Document #: MCS-PWG 2022-013

NIST Multi-Cloud Security Public Working Group (MCSPWG)

DRAFT Meeting Minutes

Meeting #9, May 2, 2022, 3:00 PM ET

		Action items
1	Nida Davis started the meeting at 3:00 PM ET, April 25, 2022. — Attendance: 13 attendees – see Annex B for the list captured on screen during the meeting. See Annex C on the meeting chat. — We refer to the use cases in kick-off presentation https://drive.google.com/drive/u/0/folders/1oo_bjSJgd7Q8mJ2I0NBFykyD71ehYhdq — No recording was stored for the meeting. — Meeting minutes for every meeting are posted for comments https://drive.google.com/drive/u/0/folders/1oo_bjSJgd7Q8mJ2I0NBFykyD71ehYhdq	
2	Nida Davis started the meeting with an invitation for anyone to initiate a pattern. When no one stepped forward, Nida opened the discussion on patterns and trust boundary for multi-cloud. Discussion followed raised the following considerations: a) Is it about distinct systems? b) Cloud service models c) Hybrid cloud in relation to multi-cloud d) Defined trust boundary as legal, authorization and governance e) Different boundaries and technologies f) Shared responsibilities model g) layer	
3	**Discussion returned to the use cases (slide #18) from the Kick-off presentation** [see #1 above]. Nida Davis requested Michaela to provide the NIST draft document on multi-cloud – see Annex E that was provided by Michaela in an email after the meeting. Annex D is a post meeting contribution from Nida Davis in support to the meeting discussion.	
4	**Next Meeting** Nida stated that the next meeting, we will continue the discussion on patterns of multi-cloud. Members should review the discussion, meeting minutes, use cases https://drive.google.com/drive/u/0/folders/1oo_bjSJgd7Q8mJ2I0NBFykyD71ehYhdq and provide comments/questions for discussion.	Review use cases for next week discussion
5	The next meeting will be next week, May 9, 2022, at 3:00 PM ET. See Annex A for meeting Bluejeans details. Note: Individual folders for each group are set up within the MCSPWG Public Document https://drive.google.com/drive/u/0/folders/1c9OV10sAQGFRMplsQALSrKNMtjqKx1CQ	
6	Meeting adjourned at 4:09 PM ET.	

Annex A

Document #: MCS-PWG 2022-012

NIST
MULTICLOUD SECURITY PUBLIC WORKING GROUP (MCSPWG)
DRAFT MEETING AGENDA
May 2, 2022, 3:00 PM ET

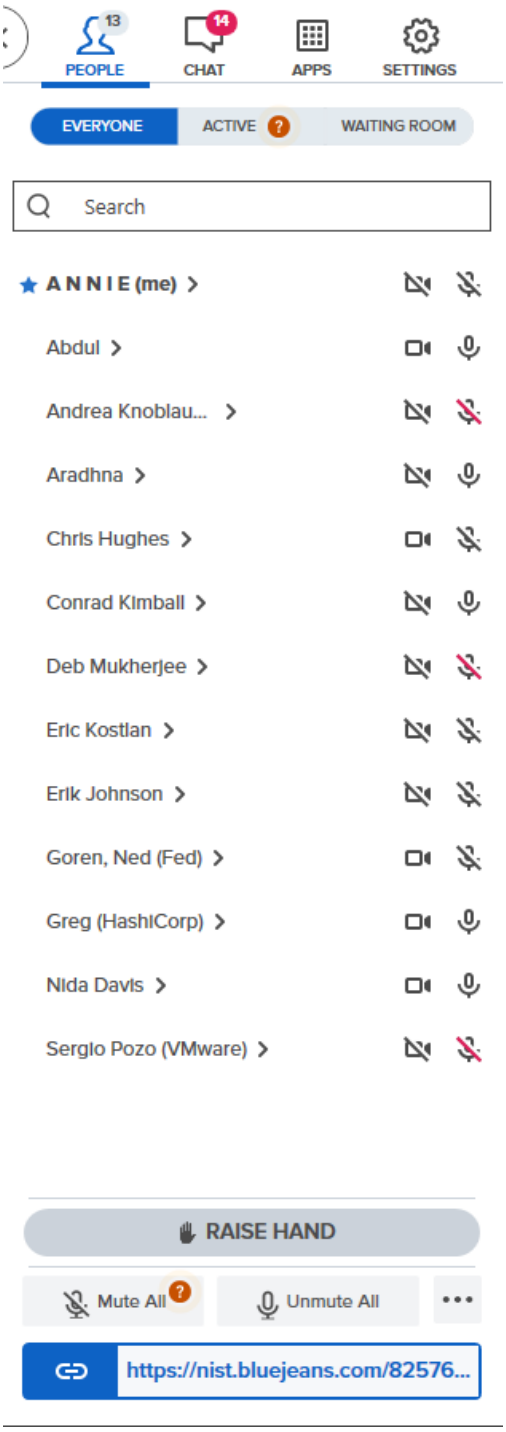
1. Welcome
2. Review of Use Case Patterns – 30 minutes
3. **Group Leads Update – 10 minutes**
   I. Team 1: ZTA-ICAM, team leads: Gregory Thomas & Katy Craig [https://drive.google.com/drive/folders/1mZ8358M_dOJ1HGZwdhleYQ6DxTrqKkUL]
   II. Team 2: ZTA-AC, team leads: Aradhna Chetal & Swapnil Kulkarni & Sergio Pozo (*needs clarification*) [https://drive.google.com/drive/folders/1F3sABpsiEjOQFK-WFMxpAcicw0Ji1-ad]
   III. Team 3: RM-ATO, team leads: Angel Phaneuf & Deb Mukherjee [https://drive.google.com/drive/folders/1kllR8u0aYTBMyXRWps3GY4R1Lx69-EqA]
   IV. Team4: Continuous Monitoring, Abdul Rahman Sattar [https://drive.google.com/drive/folders/1Nau9A3Qtgq-s1NVYteiEFjK3C8Hur5rx]
4. **Open Floor (technical discussion)**
5. Meeting adjournment

Multi-cloud Security Public Working Group Bi-weekly Meeting (VIRTUAL)
The agenda for each meeting will be included in the email reminder .
Please feel free to propose items for the agenda by emailing those topics to us at mcsec@nist.gov
The charter of the WG**: https://csrc.nist.gov/Projects/mcspwg/mcspw-charter**

BlueJeans virtual meeting: **https://nist.bluejeans.com/825766225/2335**
Phone Dial-in
+1.202.795.3352 (United States (Washington DC))
+1.408.317.9254 (US (San Jose))
(Global Numbers)
Meeting ID: 825 766 225
Passcode: 2335

Annex B

Meeting #08 Attendees



Annex C

Meeting Chat

MCSPWG

May 02, 2022

(3:13 PM) Chris Hughes: Agree

(3:13 PM) Chris Hughes: Or we can't move forward clearlyt

(3:13 PM) Conrad Kimball: Also, many CSPs are offering on-premises implementations (AWS Outposts, AWS Snowball, Azure Stack, GKE on-prem, etc.).

(3:13 PM) Erik Johnson: Can be a blend of different cloud service models (Iaas/PaaaS/SaaS, and potentially including specialized supporting services such as IDaaS

(3:14 PM) Chris Hughes: Agreed Erik

(3:15 PM) Abdul: https://drive.google.com/file/d/1jMR6xXPKeayUeI8vGAtibkigFcsvC86L/view

(3:17 PM) Erik Johnson: Is a common customer/System Owner an inherent part of the definition (i.e. the focus of our scope), or coudl it involve multiple customers (ie.. different agencies or an agency and a commercial firm)?

(3:21 PM) Aradhna: r u sharing anything?

(3:21 PM) Aradhna: all I see is Chris in widescope

(3:22 PM) Deb Mukherjee: what slide are you refering to Nida?

(3:25 PM) Greg (HashiCorp): I disagree 100%

(3:25 PM) Greg (HashiCorp): It is all multi-cloud

(3:26 PM) Greg (HashiCorp): The whole world is multi-cloud even in the Datacenter.

(3:27 PM) Greg (HashiCorp): A provider means = one that provides

(3:27 PM) Greg (HashiCorp): This could be an identity, a service or an identity

(3:28 PM) Chris Hughes: This emphasizes why multi-cloud is difficult, almost no one can agree on what it is

(3:29 PM) Greg (HashiCorp): Multi-Cloud/Hybrid

(3:30 PM) Chris Hughes: If we consider SaaS multi-cloud, most organizations are using tens to hundreds of SaaS offerings.. so technically everything is multi-cloud these days

(3:31 PM) Greg (HashiCorp): VPN and IPSEC are also very scary.

(3:31 PM) Greg (HashiCorp): Lot's of trust to IP's

(3:33 PM) Erik Johnson: what is our goal in developing a definition? Something that's philosophicallly comprehensive, or something that gives us a distinct and manageable set of use cases to work with?

(3:33 PM) Nida Davis: customer "does not know"

(3:33 PM) Nida Davis: or customer "does not need to know"

(3:33 PM) Greg (HashiCorp): Agree that customer would not know. Or not really sure how the customer is part of the definition.

(3:34 PM) Chris Hughes: This is a good track - perhaps we keep the definition from the perspective of one persona - e.g. the Cloud Consumer

(3:35 PM) Greg (HashiCorp): What about Privileged access? Would the operators have to stand up what the customers are using?

(3:35 PM) Erik Johnson: In the FedRAMP environment the customer does have full stack visibility info what all the leveraged and supporting services are and can obtain access to all their FedRAMP packages for due diligence purposes if they so desire

(3:37 PM) Nida Davis: Platform as a Service?

(3:38 PM) Chris Hughes: Team - I unfortunately have a hard stop in a few minutes. But I agree with Aradhna that we need to define this in writing, otherwise we have an infinity loop of debate on the topic, and we can't move forward. So, we need a shared definition, and we ultimately may never have 100% consensus

(3:41 PM) Conrad Kimball: Multi-cloud includes hybrid cloud.

(3:41 PM) Erik Johnson: Agreed Chris.

And preferably a definition that's narrow enough to give us a manageable scope rather than trying to boil the ocean

(3:42 PM) Deb Mukherjee: hybrid could be between 2 CSPs, where multi-cloud more than 2 CSPs

(3:42 PM) Conrad Kimball: Multi = more than 1, not more than 2

(3:42 PM) Deb Mukherjee: hybrid?

(3:42 PM) Greg (HashiCorp): The whole gov. is hybrid. How else can they connect to the public cloud? Over the public internet?

(3:42 PM) Deb Mukherjee: hybrid?

(3:44 PM) Erik Johnson: Hybrid cloud Definition (s): The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

(3:44 PM) Erik Johnson: The above is from NIST 800-145

(3:45 PM) A N N I E: Hybrid cloud is defined in NIST SP 800-145

(3:45 PM) Nida Davis: Thank you annie

(3:45 PM) Erik Johnson: https://csrc.nist.gov/glossary/term/Hybrid_cloud#:~:text=Hybrid%20cloud%20Definition%20%28s%29%3A%20The%20cloud%20infrastructure%20is,%28e.g.%2C%20cloud%20bursting%20for%20load%20balancing%20between%20clouds%29.

(3:46 PM) Nida Davis: Hybrid cloud Definition (s): The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

(3:47 PM) Nida Davis: Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud

infrastructures (private, community, or public) that remain unique entities, but are bound

together by standardized or proprietary technology that enables data and application

portability (e.g., cloud bursting for load balancing between clouds).

(3:49 PM) Nida Davis: yup

(3:49 PM) Greg (HashiCorp): We have to include Hybrid Cloud as defined.

(3:50 PM) Nida Davis: yes

(3:50 PM) Nida Davis: September 2011

(3:51 PM) Conrad Kimball: Do not make assumption that cloud = virtual.

(3:52 PM) Nida Davis: Cloud Provider - to - Cloud Provider

(3:53 PM) Conrad Kimball: EC2 offers bare-meal compute instances; Azure offers bare-metal infrastructure (https://docs.microsoft.com/en-us/azure/baremetal-infrastructure/concepts-baremetal-infrastructure-overview)

(3:53 PM) Nida Davis: CSP-Using-CSP

(3:53 PM) Nida Davis: that is easy

(3:55 PM) Conrad Kimball: GCP also offers a bare-metal solution: https://cloud.google.com/bare-metal/docs/bms-planning

(3:57 PM) Conrad Kimball: Boeing is intentionally multi-cloud.

(3:58 PM) Nida Davis: CSP-to-CSP Access Model

(4:00 PM) Greg (HashiCorp): Should be one system

(4:02 PM) Greg (HashiCorp): That has to be the shared responsibility model. Plus the CSPs compete with each other

(4:02 PM) Nida Davis: makes sense

(4:02 PM) Greg (HashiCorp): They will never want to do that.

(4:02 PM) Greg (HashiCorp): The customer needs help and this solution. Already hard enough

(4:03 PM) Greg (HashiCorp): I agree

(4:06 PM) Greg (HashiCorp): Could someone post the notes! I will update what I took down once posted

(4:06 PM) Greg (HashiCorp): I have to drop thanks and if in slack I will update

Annex D

Nida Davis's Post Meeting Contribution

I have pulled together a quick scan of a number of sites, we have also the slides shared by Michaela, and we will have a definition draft from NIST by next week. It looks like a definition is evolving two common pattern attributes:

A. A system or (app, components, interfaces, and DB) operates concomitantly / over multiple clouds.

B. A system (app, components, interfaces, and DB) operates heterogeneously as a single architecture over multiple clouds.

C. A system (app, components, interfaces, and DB) operates across multiple cloud trust boundaries as a single architecture with patterns of a fully native cloud, partial mix of native and modernized to operate in cloud, native and legacy connecting via interfaces, …etc.

D. All pieces and parts of the systems operating are on the behest of the organization that solicited the use and consumption of the cloud services (be it SAAS, SAAP, …etc).

I attached parts and pieces from different sources that cover multi-cloud. Further discussion and a formalized draft definition of Multiple-Cloud is important. I wonder if we simply viewed this as a case of "Service Mesh Architecture" and overlaid it as a System operating as a "single architecture" over multiple clouds using multiple services. Below is a good picture of what is or is not a multi-cloud. In the graph: Hybrid = (One Public Cloud + On Premise) whereas Multiple-Cloud = (Multiple Public Clouds for each separate app/system component + The Clouds DO NOT have to be connected) … if the clouds do not have to be connected, that is a classic hub-and-spoke architecture model. There is nothing to say that Multipl-Cloud = (Multiple Public Clouds for each separate app/system component + the components are connected to operate as one single system). The clouds may not be connected at a physical or virtual level to operate a single architecture. However, the System is connected to operate as a single solution spanning multiple clouds.

I look forward to the definition Michaela and team are crafting. Thank you everyone for your engagement today. Jose and Greg, this confirms the common view we shared today that regardless of how many clouds or type of clouds we are talking about, we should look at all the pieces and parts of the System as one across multiple clouds.

What is Multi-Cloud? | VMware Glossary

Multi-Cloud is the superset of multiple public cloud, hybrid, on-premises, and edge. A multi-cloud deployment model relies on the use of more than one public cloud service provider for compute or storage resources, independent of the use of other private cloud or on-

premises infrastructure. A multi-cloud deployment that includes private cloud or on-premises infrastructure is considered a hybrid multi-cloud.

What is Multicloud? | IBM

What is multicloud?

Multicloud is the use of cloud services from more than one cloud vendor. It can be as simple as using software-as-a-service (SaaS) from different cloud vendors – e.g., Salesforce and Workday. But in the enterprise, multicloud typically refers to running enterprise applications on platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) from multiple cloud service providers, such as Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud and Microsoft Azure.

A multicloud solution is a cloud computing solution that's portable across multiple cloud providers' cloud infrastructures. Multicloud solutions are typically built on open-source, cloud-native technologies, such as Kubernetes, that are supported by all public cloud providers. They also typically include capabilities for managing workloads across multiple clouds with a central console (or 'single pane of glass'). Many of the leading cloud providers, as well as cloud solution providers such as VMware, offer multicloud solutions for compute infrastructure, development, data warehousing, cloud storage, artificial intelligence (AI) and machine learning (ML), disaster recovery/business continuity and more.

https://phoenixnap.com/blog/multi-cloud

Multi-Cloud Definition

A multi-cloud is a cloud computing strategy in which a company relies on multiple cloud providers instead of a single vendor. An organization can pick and choose the best services from each provider based on the following factors:

- Service cost.
- Technical requirements.
- Geographic availability.

The driving force behind the multi-cloud concept is that no single provider can offer a solution to all the problems a business can face. Different vendors specialize in other areas and tasks, so companies can use multiple clouds to create a custom infrastructure that ideally fits all business goals.

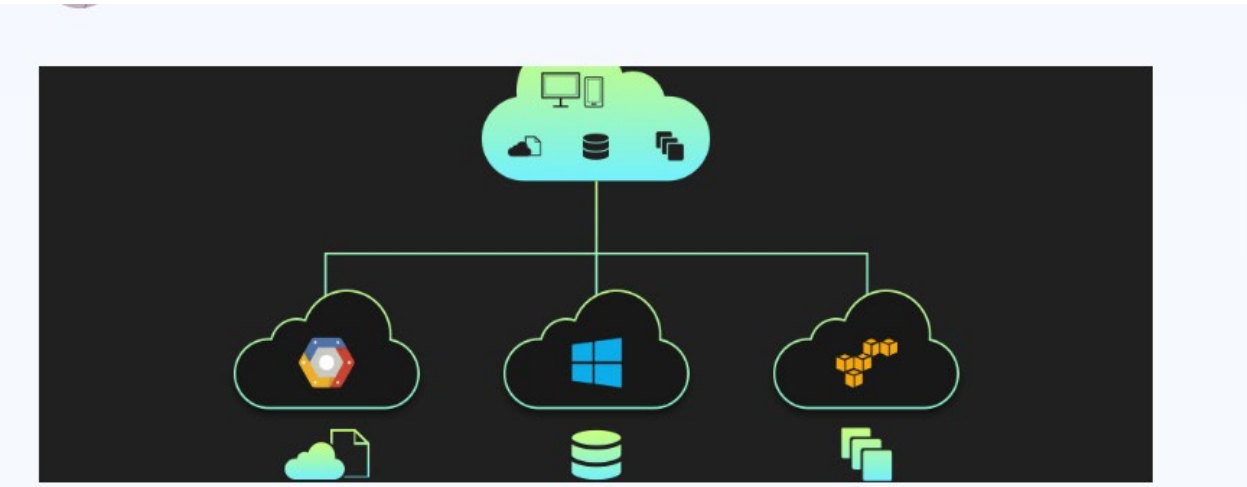
Here are a few examples of how a company can use a multi-cloud setup:

- A company using Google Cloud Platform (GCP) for development and testing while relying on Azure for business analytics.
- An organization using different providers for IaaS, PaaS, and SaaS services.
- A company using Azure in the US and Alibaba in Asia to ensure the app does not suffer from latency.
- An organization consuming emails as service from one vendor, CRM services from another, and IaaS fro

https://www.simform.com/blog/multi-cloud-architecture/

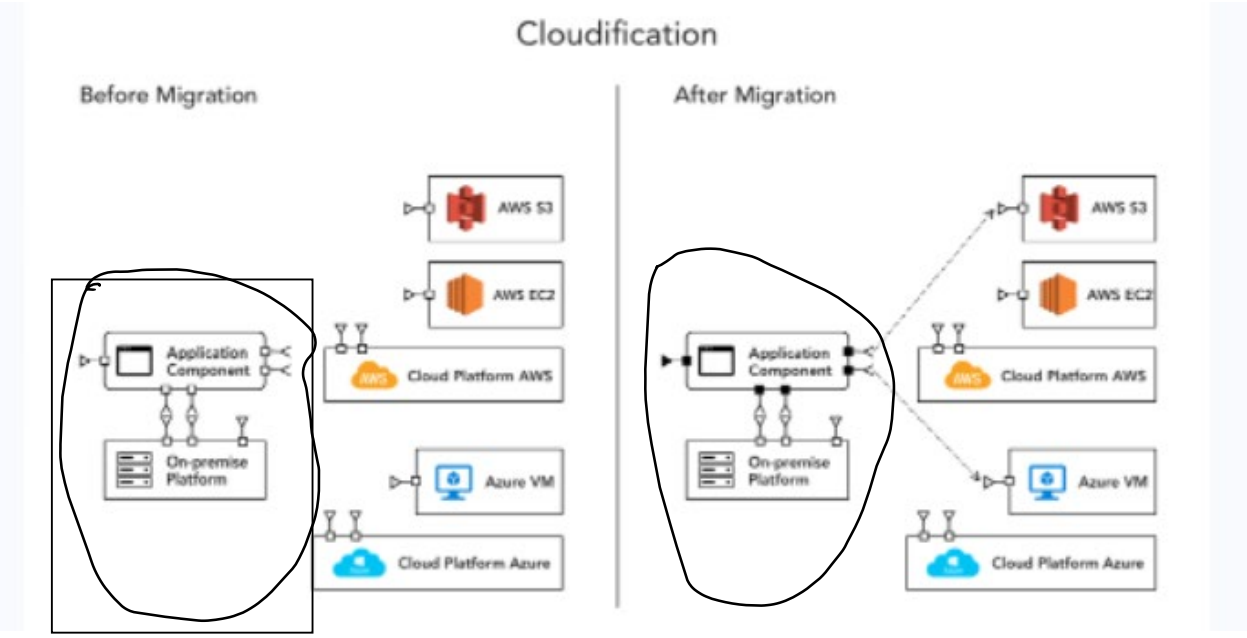
Deploying a multi-tenant application across multiple cloud platforms can be very challenging. In this blog, we've explained 6 multi-cloud architecture designs which can help businesses to build an effective multi-cloud strategy.

Multi-cloud strategy is the **concomitant** use of two or more cloud services such as AWS, Azure, Google Cloud and more: “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.”



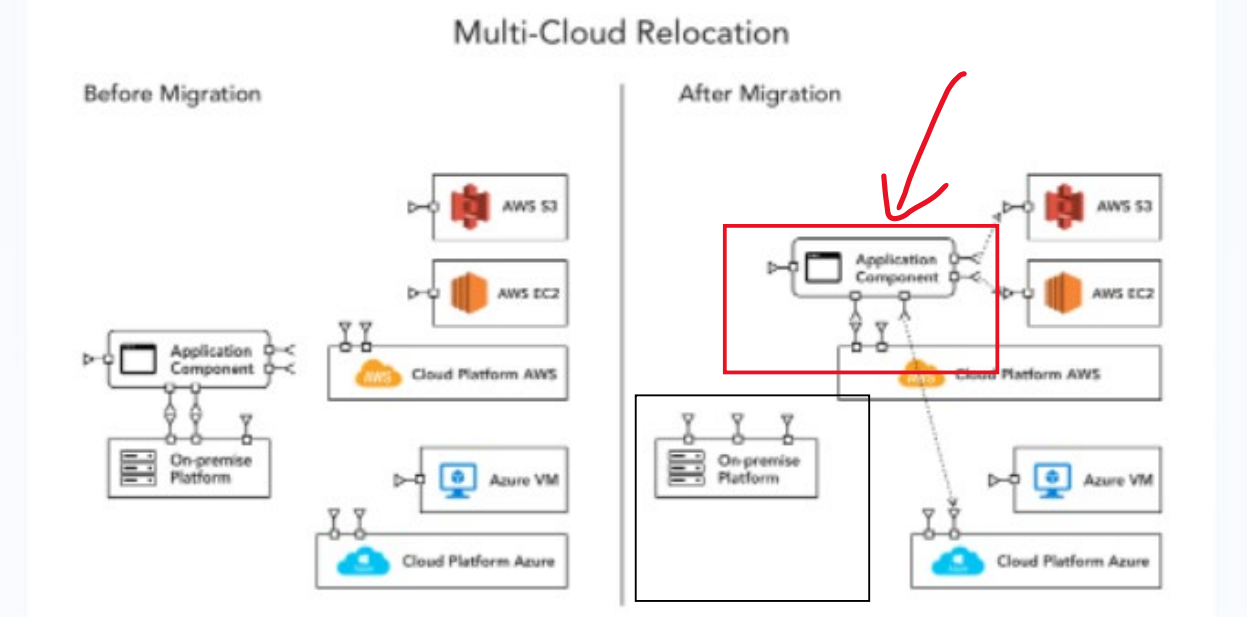
Pattern One: Cloudification

An application uses cloud services – it is not moved to cloud but rather remains on premise of data center and connects to cloud-based services [integration patterns].



Pattern Two: Multi-Cloud Relocation

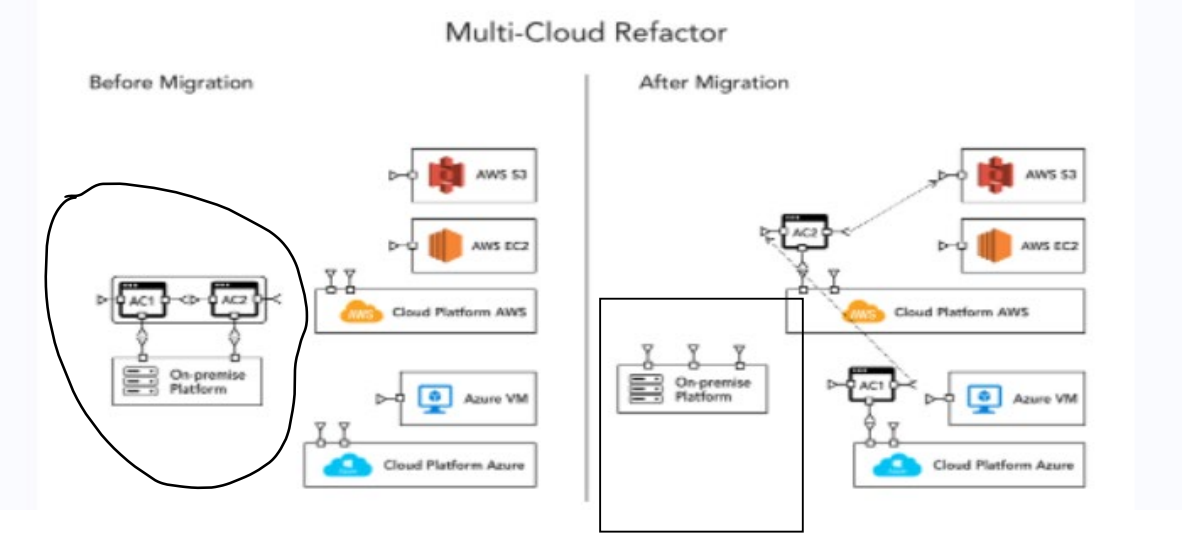
An application component is moved to cloud services to host (AWS Cloud in this example) – application connects to other cloud-based services such as Azure [integration patterns].



Pattern Three: Multi-Cloud Refactor

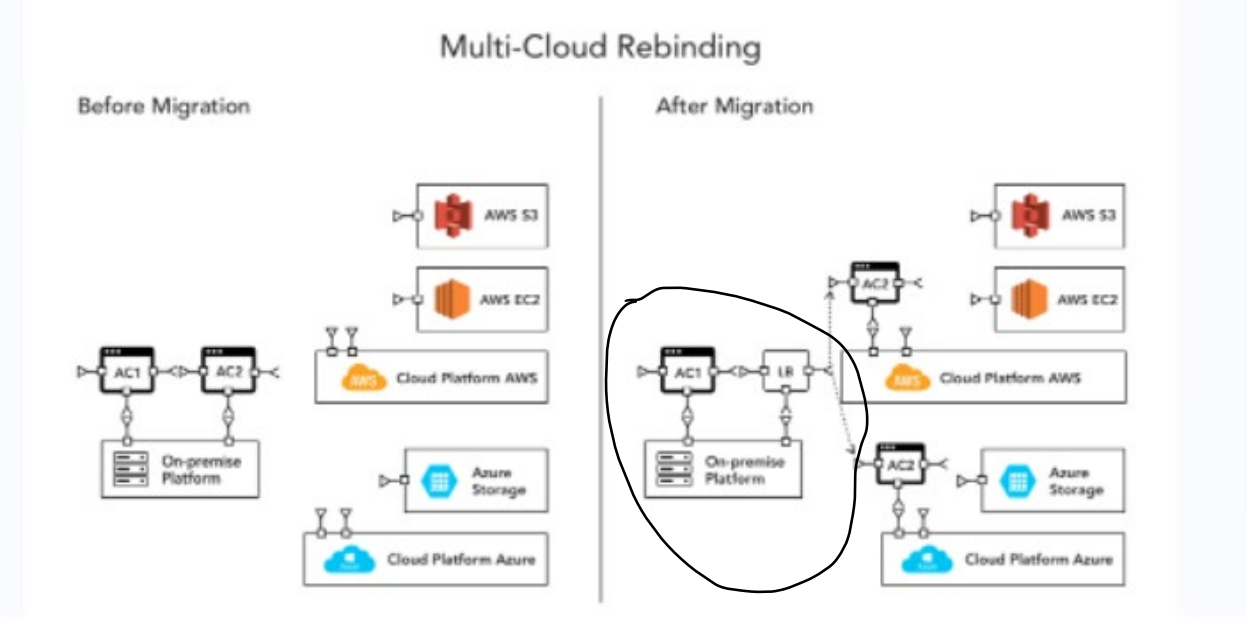
An application (legacy) is rearchitected to optimize performance on multiple clouds:

"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."



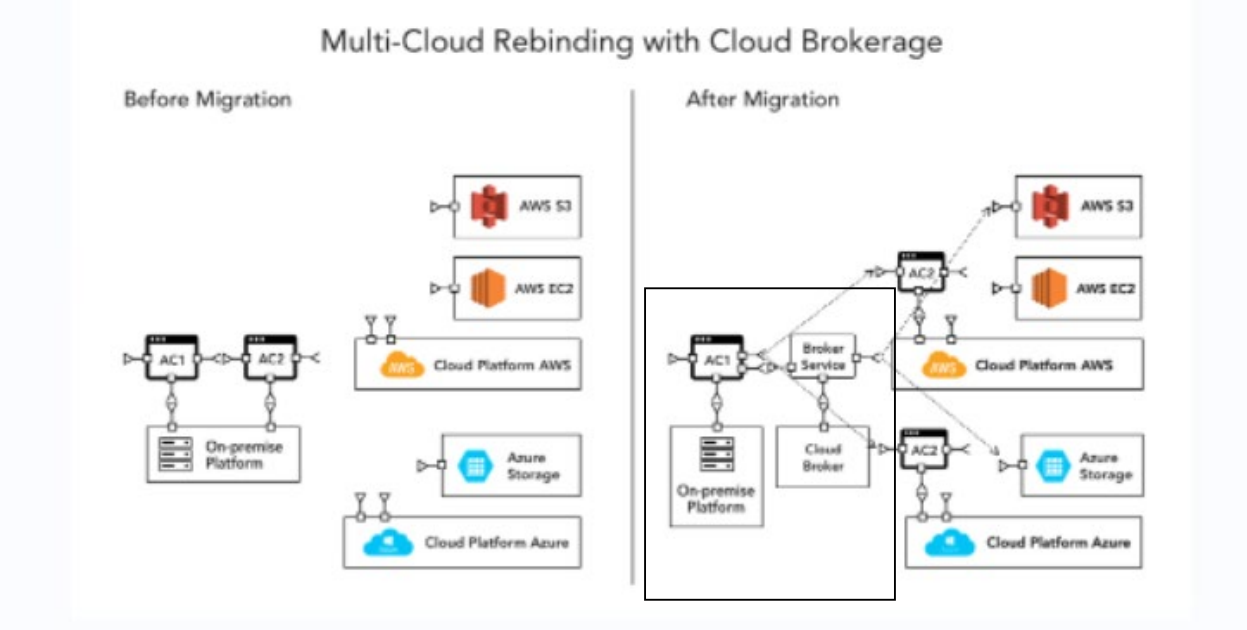
Pattern Four: Multi-Cloud Rebinding

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.



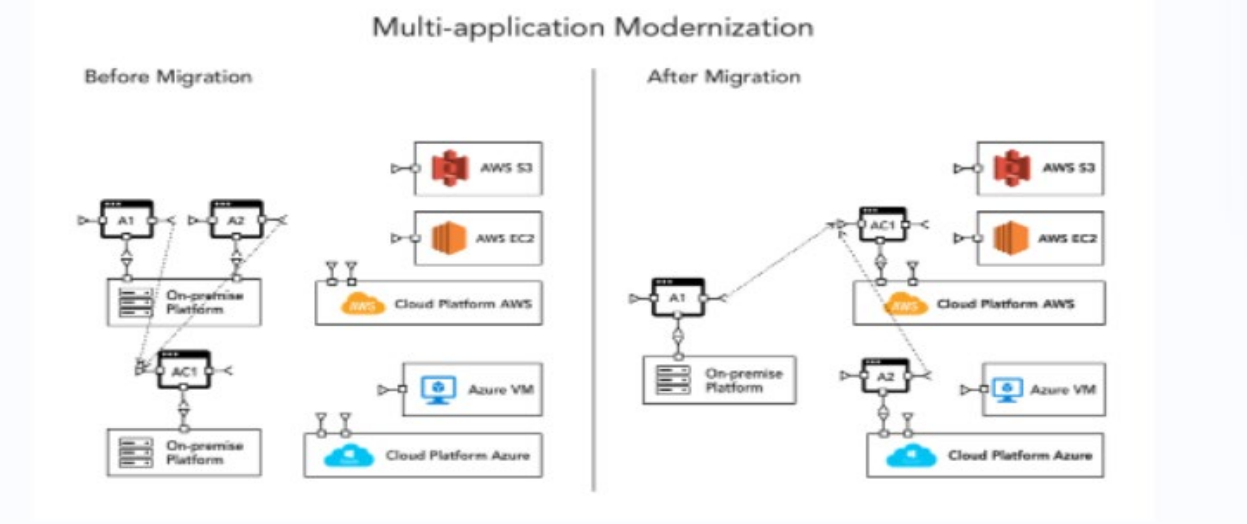
Pattern Five: Multi-Cloud Rebinding with Cloud Brokerage

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.



Pattern Six: Multi-Application Modernization

Different on-premise applications A1/A2, AC1 are re-architected as a portfolio and deployed on cloud environment.



Multi-Cloud is a model of cloud computing where an organization utilizes a combination of clouds, which can be two or more public clouds, two or more private clouds, or a combination of both public and private clouds.

Pattern Seven: Native Cloud Application operating on multiple clouds (multiple components) without a connection to the organization (all access/authorization handled in cloud) Question here on best practices how would the organization handle access/authorization across multiple clouds?.

Pattern Eight: Native Cloud Application operating on multiple clouds (multiple components) with connection to the organization to manage all access/authorization handled in cloud (federation).

Hybrid: Native or Migrated Application operating on one cloud (multiple components and DB) with or without connection to the organization to manage all access/authorization handled in cloud (federation).

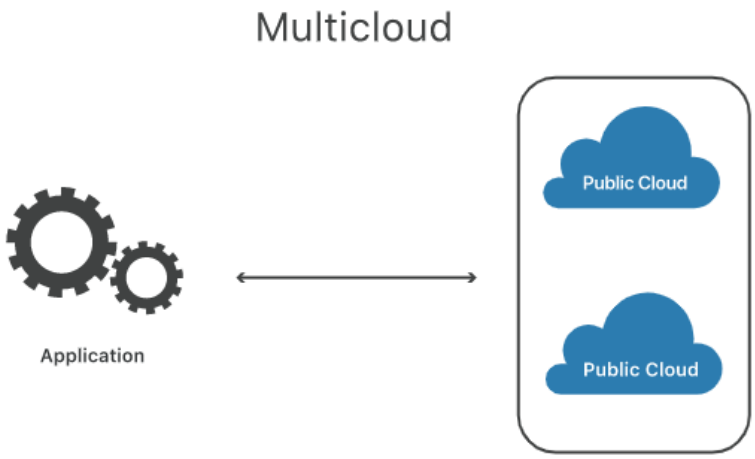
Out of SCOPE: Cloud Service Provider – to – Cloud Service Provider linkages and connections (virtual or physical) that are not part of the scope definition of the system = (application/components/interfaces / DB) or are clearly defined as the responsibility of the Cloud Service Provider duty to manage.

https://www.juniper.net/us/en/research-topics/what-is-multicloud.html

Multicloud is a cloud computing deployment model that enables organizations to deliver application services across multiple private and public clouds containing some or any combination of the following: multiple cloud vendors, multiple cloud accounts, multiple cloud availability zones, or multiple cloud regions or premises.

https://www.cloudflare.com/learning/cloud/what-is-multicloud/

"Multi-cloud" means multiple public clouds. A company that uses a multi-cloud deployment incorporates multiple public clouds from more than one cloud provider. Instead of a business using one vendor for cloud hosting, storage, and the full application stack, in a multi-cloud configuration they use several.


Multicloud
Public Cloud
Public Cloud
Application

.

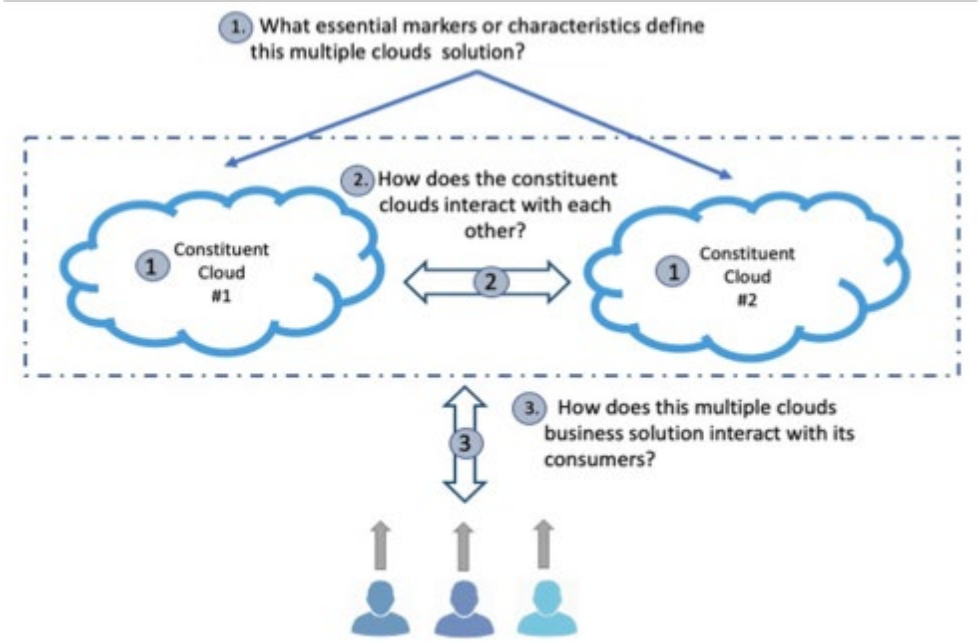
Annex E

NIST DRAFT MULTI-CLOUD CONCEPTUAL MODEL

NIST's draft multi-cloud conceptual model document from where the patterns were extracted, uses a methodology designed to facilitate a consistent analysis of the documentary material collected from existing cloud orchestrations of more than one constituent cloud. The aimed outcome of the analysis is the identification of the core characteristics of the *multi-cloud conceptual model* and of the modalities of interaction among constituent clouds.

Note: In the context of the draft document (and this email) orchestration term refers to the arrangement and coordination of automated tasks resulting in a consolidated process or workflow.

The analysis principles (aspects) we used internally at NIST are graphically depicted below:



We also used the following classification markers:

1. **Resource ownership and management**: This characterizes the resource ownership (or use or control rights) of the constituent clouds: for example, are the constituent clouds all public, all private, or combinations of private and public clouds?

2. **Number of cloud providers (legal entities managing the cloud stack):** This is the number of constituent clouds or cloud providers.

3. **Cloud providers' interaction:** This characterizes how the constituent cloud providers interact with each other. This marker is focusing on identifying if the constituent cloud providers offered their services independently to the consumer which in turn

orchestrates them into a multiple cloud solution or are they collaborating with each other to offer a solution to the consumers?

4. **Cloud consumer service <u>model</u>:** This characterizes if a multiple cloud solution supports individual, federated or communities of consumers.

5. **Other key defining features:** This captures several other important aspects of a multi-cloud solution such as how the Service Level Agreements are structured among the cloud providers and the with the cloud consumers.

Similar to the SP 800-145, we proposed that:

Multi-cloud. *The cloud architecture is a composition of two or more distinct clouds of the same deployment model (e.g. all private or all public) provided by more than one cloud provider.* A multi-cloud architecture integrates individual technologies to create a single cloud-IT environment that ideally will maximize benefits successfully with using one type of deployment model, i.e. either private or public.

Excerpt from SP 800-145:

Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).*

Public cloud. *The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.*

Private cloud. *The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.*

Community cloud*. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.*