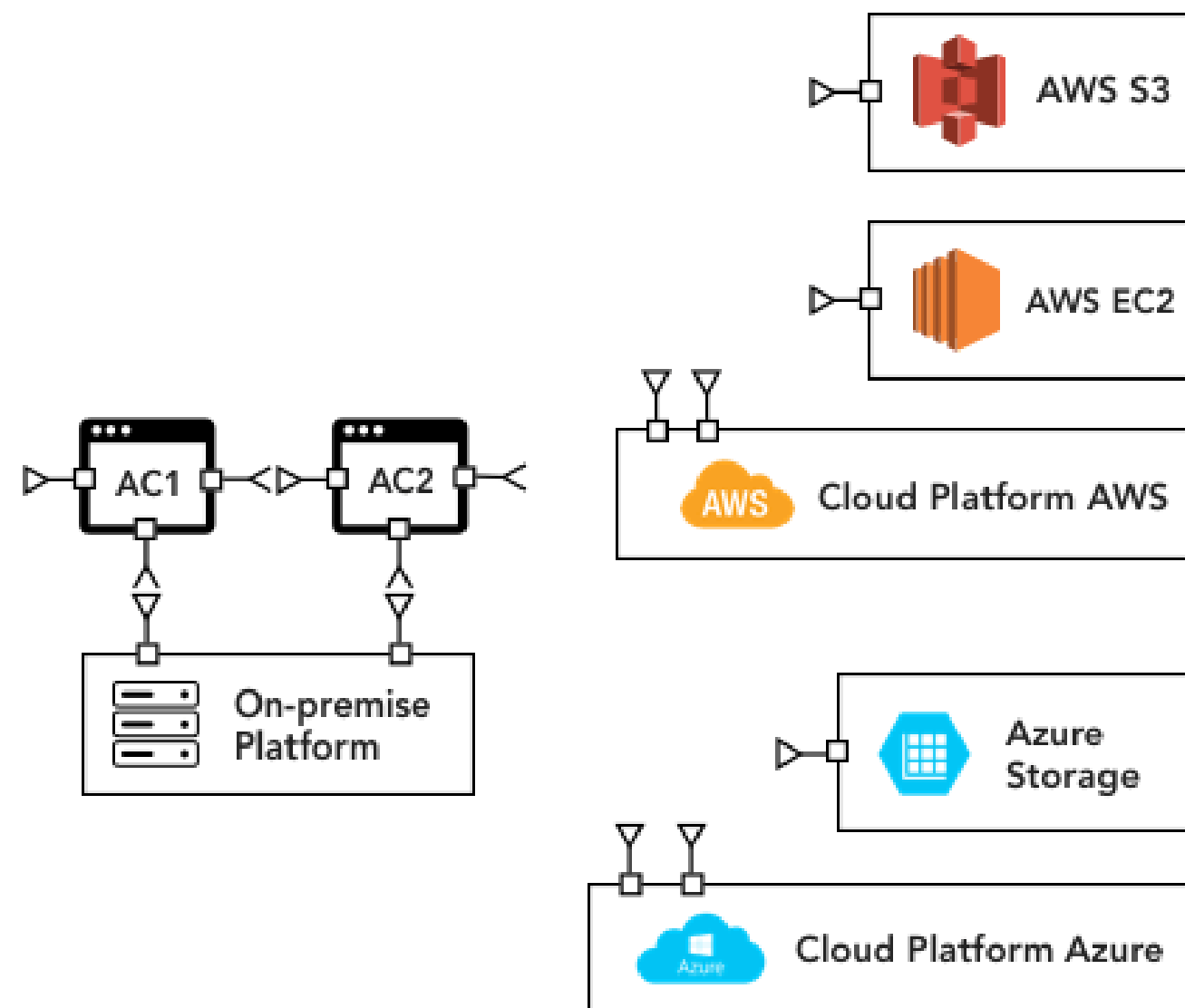




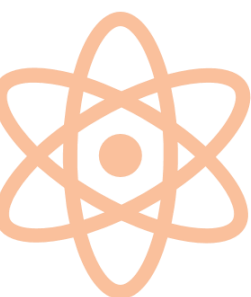
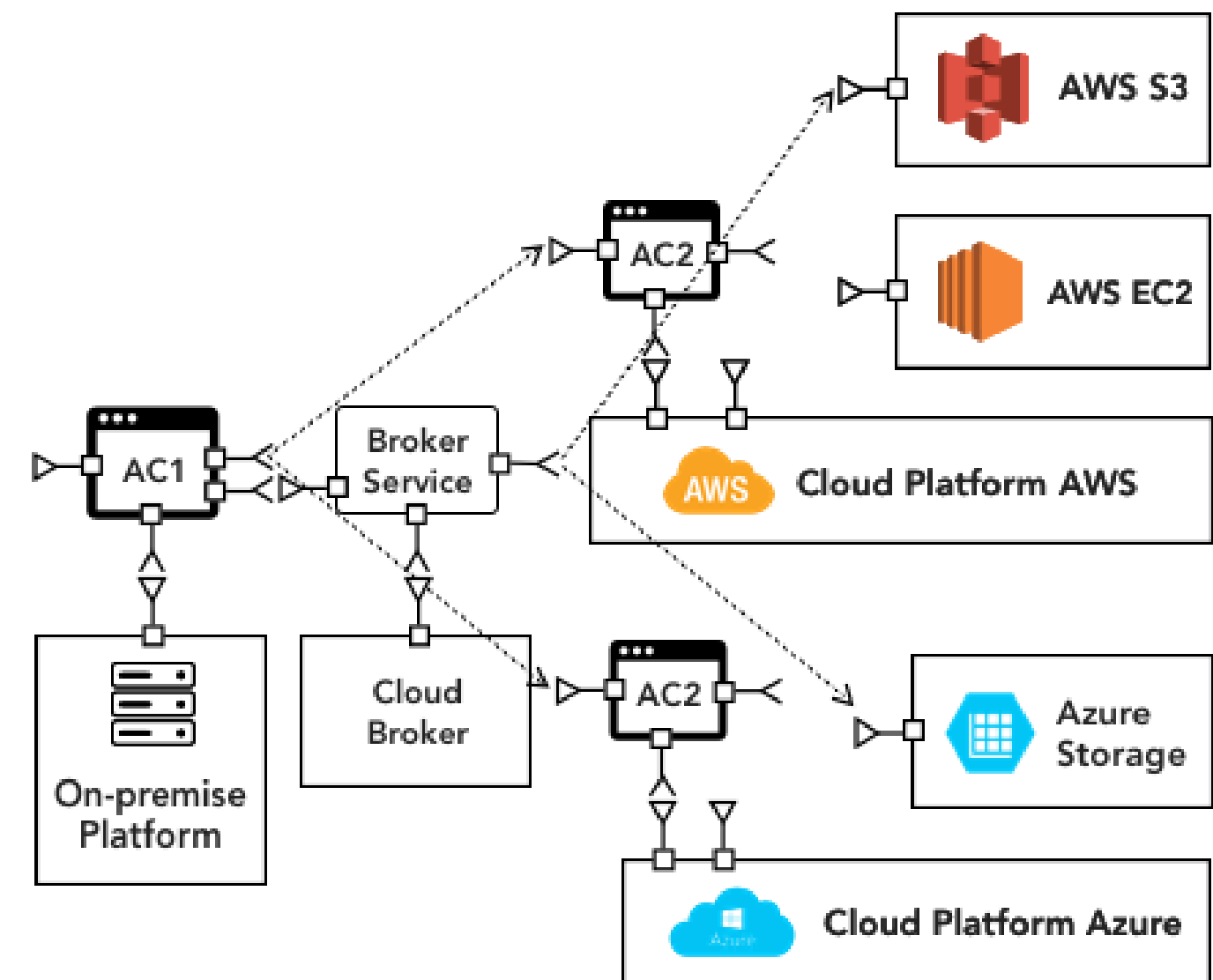
# Sample multi cloud deployment architecture

## Multi-Cloud Rebinding with Cloud Brokerage

Before Migration



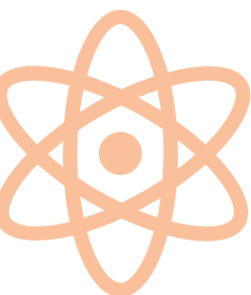
After Migration



# Sample multi cloud deployment architecture

## Multi-Application Modernization

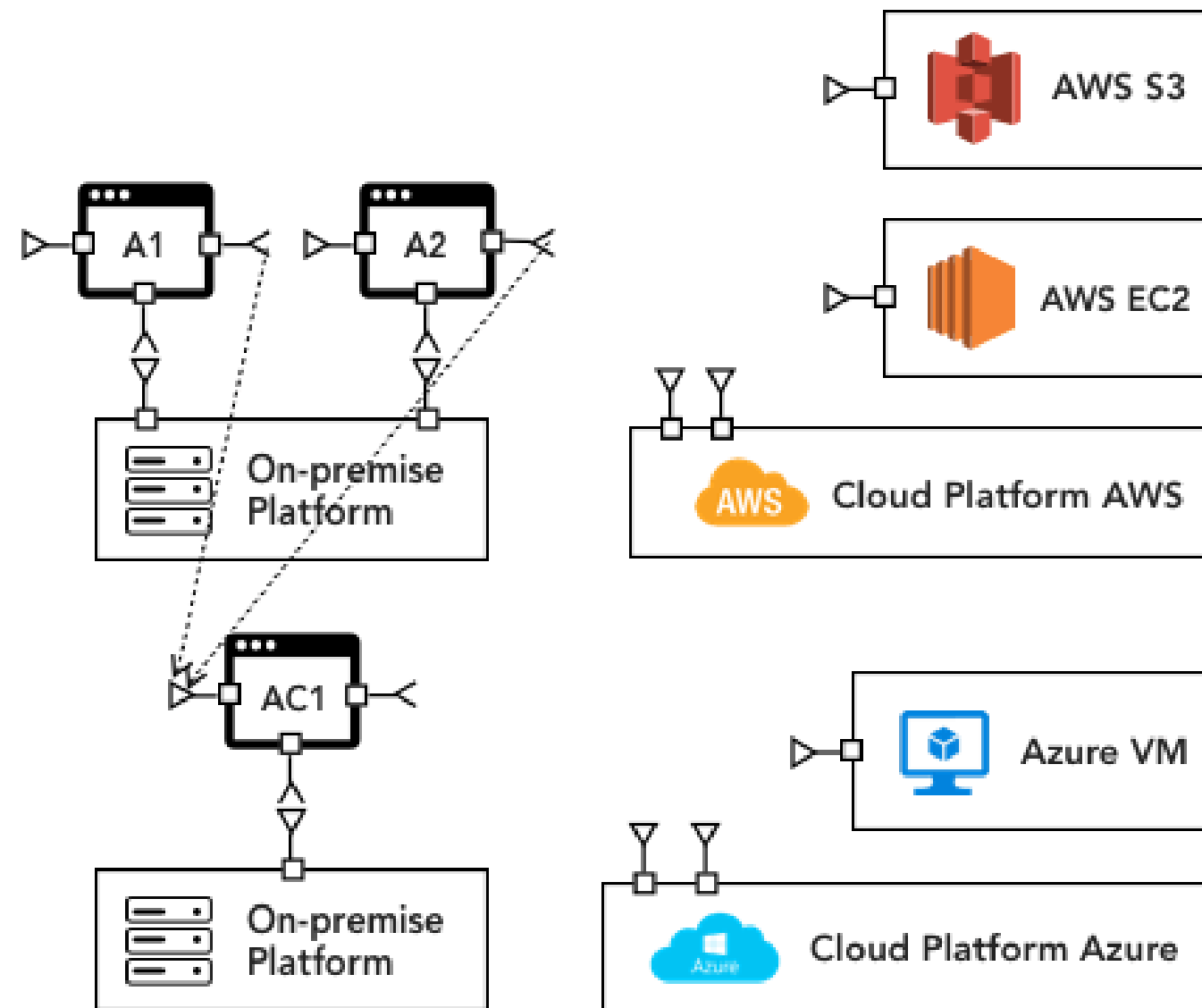
- Different on-premise applications A1/A2, AC1 are re-architected as a portfolio and deployed on cloud environment.
- **Benefits:** It provides consistent information and rules in shared components. Reduced operation and maintenance costs for shared components is another benefit.



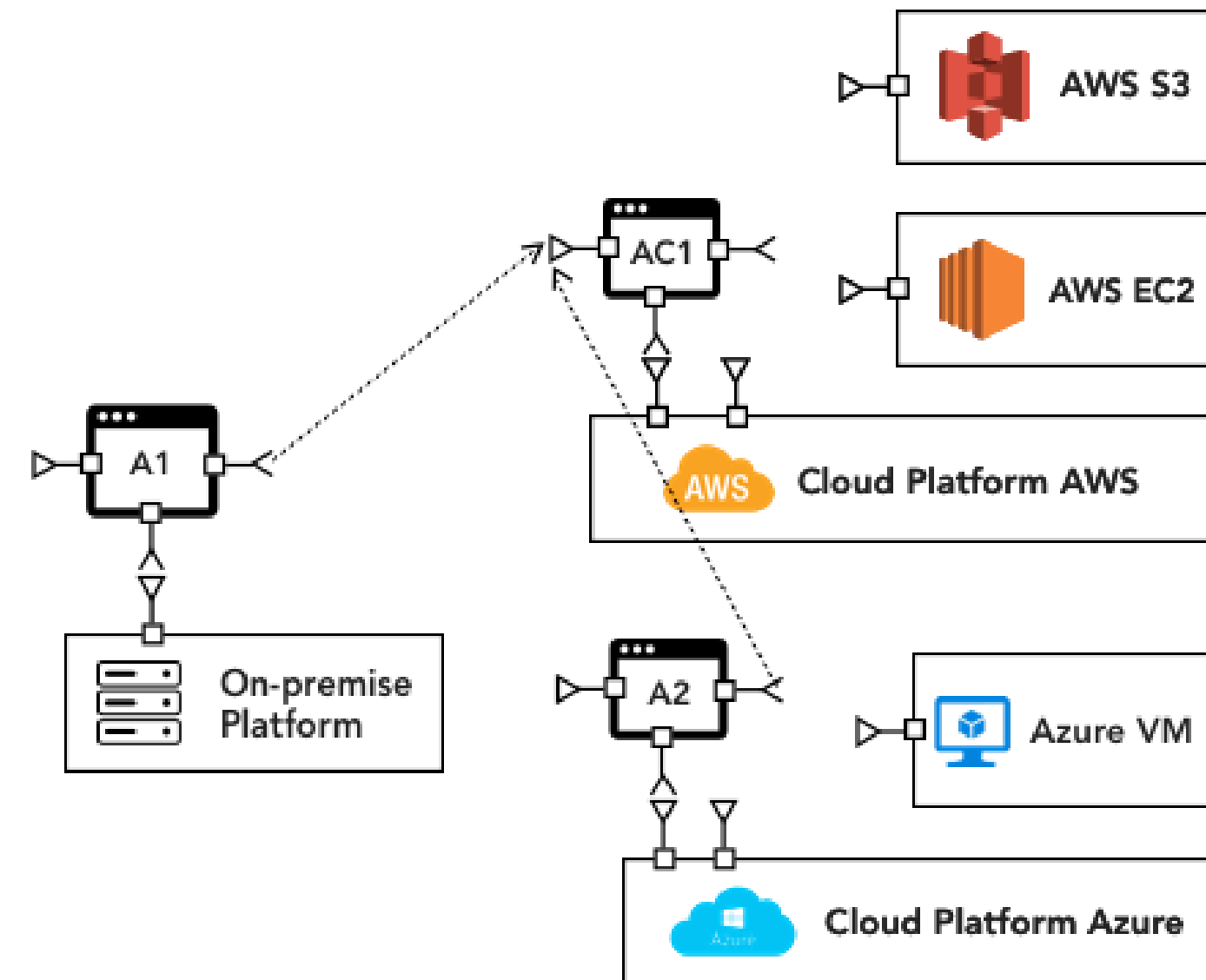
# Sample multi cloud deployment architecture

## Multi-application Modernization

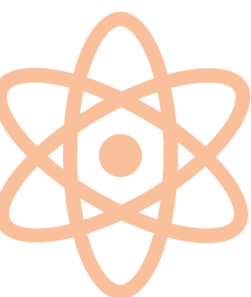
Before Migration



After Migration



Source: <https://www.simform.com/wp-content/uploads/2017/10/Cloudification-15.png>

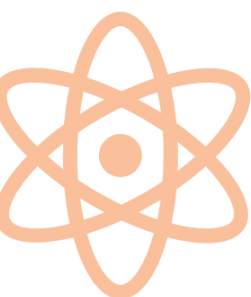


# Lab Activity

# Setup alerting in multi cloud environment

## Amazon CloudWatch

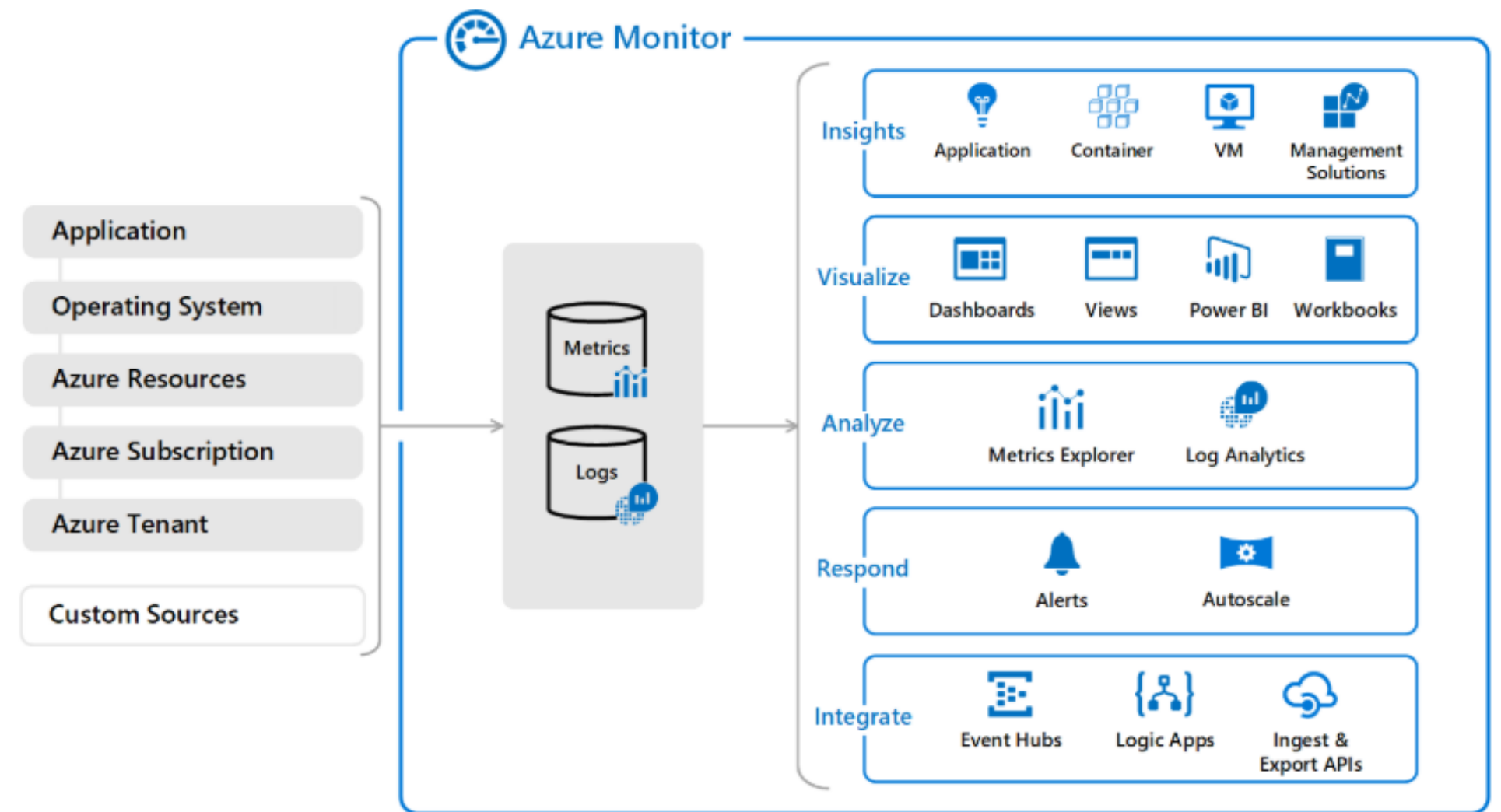
- Amazon Web Services monitoring for the cloud resources and applications running on Amazon AWS.
- It lets you view and track metrics on Amazon EC2 instances and other AWS resources such as Amazon EBS volumes and Amazon RDS DB instances.
- You can also use it to set alarms, store log files, view graphs and statistics, and monitor or react to AWS resource changes.
- Amazon Cloudwatch gives you an insight into your system's overall health and performance.
- You can use this information to optimize your application's operations. The best part of this monitoring solution is you don't need to install any additional software.
- It is a good practice to have multi-cloud management strategies.



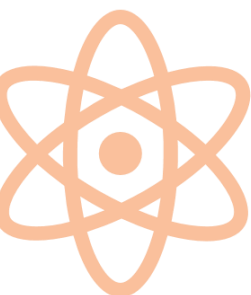
# Setup alerting in multi cloud environment

## Azure Monitor

- Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.
- It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.



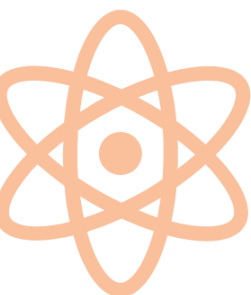
Source: [https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRhu7nSrJkGPLsRKE\\_PMA1D\\_m4xdD8M4qOg2UIBpIPi5qb-EX0r](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRhu7nSrJkGPLsRKE_PMA1D_m4xdD8M4qOg2UIBpIPi5qb-EX0r)



# Setup alerting in multi cloud environment

## Stack Driver

- Stack Driver is a Google cloud service monitoring application that presents itself as intelligent monitoring software for AWS and Google Cloud.
- It offers assessment, logging, and diagnostics services for applications running on these platforms.
- It renders you detailed insights into the performance and health of your cloud-hosted applications so that you may find and fix issues quickly.
- Whether you are using AWS, Google Cloud Platforms, or a hybrid of both, Stack Driver will give you a wide variety of metrics, alerts, logs, traces, and data from all your cloud accounts.
- All this data will be presented in a single dashboard, giving you a rich visualization of your whole cloud ecosystem.

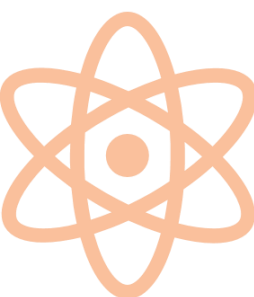




# Setup alerting in multi cloud environment

## Sumo Logic

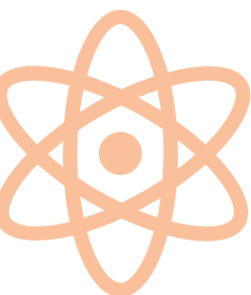
- Sumo Logic offer SaaS security monitoring and log analytics for Amazon Web Services, Azure, Google Cloud Platform, and hybrid cloud services.
- It can give you real-time insights into your cloud applications and security.
- The tool monitors cloud and on-premise infrastructure stacks for operation metrics through advanced analytics.
- It also finds errors and issues warnings quickly actions can be taken.
- Sumo Logic can help IT, DevOps, and Security teams in business organizations of all sizes.
- It is an excellent solution for cloud log management and metrics tracking. It provides cloud computing management tools and techniques to help you eliminate silos and fine-tune your applications and infrastructure to work seamlessly.



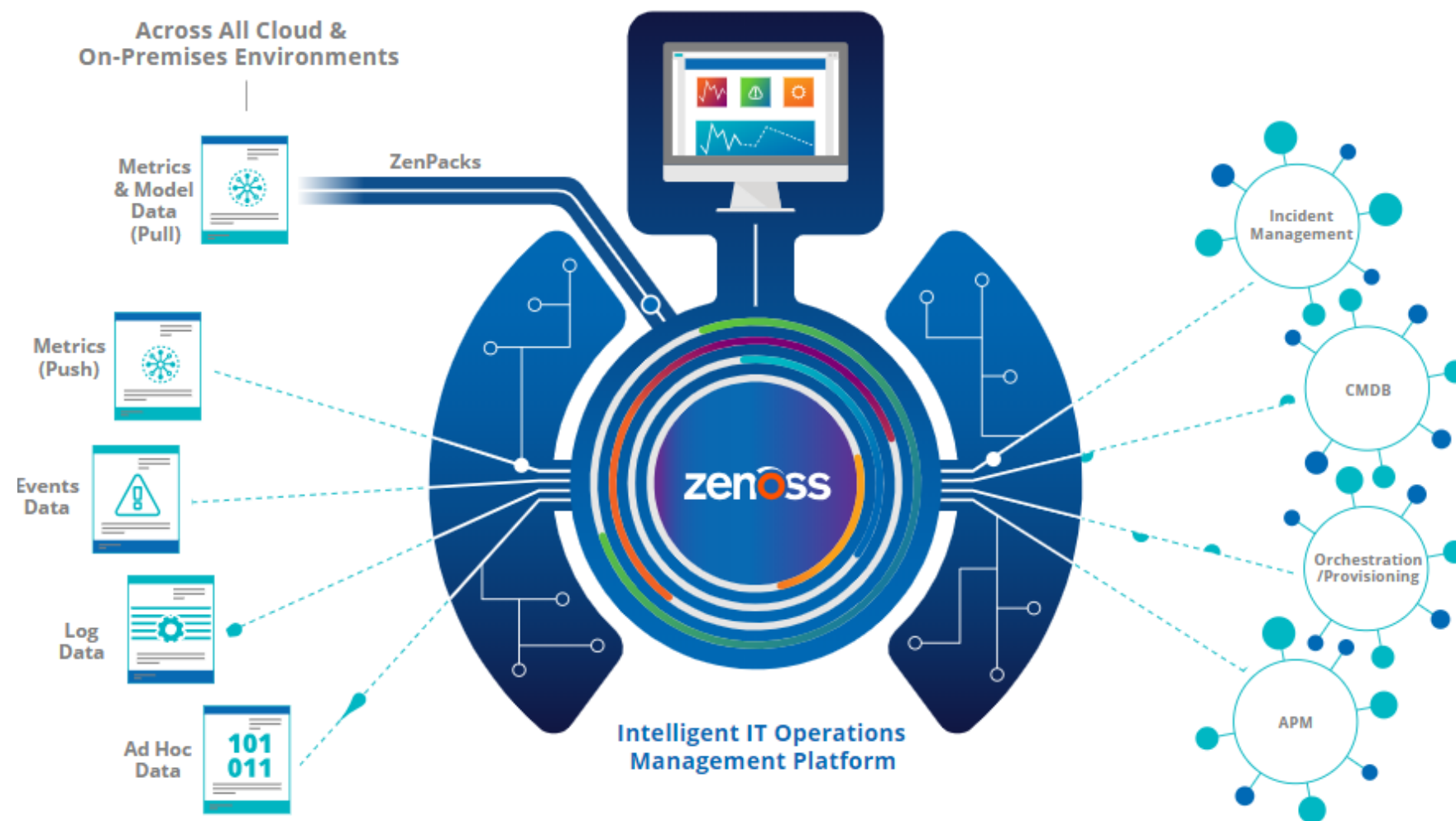
# Setup alerting in multi cloud environment

## Unigma

- Unigma is a management and monitoring tool that correlates metrics from multiple cloud vendors.
- You can view metrics from public clouds like Azure, AWS and Google Cloud.
- It gives you detailed visibility of your infrastructure and workloads and recommends the best enforcement options to your customers.
- It has appealing and simple-to-use dashboards that you can share with your team or customers.
- Unigma is also a significant tool in helping troubleshoot and predict potential issues with instant alerts.
- It assists you to visualize cloud expenditure and provides cost-saving recommendations.



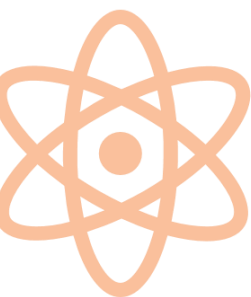
# Setup alerting in multi cloud environment



Source: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRHINvBfKZJOlp55m-beYh6H7cekKVUsT4uLcRvqBtrgHq8AqzUeQ>

## Zenoss

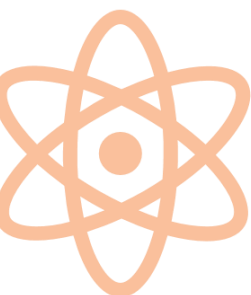
- Zenoss monitors enterprise deployments across a vast range of public cloud hosting platforms including AWS, Azure and GCP.
- It has various cloud analysis and tracking capabilities to help you check and manage your cloud resources well.
- It uses the ZenPacks tracking service to obtain metrics for units such as instances. The system then uses these metrics to ensure uptime on cloud platforms and the overall health of their vital apps.



# Setup alerting in multi cloud environment

## Sensu

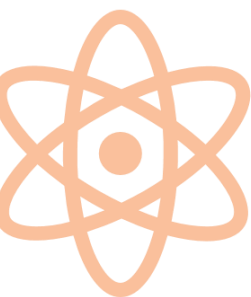
- Sensu empowers you to maintain total visibility over your entire infrastructure that means both the public cloud (AWS, GCP, Azure) and private cloud (OpenStack, VMware, Xen).
- Sensu effortlessly traverses complex network topologies, including NATs, VPNs, and firewalls while monitoring large-scale environments running tens of thousands of virtual machines and applications.
- With Sensu Enterprise it is easy to collect StatsD and Prometheus metrics, and store the data in the tools you're already using – including InfluxDB, Elasticsearch, or Splunk.
- Modern infrastructures are increasing in velocity, and increased velocity further exacerbates the problem of connecting disparate data from the bounty of tools at our disposal.
- With Sensu as your monitoring event pipeline, you can apply workflow automation principles to monitoring.



# Setup alerting in multi cloud environment

## Dynatrace

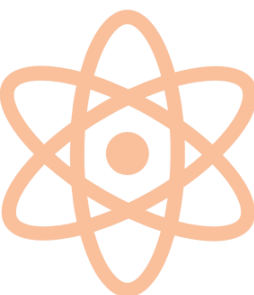
- Dynatrace is a top app, infrastructure, and cloud monitoring service that focuses on solution and pricing.
- Their system integrates with a majority of cloud service providers and micro-services.
- It gives you full insight into your user's experience and business impact by screening and managing both cloud infrastructure and application functionality.
- AI powers Dynatrace. It offers a fast installation process to allow users quick free tests.
- The system helps you optimize customer experience by analyzing user behavior, meeting user expectations, and increasing conversion rates.



# Setup alerting in multi cloud environment

## Uila

- Monitor health of your Multi-cloud environment, including Amazon Web Services (AWS), Microsoft Azure and Google Cloud.
- View all cloud resources from multiple cloud providers in a single pane of glass, regardless of region or zone.
- Proactively alert cloud IT teams to service degradations from the user's perspective before any business impact.
- Rightsize cloud resources for workloads without any performance impact.
- In-depth understanding of Applications, Infrastructure, Cloud components, external devices and their relationships in a single pane of glass.
- Get to Root-cause quickly and pinpoint resource or cloud provider bottlenecks in the dependency chain for poor workload performance.
- Visualize dependency relationships for a multi-tiered application across regions for the same cloud provider.
- View each application service performance by its response time and transaction load on associated VMs or Instances.



 **Break**

 **10 Min**



## Section 8



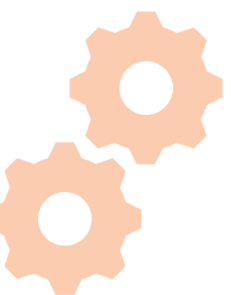
# Choose right cloud vendor(s)



50 Min

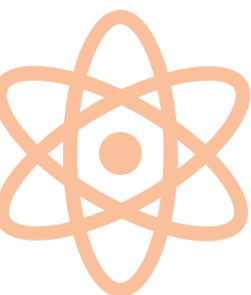
# Goals

- ✓ Determine right cloud provider(s) for your requirement
- ✓ Explore which workload is appropriate for which cloud
- ✓ Migrate workload from one cloud vendor to another
- ✓ Lab Activities



# Determine right cloud provider(s) for your requirement

- The requirements and evaluation criteria will be unique to every organization When it comes to selecting appropriate cloud provider.
- Focus on some of the common areas during assessment of any cloud service provider.
- It is not an easy task to select among the cloud market giants like Amazon, Microsoft and Google through to other cloud providers.
- Identify suitable technology, service, security, cost, performance, data requirements and business needs

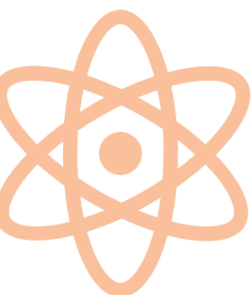


# Determine right cloud provider(s) for your requirement

Before you begin, list your specific requirements and minimum expectations.

## Technologies

- Is the cloud provider platform and technologies align with your current environment and will support your cloud objectives?
- Does the cloud provider standards and services suit your workloads and compliance requirements?
- Does the cloud provider offer migration services and assistance in the re-architecture and planning?



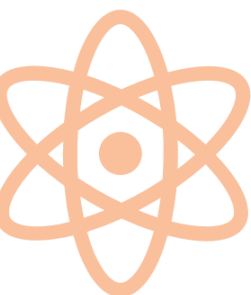
# Determine right cloud provider(s) for your requirement

## Cloud Provider's Service roadmap

- Does the cloud provider's roadmap fit your long term needs?
- Does the cloud provider continue to innovate and grow their service offerings over time?

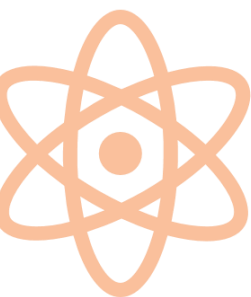
## Data management

- Does the cloud provider support your types of data according to sensitivity and policies on data residency, regulatory or data privacy rules governing personal data (PII)?
- Do they support the location your data resides in and compliance requirement with local, country or continent laws it is subject to?



# Determine right cloud provider(s) for your requirement

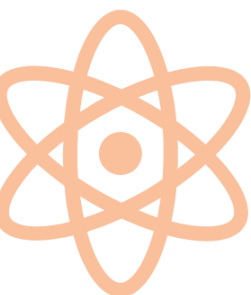
- Are they transparent about their data centre locations and clearly defines your responsibility and their responsibility?
- Do they offer the ability to protect data in transit through encryption of data moving to or within the cloud?
- Do they have mechanism to encrypt data in the sensitive data volumes at rest and limiting any exposure to unapproved administrator access?
- Do they have option to encrypt the sensitive data in object storage with server/client side encryption?



# Determine right cloud provider(s) for your requirement

## Cloud security

- Does the cloud provider publishes their data and system security operations and security governance processes?
- Does the cloud security controls support your own security policies and compliance requirements?
- Do they offer audit capability of user access activity, network activities, compliance reports which aligns your company policy?
- Do they publish their security audit reports, incident reports and remedial actions periodically?



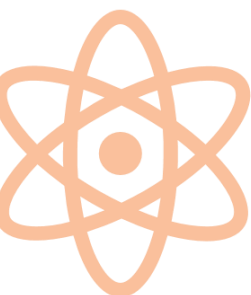


# Explore which workload is appropriate for which cloud

## Industry Standards and Certifications

### Do they comply with recognized standards, frameworks and industry best practices?

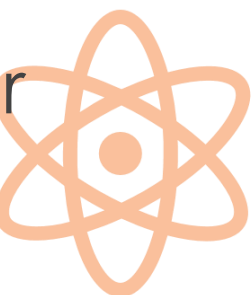
- Cloud Standards Customer Council
- Distributed Management Task Force (DMTF)
- The European Telecommunications Standards Institute (ETSI)
- International Standardization Organization / International Electro-technical Commission Joint
- Technical Committee 1 (ISO/IEC JTC 1)
- International Telecommunications Union (ITU)
- National Institute of Standards and Technology (NIST)
- Open Grid Forum (OGF)
- Object Management Group (OMG)
- Open Cloud Consortium (OCC)
- Organization for the Advancement of Structured Information Standards (OASIS)
- Storage Networking Industry Association (SNIA)
- The Open Group
- Association for Retail Technology Standards (ARTS)
- Tele Management Forum (TM Forum)
- IEEE Cloud Computing Initiative
- Cloud Security Alliance (CSA)
- Cloud Computing Interoperability Forum (CCIF)



# Explore which workload is appropriate for which cloud

## Service Level Agreement (SLA)

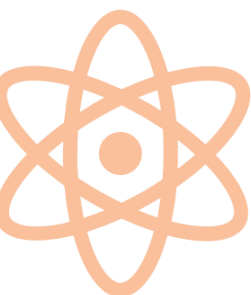
- Does the cloud provider SLA includes the uptime % i.e. availability, accessibility requirement, service capacity limit of users, connections, resources, etc.), response time and elasticity i.e. adoptability to changes?
- Does the SLA of cloud provider is relevant, explicit, measurable, unambiguous, auditable and clearly articulated ?
- Does the SLAs clarify about how issues will be identified, by whom and when it will be resolved, the time period?
- Did they have clear list of terms that limit the scope of the SLA and list exclusions and caveats?
- Does the cloud provider specify the compensation if SLA is breached and the processes for logging and claiming ?



# Determine right cloud provider(s) for your requirement

## Service Level Agreement (SLA)

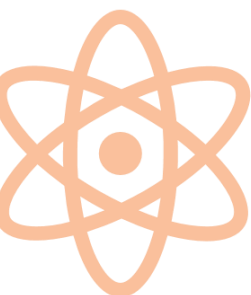
- Does the cloud provider specify the terms relating to Indemnification, Intellectual property rights, Limitation of liability and warranties?
- Does the cloud provider can unilaterally change the terms of service or contract?
- What are the policies on contract renewals and exit or modification notice periods?
- What insurance policies, guarantees and penalties are included and what caveats accompany them?
- Does the cloud provider publish their organization to auditing operations and compliance to policies?



# Determine right cloud provider(s) for your requirement

## Service Level Agreement (SLA)

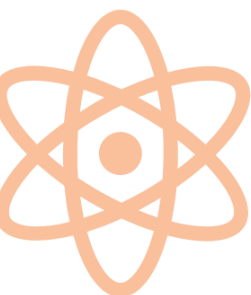
- Does the cloud provider clearly defined security policies and data management policies especially relating to data privacy regulations?
- Do they provide sufficient guarantees around data access, data location and jurisdiction, confidentiality and usage /ownership rights?
- Does the cloud provider has strong backup and resilience provisions?
- Does their data conversion policy allow to transfer data when you decide to leave?
- Do they have clear definition of the service, deliverables, roles and responsibilities in terms of service delivery, provisioning, service management, monitoring, support, escalations, etc?
- How the responsibility is distributed between customer and cloud provider? How do these policies fit with your organization requirements?



# Explore which workload is appropriate for which cloud

## Cloud adoption and migration journey

1. Understand your current portfolio
  - Current Architecture
  - Security and compliance
  - Data requirements
  - Dependencies
2. Analyze pain and understand gain
  - Gains (Advantages and benefits)
  - Pains (Disadvantages and drawbacks)
3. Create your grid
  - High Value / High Effort
  - High Value / Low Effort
  - Low Value / High Effort
  - Low Value / Low Effort

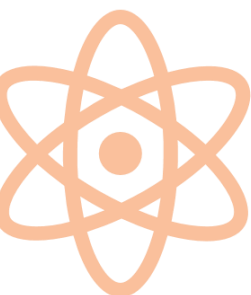


# Explore which workload is appropriate for which cloud

## 1. Understand your current portfolio

### Architecture

- Understand the multiple components in application architecture. Categorize applications as monolithic legacy or microservices.
- Decompose and group workloads into manageable chunks of effort for cloud adoption based on distribution and standardization.
- Are those critical stateful applications or traditional legacy systems, and does it need to be replaced or re-architected to move to cloud.
- Does it require less effort, such as applications that can be moved as-is.
- Are the workloads are standardized, stateless, use a microservices architecture, or follow the twelve-factor app methodology.





# Explore which workload is appropriate for which cloud

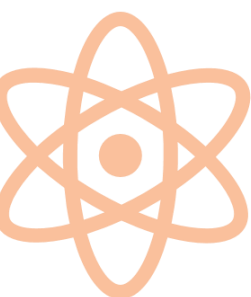
## 1. Understand your current portfolio

### Security and compliance

- Some applications have attributes that align with regulatory requirements such as PCI or HIPAA, or other externally driven requirements.
- Your organization might also have its own compliance parameters that are driven by business objectives.
- It's critical to surface all of these compliance requirements as you analyze the current landscape and prepare to vet cloud target options.
- You might need to establish plans to satisfy each compliance requirement that is associated with each workload.

### Data

- Data is an important element to consider.
- What type of data do you need: object storage, block storage, or real-time storage?
- Will your data be hosted on-premises?
- Will it be hosted inside country borders or outside country borders? How will you access the data? What speed do you need?





# Explore which workload is appropriate for which cloud

## 1. Understand your current portfolio

### Technology

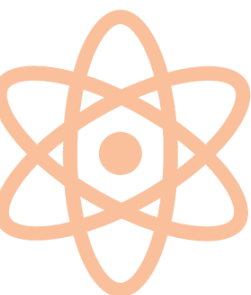
Technical options and decisions that have been made available over time play a key factor in workload assessment. These types of attributes can guide your analysis and prioritization in the context of business alignment.

### Dependencies

Upstream and downstream dependencies play a key role in workload assessment. Almost all workloads are either closely coupled or loosely coupled with key technical and business functions within an enterprise. Understand the impact of changing, dispositioning, or replacing each workload to avoid unsuccessful cloud adoption attempts.

### Scalability

Scalability is inherent to applications that are designed to run in cloud environments. Scalability requires a level of abstraction between particular system calls, particular IP addresses, application state, and underlying platforms. You might need to adjust some applications to be positioned to scale based on usage and peak periods and to take advantage of capabilities such as cloud bursting.



# Explore which workload is appropriate for which cloud

## 2. Analyze pain and understand gain

It's important to understand the value of moving to cloud and understand the "pain," or effort, which is associated with each workload. Your organization must establish a quantifiable measurement to gauge the pain or gain. This measurement is further dependent on individual workload characteristics and includes factors such as platform type, unique hardware considerations, stability, and business criticality.

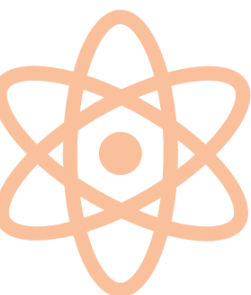
Your organization might establish these measurements for pain and gain:

### Gains:

- Faster time to market
- Reduced time to deploy a new build
- Increased frequency of updates or releases
- Increased user satisfaction

### Pains:

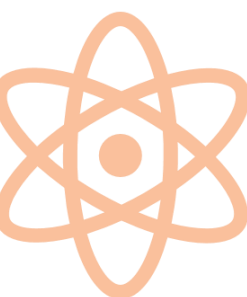
- Unsupported software or operating systems
- Complex code that requires rework
- Level of risk



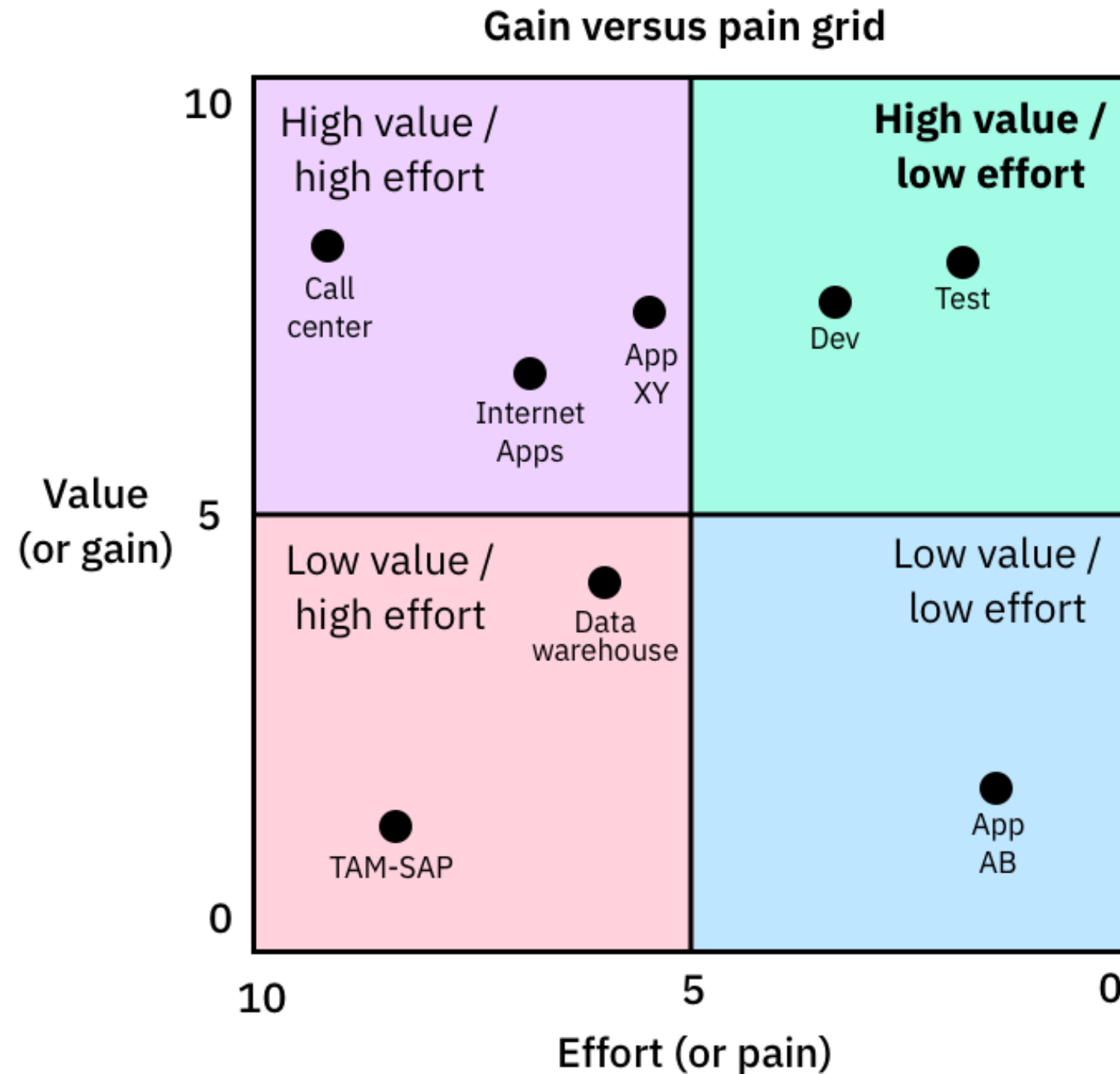
# Explore which workload is appropriate for which cloud

## 3. Create your grid

- After workload attributes are collected and can be measured, explore prioritization in the context of plotting across a gain-versus-pain grid.
- This activity helps you decide which workloads can be grouped into waves of effort.
- A gain-versus-pain grid also informs your sequence as your plan evolves into analyzing your data and including stakeholders.
- In this example grid, the workload is plotted based on the assessed attributes, the gain that is associated with cloud disposition, or both.
- Typically, the upper-right quadrant reflects the workloads to target first, as they represent the most value with minimal effort.



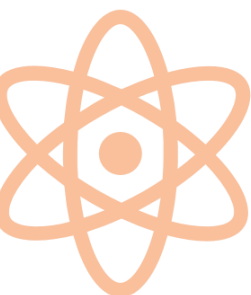
# Explore which workload is appropriate for which cloud



## 3. Create your grid

Cloud workload assessments represent an important initial step in your cloud adoption journey

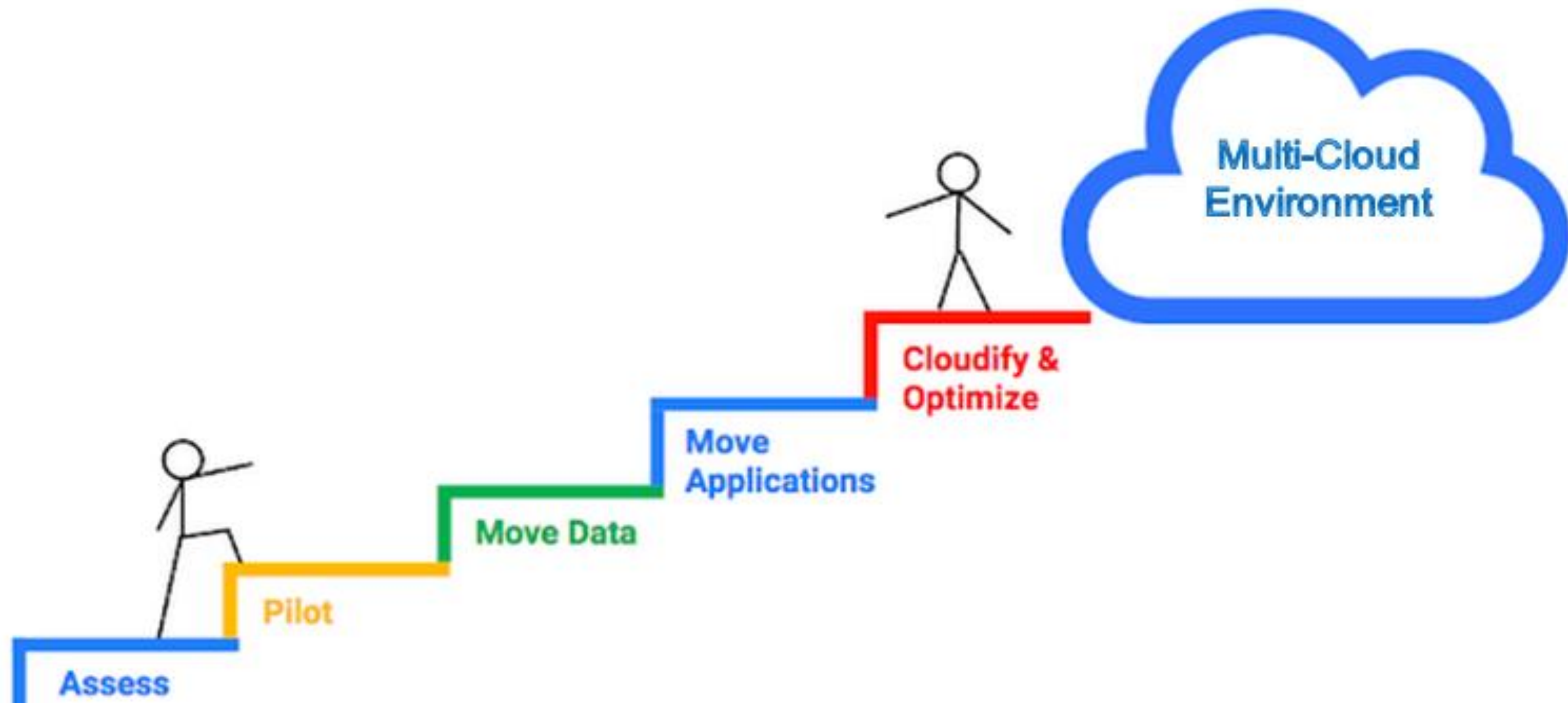
Source: <https://www.ibm.com/cloud/garage/images/practices/gain-pain-grid.png>



# Lab Activity

# Migrate workload from one cloud vendor to another

## A Sequential Approach to Cloud Migration



Source: <https://storage.googleapis.com/gweb-cloudblog-publish/images/five-phases-2pz94.max-700x700.PNG>





# Migrate workload from one cloud vendor to another



Source: [https://www.connectria.com/wp-content/uploads/2019/01/Cloud-Migration-Services\\_graphic.png](https://www.connectria.com/wp-content/uploads/2019/01/Cloud-Migration-Services_graphic.png)





 **Break**

 **10 Min**

# Summary



**50 Min**

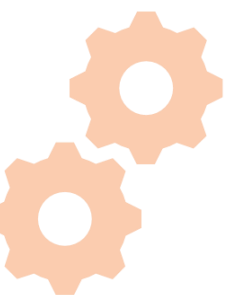
# Wrap-up and Discussion



30 Min

# Goals

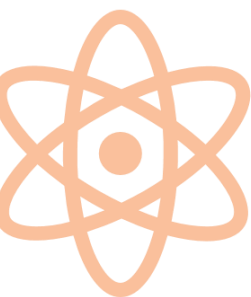
- ✓ Wrap up summary
- ✓ Next steps in the multi-cloud journey
- ✓ Discussion
- ✓ Useful Links



# Wrap up summary

## Course Summary

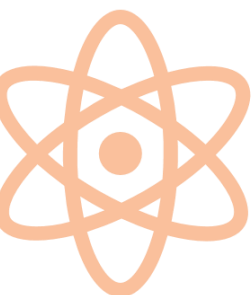
- Getting started with Multi-cloud
- Myth: Multi-Cloud=Hybrid Cloud => all Hybrid clouds are Multi-cloud, but not all multi-clouds are hybrids
- Create Cloud Trial Accounts
- Review the Application code from GitHub
- Multi-Cloud Strategy
- Split your infrastructure for multi-cloud platform
- Build scalable, flexible multi-cloud architecture using AWS, Azure and GCP



# Wrap up summary

## Course Summary

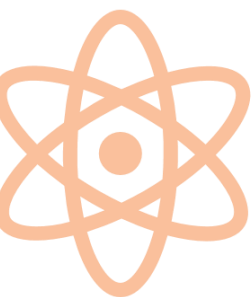
- Setup VPN connectivity between multi-cloud environments
- Migrate your application and database to cloud
- Deploy your application from GitHub to AWS, Azure and GCP
- Build CI/CD pipeline in Azure
- Setup backup in another cloud
- Deploy microservices application into more than one cloud
- Load Balance the workload using global load balancer



# Wrap up summary

## Course Summary

- Migrate Dockers application from AWS to Azure to GCP
- Build security aware multi-cloud platform
- Explore right tools/services for boosting security
- Make Multi Cloud more resilient against DDoS attacks
- Build robust multi cloud monitoring solution
- Balance your workload between various cloud vendor
- Move workloads to appropriate cloud providers

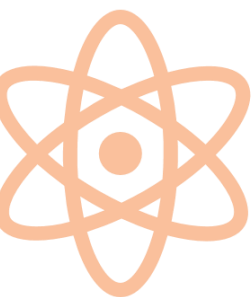




# Wrap up summary

## Course Summary

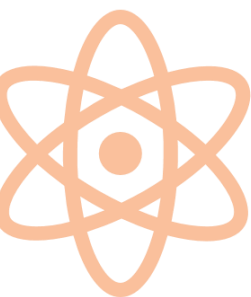
- Migrate storage from AWS and GCP to Azure
- Troubleshooting multi cloud environment
- Setup alerting in multi cloud environment
- Industry best practices for multi cloud platform
- Sample multi cloud deployment architectures
- Determine right cloud provider(s) for your requirement
- Explore which workload is appropriate for which cloud
- Migrate workload from one cloud vendor to another



# Next steps in the multi-cloud journey

## Next steps in the multi-cloud journey

- Not all workloads will migrate to the multi-cloud. Invest in the right tools for visibility and control across traditional and modern workloads.
- Build the right set of skills to manage multi-cloud operations at scale. You will need Cloud Engineers for multi-cloud management and DevSecOps Engineers for continuous delivery and deployment securely.
- Deploy multi-cloud architectures for specialized workloads.
- Multi-cloud will help you avoid vendor lock-in and build resilience.
- Build interoperability across datacenter and multi-cloud architectures using APIs and standards.



# Next steps in the multi-cloud journey

## Discussion – Open Q & A



**Group Discussion**



# Next steps in the multi-cloud journey

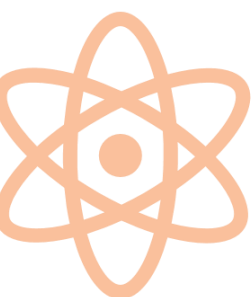
## Useful Links

Cloud Computing Security: From Single to Multi-clouds  
(<https://ieeexplore.ieee.org/abstract/document/6149560>)

Performance Modelling and Simulation of Three-Tier Applications in Cloud and Multi-Cloud Environments  
(<https://ieeexplore.ieee.org/document/8130276>)

Scheduling Data-Driven Workflows in Multi-cloud Environment  
(<https://ieeexplore.ieee.org/document/7396151>)

DevOps Reference Architecture for Multi-cloud IOT Applications  
(<https://ieeexplore.ieee.org/document/8452669>)



# Next steps in the multi-cloud journey

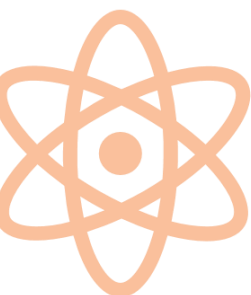
## Useful Links

A Mobile Secure Storage Approach in Multi-cloud Environment  
(<https://ieeexplore.ieee.org/document/8421368>)

Dynamic Data Slicing in Multi Cloud Storage Using Cryptographic Technique  
(<https://ieeexplore.ieee.org/document/8074515>)

Efficient low-cost storage strategy in multi-cloud  
(<https://ieeexplore.ieee.org/document/7925191>)

Malware detection for multi cloud servers using intermediate monitoring server  
(<https://ieeexplore.ieee.org/document/8390135>)



# Next steps in the multi-cloud journey

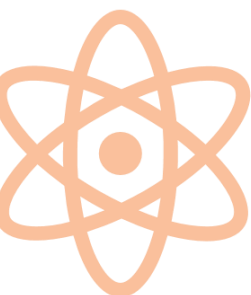
## Useful Links

Decision support tool for IoT service providers for utilization of multi clouds  
(<https://ieeexplore.ieee.org/document/7423285>)

Efficient Content Sharing by Multiple Users with RAID Based Multi-Cloud Storages  
(<https://ieeexplore.ieee.org/document/8549497>)

Simultaneous Ammunition For The Data Security And Privacy In The Multi-Cloud Computing  
(<https://ieeexplore.ieee.org/document/8455162>)

Happy Reading 





 **THANK YOU**  
**WE HOPE YOU ENJOYED THIS COURSE**