Document #: MCS-PWG 2022-016

NIST Multi-Cloud Security Public Working Group (MCSPWG)

DRAFT Meeting Minutes

Meeting #11, May 16, 2022, 3:00 PM ET

		Action items
1	The meeting at 3:06 PM ET, May 16, 2022. — Annex A – Meeting Agenda posted on https://drive.google.com/drive/u/0/folders/1oo_bjSJgd7Q8mJ2I0NBFykyD71ehYhdq; https://csrc.nist.gov/Projects/mcspwg/meetings Meeting minutes for every meeting are posted for comments — Annex B for the list of attendees captured on screen during the meeting. — Annex C on the meeting chat. — Annex D – Example on research flowchart https://drive.google.com/file/d/1uvkVnbAmNXQMiuFi0HsG_II2T1DNXPgE/view — Annex E – collection of patterns discussed on previous meetings. 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.	
2	During May 9 meeting, discussion covered certain concepts of compositions and established some common understanding of multi-cloud. The ambition at this meeting was to finalize or extend from last week meeting's discussion. Unfortunately, no notes were taken for May 9 meeting. A presentation was given by Jose Gomez on May 9, but Jose was not in attendance at this meeting for us to follow-up or expand on the concepts.	Request presentation used on May 9 meeting.
3	The last meeting discussion also covered on low and high impact levels, trust and authorization boundaries, the impact levels on a multi-cloud system/ecosystem. The suggestion was to revert to the groups to determine the details including use cases, classification, etc. with reference to the previous discussion on patterns, control sets, 7 layers, data for low to high impact (e.g., see Annex E).	Group Leads
4	Michaela Iorga shared flowchart that was used for cloud computing forensic document (see Annex D). This is an example for preparing a plan with logical flow to develop the outcome. The example includes questions to explain each step. When each group presents "plan", it would create opportunities for convergence, overlaps, and a possible agreement on a common set of outcomes. This is an example and not a prescriptive guidance.	Group Leads – investigate research diagram
5	As the meeting was coming to the top of the hour, we were able to receive brief reports from the group leads.	
6	Future meetings Deb Mukherjee, ATO Group Lead, reported that the group used a FigJam https://www.figma.com/file/8aZPm4VLOKrnVmPie8dfFX/May-13%2C-2022?node-id=0%3A1 to develop consensus similar to the process plan example from Michaela. The group also discussed changing meeting day and time, and Deb asked about the	

	regularity of this MCSPWG meeting. This led to an agreement to revert the weekly meetings to bi-weekly meetings beginning in June. MCSPWG will meet on May 23, and the first meeting in June 2022 will be June 6, 2022, at 3:00 PM ET (See Annex A for meeting Bluejeans details). MCSPWG will not meet on May 30, 2022.	
7	Meeting adjourned at 4:04 PM ET.	

Annex A

Document #: MCS-PWG 2022-015

NIST
MULTICLOUD SECURITY PUBLIC WORKING GROUP (MCSPWG)
DRAFT MEETING AGENDA
May 16, 2022, 3:00 PM ET

1. Welcome
2. Review Last Week's Meeting Discussion
3. Research Process & Team Sharing
4. Review Team's Work on Multi-Cloud Concept & Recommendations: Open Discussion.
5. **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]

6. **Open Floor (technical discussion)**
7. Meeting adjournment

Meeting logistics

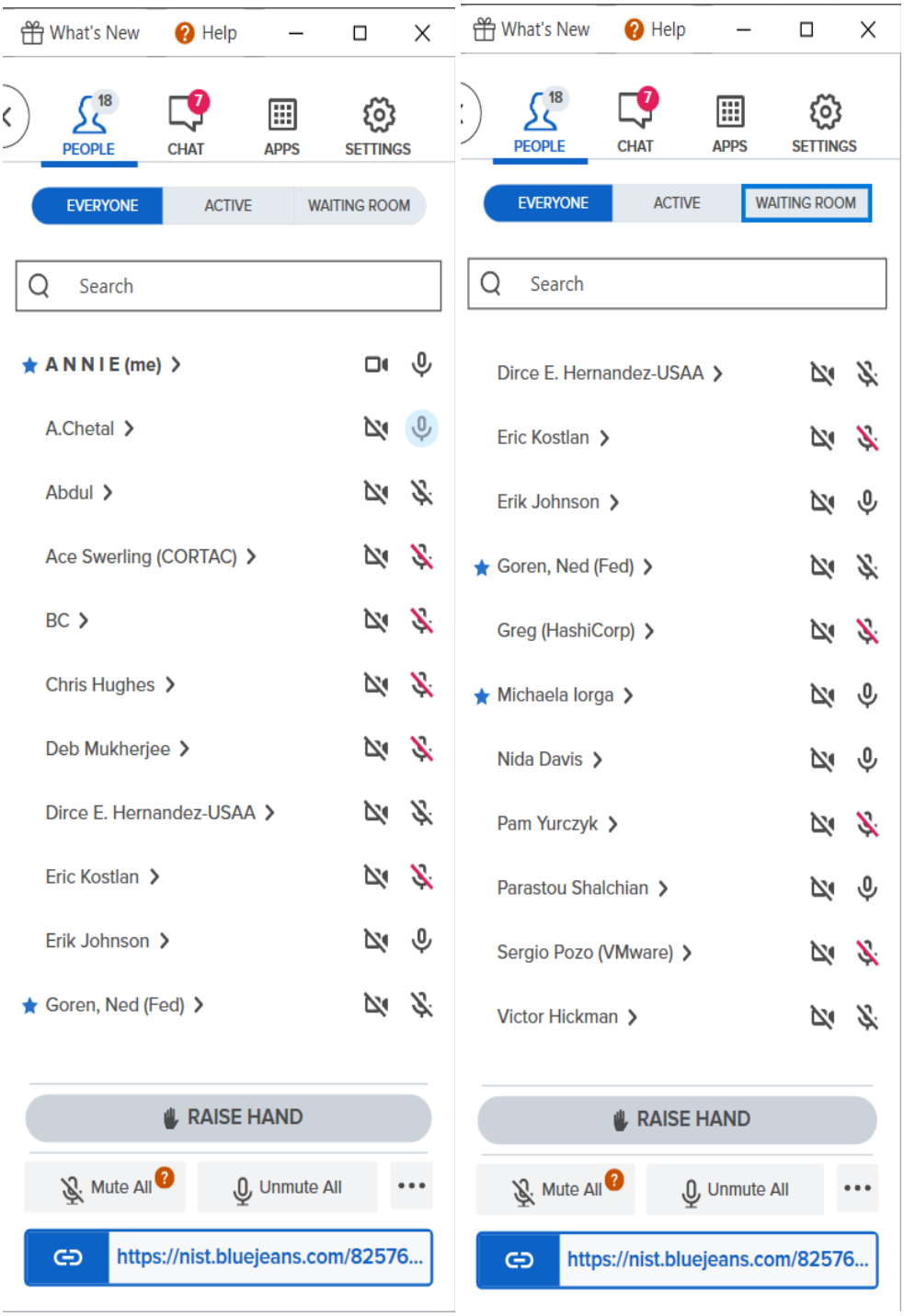
Multi-cloud Security Public Working Group Bi-weekly Meeting (VIRTUAL)
The agenda for each meeting will be included in the email reminder.
Please feel free to propose items for the agenda by emailing those topics to us at mcsec@nist.gov
The charter of the WG**: https://csrc.nist.gov/Projects/mcspwg/mcspw-charter**

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

Want to test your video connection?
https://bluejeans.com/111

Annex B

Meeting #08 Attendees



Annex C

Meeting Chat

MCSPWG

May 16, 2022

(3:03 PM) Dirce E. Hernandez-USAA: I can hear you :)

(3:04 PM) BC: Hello!

(3:05 PM) Sergio Pozo (VMware): hi everyone!

(3:07 PM) A.Chetal: yes a recap from last meeting will be great

(3:09 PM) Greg (HashiCorp): Hi everyone.

(3:11 PM) A.Chetal: Can we get the written notess

(3:11 PM) A.Chetal: so we can agree

(3:13 PM) Parastou Shalchian: I assume the impact level for the multi cloud system will refelct the highest watermark, correct?

(3:14 PM) Nida Davis: Parastou ... let us discuss

(3:16 PM) Nida Davis: It is in the domain of the team

(3:18 PM) Parastou Shalchian: how can i unmute?

(3:22 PM) Erik Johnson: As I recall the discussion last week around the "single multi-cloud system" topic there were questions raised around whether that could translate into a single ATO boundary based on a single SSP.

(3:22 PM) Nida Davis: correct Erik

(3:24 PM) Greg (HashiCorp): Sadly, I have to leave at 3:30 will read the notes. Thanks for continuing the conversation.

(3:24 PM) Nida Davis: Thank you Greg

(3:24 PM) Nida Davis: A system of sub-systems

(3:24 PM) Erik Johnson: While its seems clear that a holistic, end-to-end architectural view of the multi-cloud system is appropriate, it may not translate well into a single ATO boundary.

(3:25 PM) Nida Davis: I agree Erik - will be challenging

(3:26 PM) Erik Johnson: Boundary: Multi-cloud ATO boundary is comprised of an integrated set of different cloud service implementations, each of which has its own distinct SSRM and each of which requires implementation of a full set of cloud controls based on its categorization (sensitivity and data stored/processed).

Consider: Multi-cloud implementations should consider architectures where control capabilities (e.g. IAM) and supporting services (e.g. IDaaS) can be implemented in a common or consistent manner across the different constituent cloud environments for consistency, efficiency, improved usability and single pane of glass operability.

(3:30 PM) Erik Johnson: Unfortunately I have to drop.

(3:31 PM) Nida Davis: Thank you Eric

(3:31 PM) Nida Davis: Erik

(3:35 PM) Ace Swerling (CORTAC): I like this algorithm to help groups converge around a common set of goals.

(3:38 PM) Nida Davis: I. Team 1: ZTA-ICAM, team leads: Gregory Thomas & Katy

II. Team 2: ZTA-AC, team leads: Aradhna Chetal & Swapnil Kulkarni & Sergio Pozo

III. Team 3: RM-ATO, team leads: Angel Phaneuf & Deb Mukherjee

IV. Team4: Continuous Monitoring, Abdul Rahman Sattar

(3:44 PM) A N N I E: will include Michaela's diagram in the minutes

(3:45 PM) Nida Davis: thank you Annie

(3:45 PM) Nida Davis: by way of example, not a prescriptive guidance

(3:46 PM) A N N I E: yes, it is noted as an example

(3:48 PM) Nida Davis: action item - share definition to align

(3:48 PM) A N N I E: ATO is using a diagram from FigJam to build similar questions as shown in Michaela's example

(3:48 PM) Nida Davis: action item - ATO flow diagram / research for options

(3:49 PM) Parastou Shalchian: Would be great to clarify the differences between team 1 and team 2 (ZTA-ICAM and ZTA-AC)

(3:49 PM) Nida Davis: Action item: research diagram sharing

(3:49 PM) Parastou Shalchian: for new members

(3:49 PM) Nida Davis: Parastou after the round, we will do so.

(3:49 PM) Deb Mukherjee: https://www.figma.com/file/8aZPm4VLOKrnVmPie8dfFX/May-13%2C-2022?node-id=0%3A1

(3:49 PM) Parastou Shalchian: thank you!!

(3:50 PM) Nida Davis: yah bi-weekly is good

(3:50 PM) Chris Hughes: Agreed

(3:51 PM) Dirce E. Hernandez-USAA: Agreed with Bi-Weekly

(3:52 PM) Nida Davis: yes that is right

(3:52 PM) A N N I E: Meet on May 23, May 30 is a US public holiday and there is no MCSPWG meeting.

(3:52 PM) Deb Mukherjee: May 23 holiday in Canada

(3:54 PM) Deb Mukherjee: 👍

(3:54 PM) A N N I E: May 23, June 6 bi-weekly

(3:55 PM) Nida Davis: we keep going

(3:58 PM) Nida Davis: we will say conceptually a multi-cloud solution is … xxx

(4:00 PM) Nida Davis: yes

(4:01 PM) Dirce E. Hernandez-USAA: don't forget about security considerations

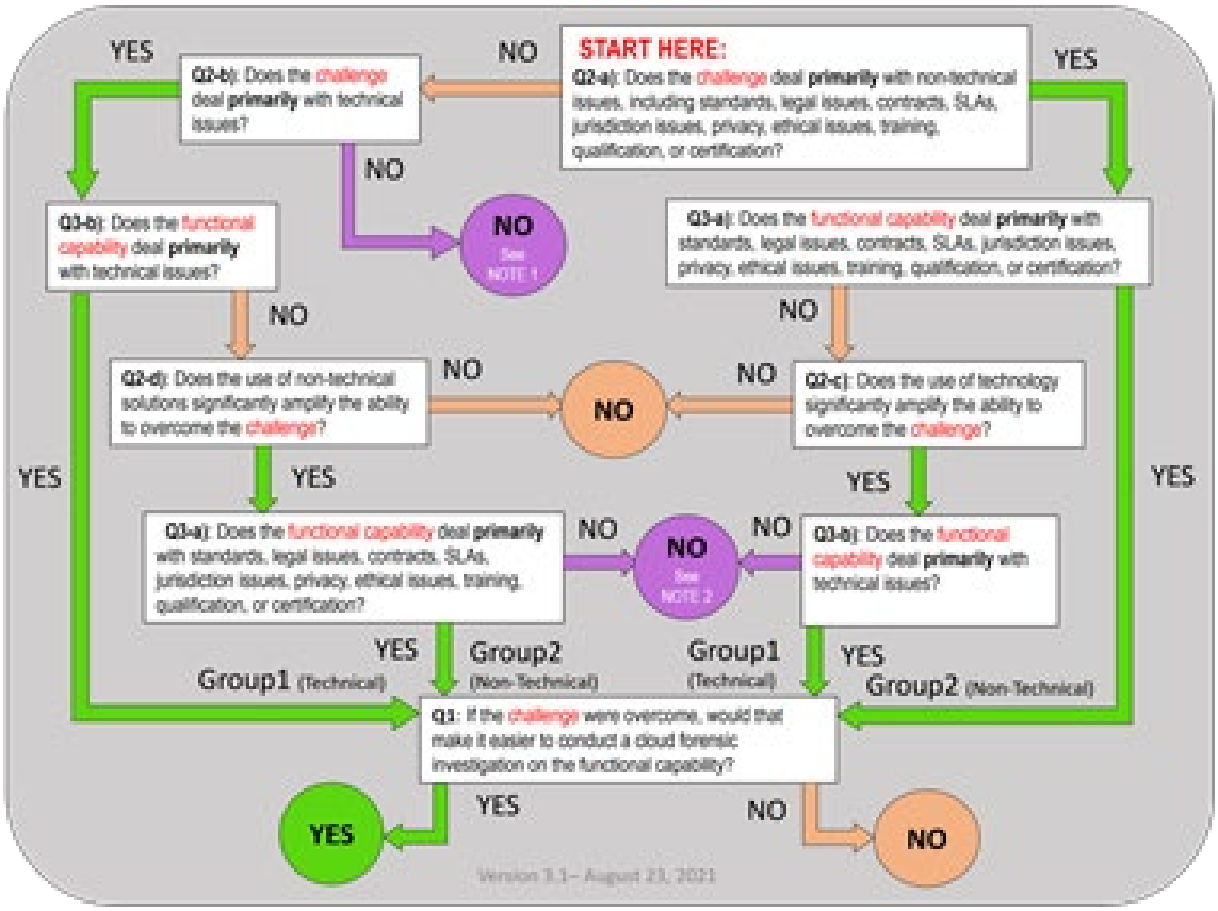
(4:01 PM) Parastou Shalchian: I need to drop for another call. Thank you everyone.

(4:01 PM) Nida Davis: yes

(4:01 PM) Deb Mukherjee: I have to drop off now. Thanks for sharing the diagram pic

Annex D

Michaela Iorga's Example on Research Flowchart from forensic project - https://drive.google.com/file/d/1uvkVnbAmNXQMiuFi0HsG_II2T1DNXPgE/view with additional notes



Annex E

Nida Davis's Post Meeting Contribution (May 2 Meeting)

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:

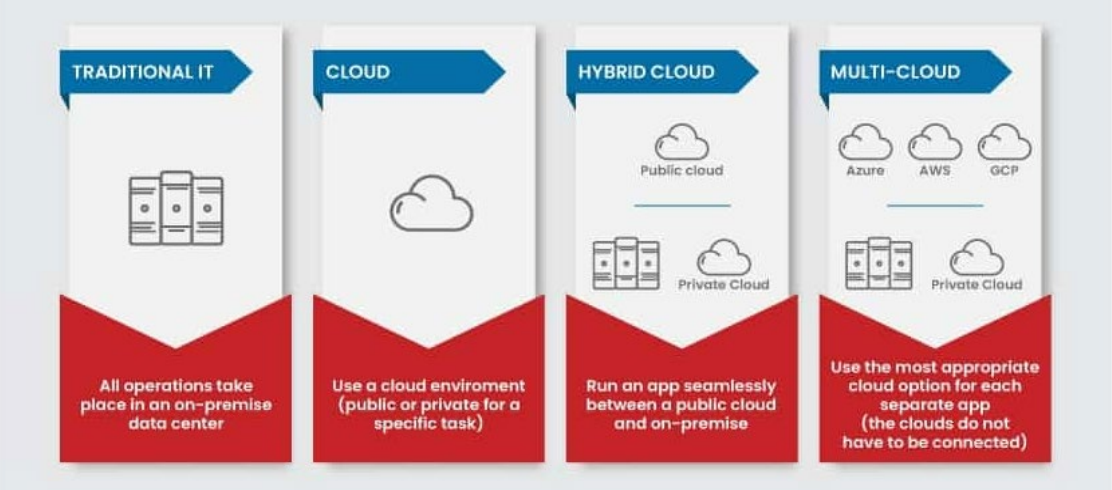
- Service cost.

- 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:

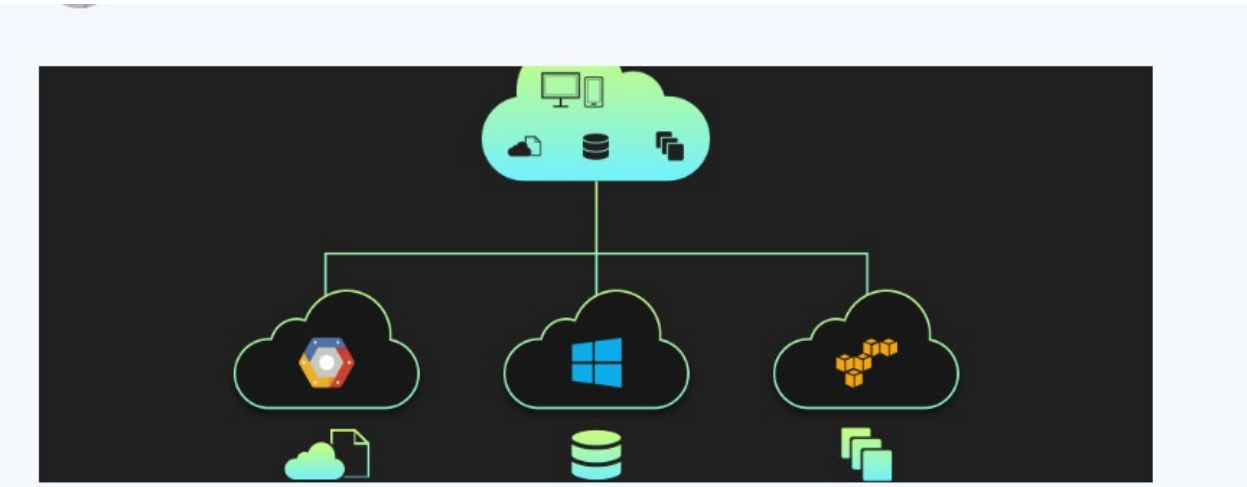
- A company using Google Cloud Platform (GCP) for development and testing while relying on Azure for business analytics.
- An organization using different providers for IaaS, PaaS, and SaaS services.
- A company using Azure in the US and Alibaba in Asia to ensure the app does not suffer from latency.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



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

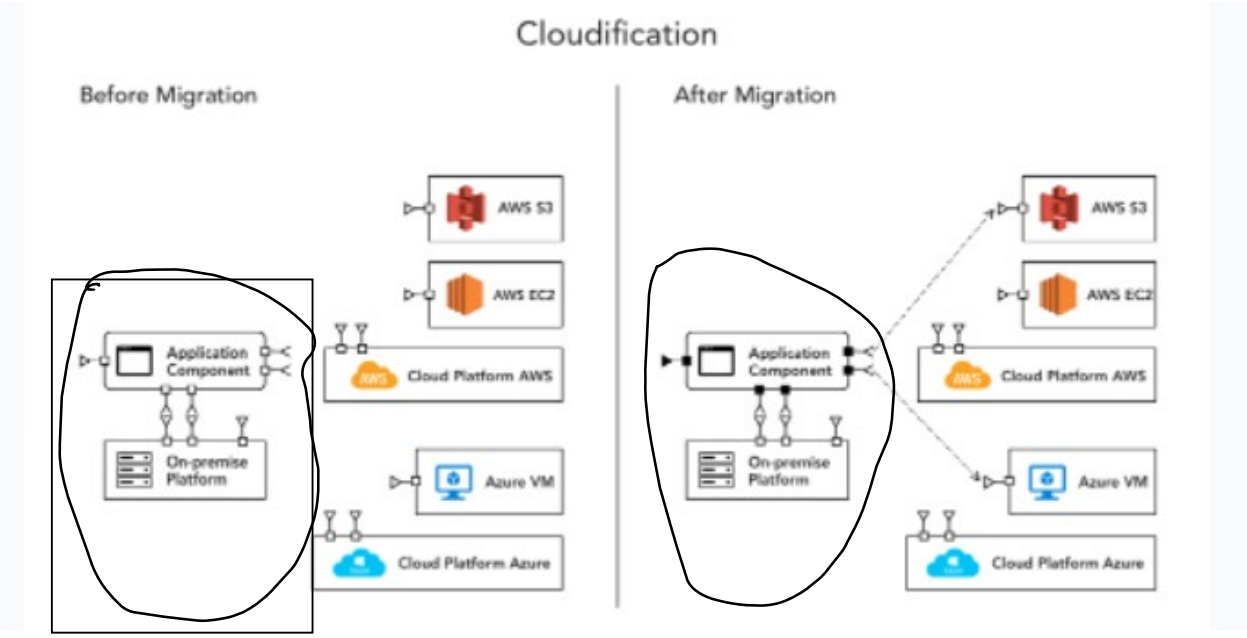
Deploying a multi-tenant application across multiple cloud platforms can be very challenging. In this blog, we've explained 6 multi-cloud architecture designs which can help businesses to build an effective multi-cloud strategy.

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.”



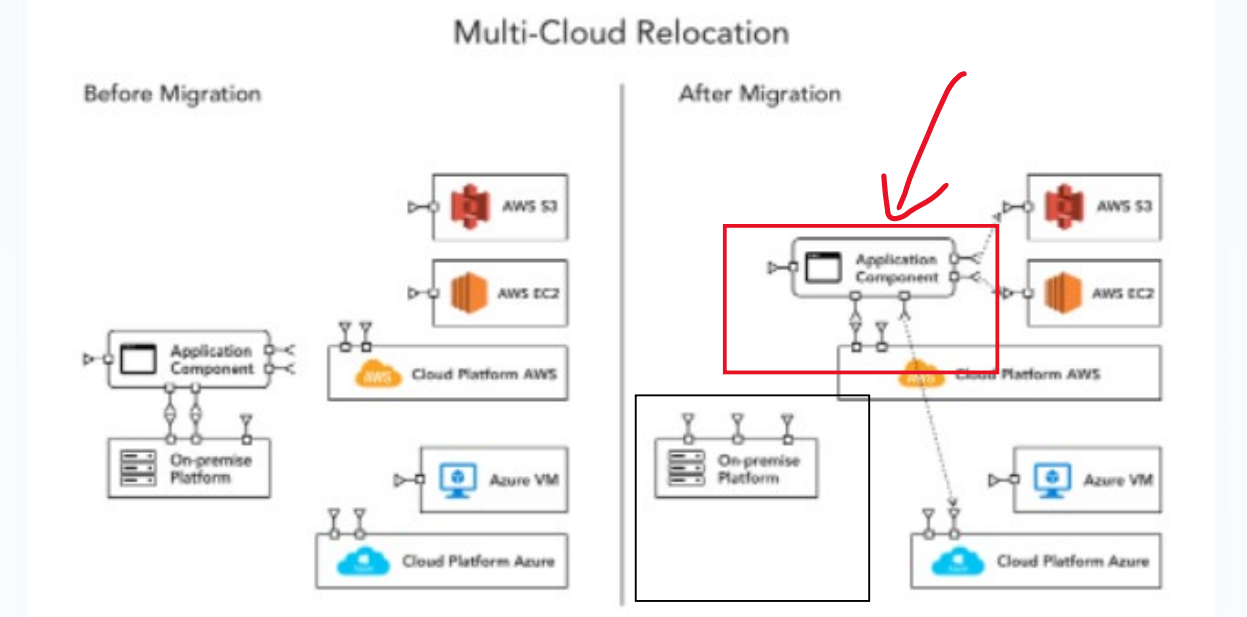
Pattern One: Cloudification

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

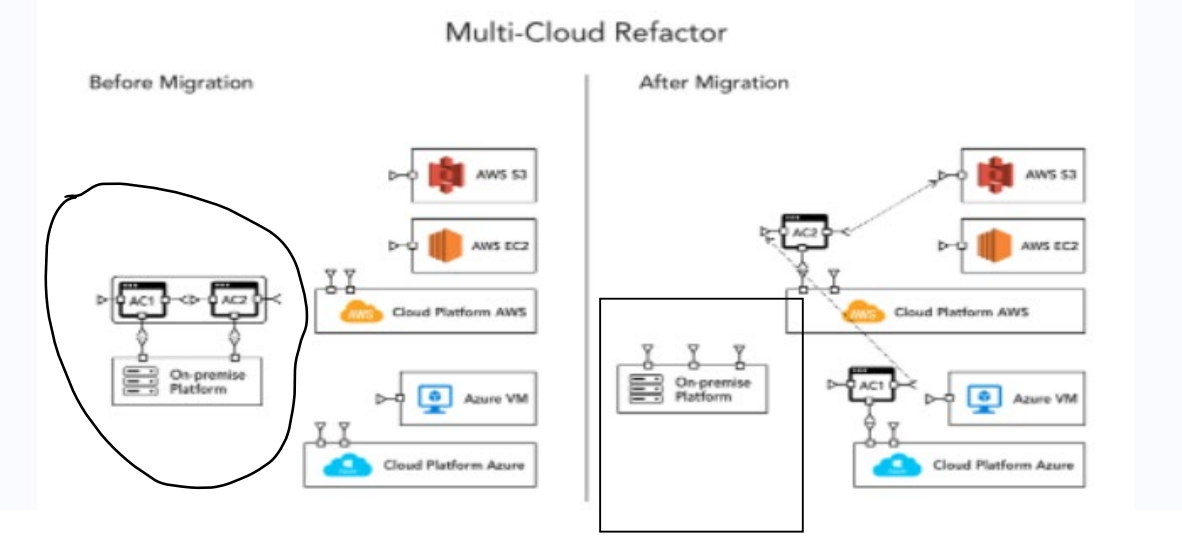
An application component is moved to cloud services to host (AWS Cloud in this example) – application connects to other cloud-based services such as Azure [integration patterns].



Pattern Three: Multi-Cloud Refactor

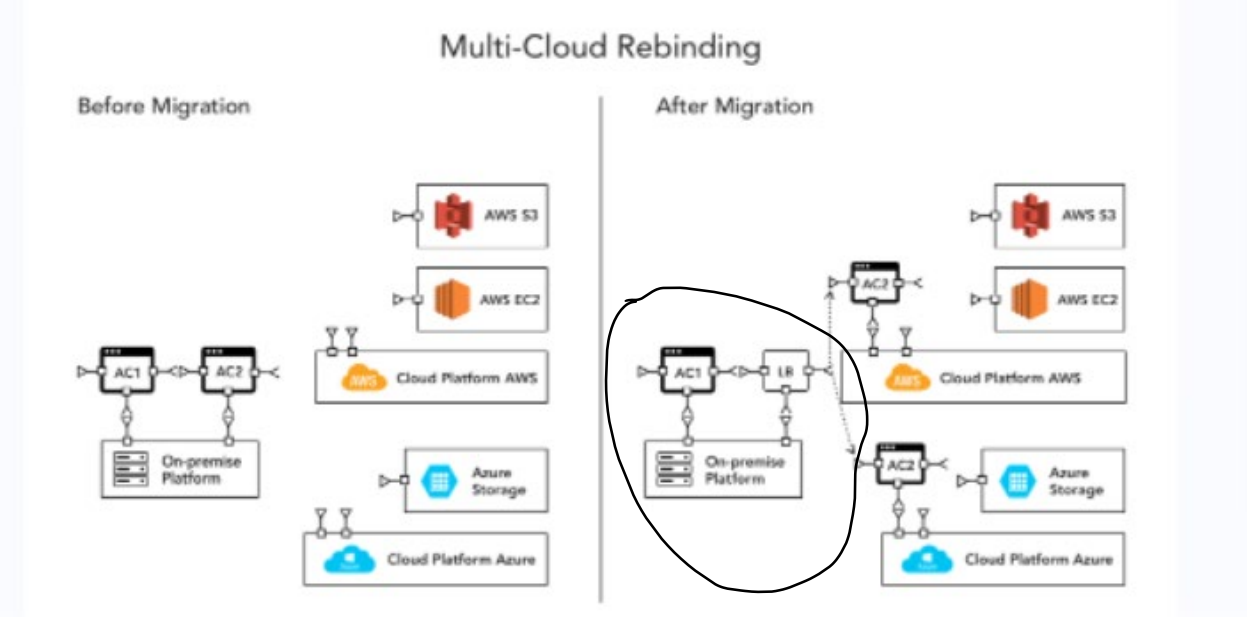
An application (legacy) is rearchitected to optimize performance on multiple clouds:

"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."



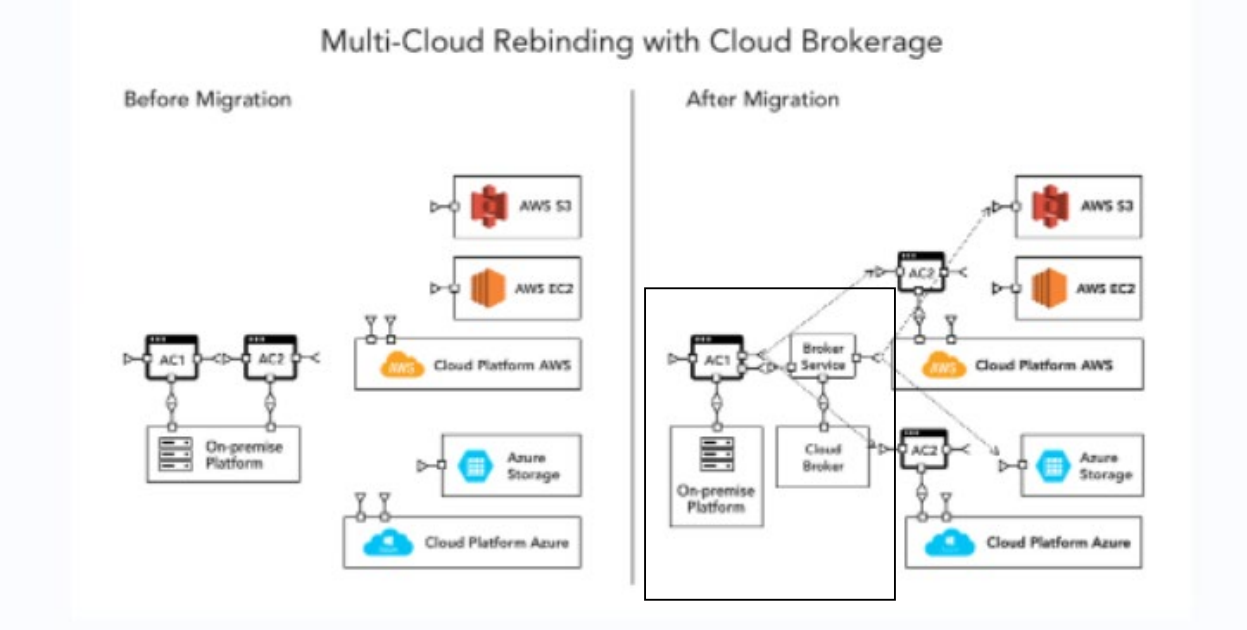
Pattern Four: Multi-Cloud Rebinding

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.



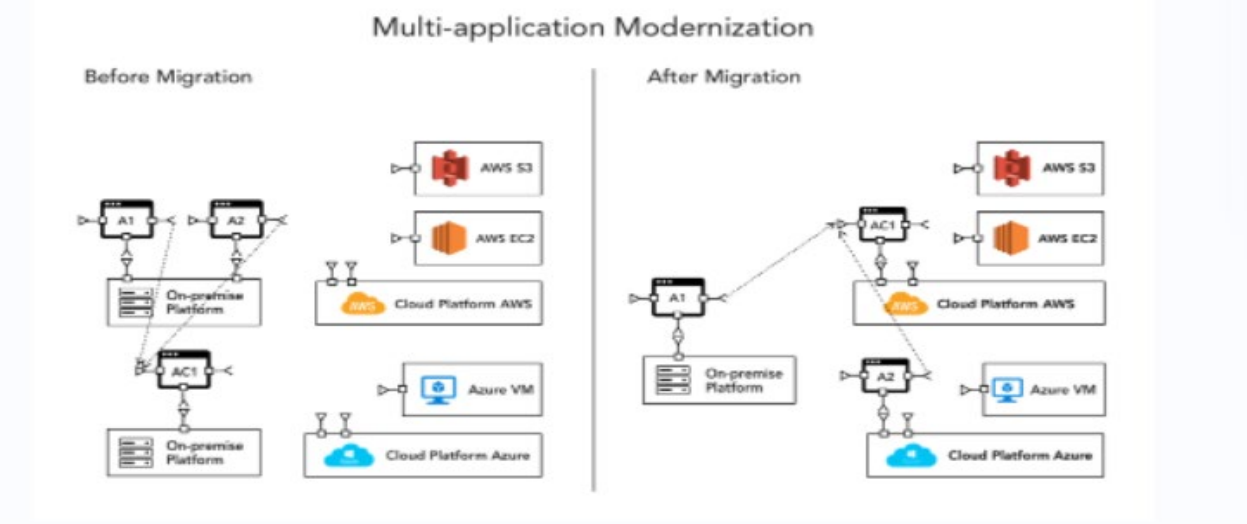
Pattern Five: Multi-Cloud Rebinding with Cloud Brokerage

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).

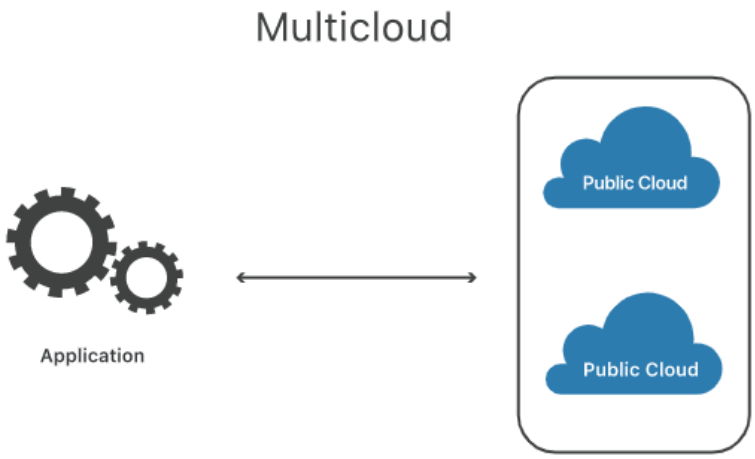
Out of SCOPE: Cloud Service Provider – to – Cloud Service Provider linkages and connections (virtual or physical) that are not part of the scope definition of the system = (application/components/interfaces / DB) or are clearly defined as the responsibility of the Cloud Service Provider duty to manage.

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

.

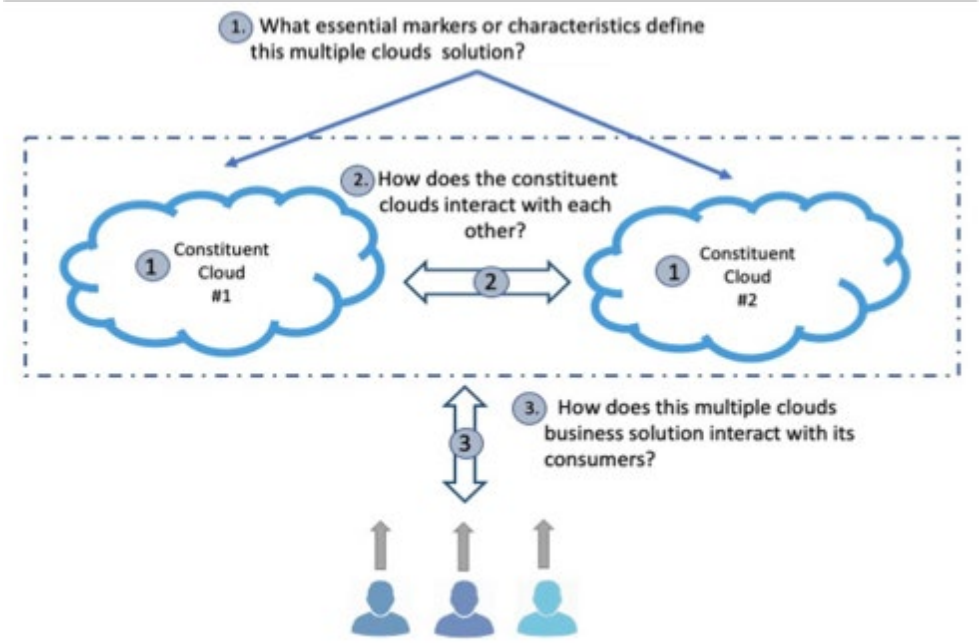
Annex E

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 model:** 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.*