Disaster Recovery as a Service

cloud security alliance®

The permanent and official location for Cloud Security Alliance Security as a Service research is https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/.

Acknowledgments

Lead Authors:

Michael Roza
Balaji Karumanchi
Shobhit Mehta

Contributors:

Ashish Vashishtha
Brian Zawada

CSA Global Staff:

Shamun Mahmud
Stephen Lumpe (cover artwork)

Special Thanks:

Bowen Close

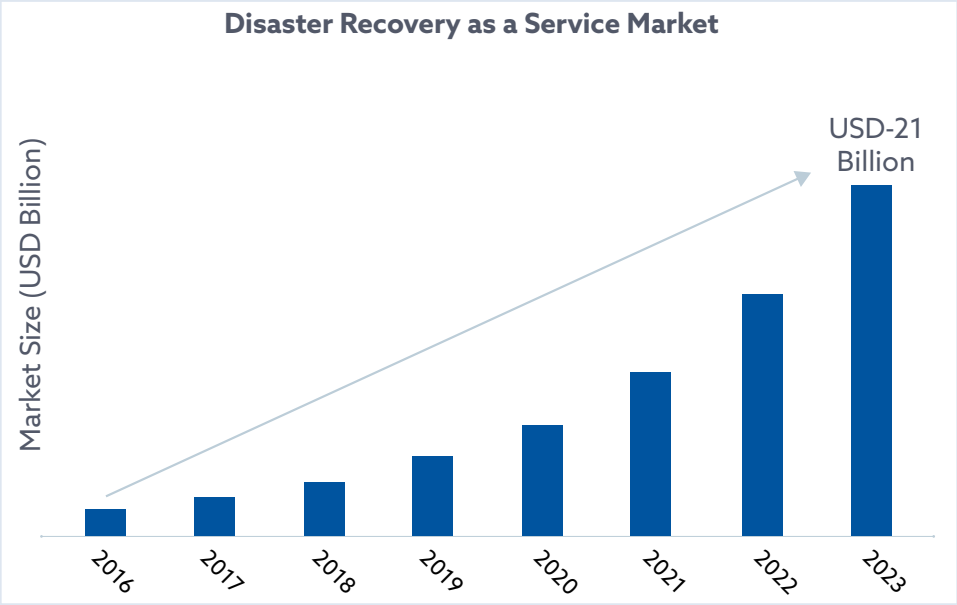
Table of Contents

1. Introduction

Disaster Recovery as a Service (DRaaS) is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment.[1] This as-a-service model enables an organization to regain access and functionality to its IT infrastructure after a disaster.

Backup, making an extra copy (or multiple copies) of data in case data is accidentally deleted or corrupted, is often offered as a standalone service. However, this service does not allow access to the applications necessary to run the business.

Gartner defines the **Disaster Recovery as a Service (DRaaS) Market** as a productized service offering in which the provider manages server image and production data replication to the cloud, disaster recovery runbook creation, automated server recovery within the cloud, automated server failback from the cloud, and network element and functionality configuration, as needed. Source servers supported must include a combination of both virtual and physical servers. To be considered DRaaS versus other options that enable do-it-yourself recovery, all elements of the service must be included in the service offering contract between the provider and customer and offer a standardized SLA for recovery.[2]



Source: Market Research Future - Disaster Recovery as a Service Market

1 VMWare, Disaster Recovery as a Service (DRaaS), https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas
VMWare, Disaster Recovery, https://www.vmware.com/topics/glossary/content/disaster-recovery

2 Gartner, DRaaS (Disaster Recovery as a Service) Reviews and Ratings, https://www.gartner.com/reviews/market/disaster-recovery-as-a-service

The Disaster Recovery as a Service (DRaaS) Market is expected to grow at a CAGR of 44% reaching $21.62 billion by 2023.

DRaaS are offered primarily in one of three service categories: Self Service DRaaS, Assisted DRaaS, and Managed DRaaS. One category may overlap with another due to SLA (Service Level Agreement) negotiations.

Responsible	Self-Service DRaaS	Assisted DRaaS	Managed DRaaS
Customer	• Creating the Disaster Recovery plan • Testing their processes • Managing backups and replication • Managing recovery • Responsible for Recovery Point Objective (RPO) and Recovery Time Objective (RTO) • Hosting infrastructure in a remote location • Maximum acceptable outage (MAO) • Maximum tolerable period of disruption (MTPD) • Minimum business continuity objective (MBCO)	• Creating the Disaster Recovery plan • Testing their processes • Managing backups and replication • Managing recovery • Responsible for Recovery Point Objective (RPO) and Recovery Time Objective (RTO) • Hosting infrastructure in a remote location • Maximum acceptable outage (MAO) • Maximum tolerable period of disruption (MTPD) • Minimum business continuity objective (MBCO)	• Customer IT possibly but not necessarily working with the provider to perform some recovery procedures
Provider	• No Responsibility	• Provide expertise in creating and implementing the Disaster Recovery plan	• Creating the Disaster Recovery Plan • Managing Disaster Recovery testing • Managing backups and replication • Managing 24/7/365 failover • Responsible for Recovery Point Objective (RPO) and Recovery Time Objective (RTO) • Hosting infrastructure in a remote location

1.1 Purpose

The purpose of this paper is to discuss some of the architectures available, the services offered, and the considerations and best practices to ensure that an organization can back up its data and IT infrastructure making it possible to regain access and functionality after a disaster.

1.2 Goal

This document aims to increase awareness of changes in Backup and Disaster Recovery services and technologies of late, the architectures they are designed to Backup and Recover, and the challenges faced, and finally, to provide recommended best practices to overcome these challenges.

1.3 Scope

In the context of this publication, we focus on the aspect of BC/DR that addresses the recovery of IT systems and services as provided by service providers and other third parties. This as-a-service model is often referred to as DRaaS. The broader recovery of a business often referred to as business continuity (BC) is not within the scope of this document.

1.4 Target Audience

This document has been written for system auditors, system engineers, system architects, system implementers, system administrators, project planners, project coordinators, cloud architects, cloud engineers, and cloud administrators of private/public/hybrid/community cloud consumers and anyone interested in the recovery of IT systems and services as provided by service providers and other third parties.

2. Architectures[3]

There are four architectural models reviewed in the following sections: one Non-DRaaS Model — In-House Own Data Center No Cloud — and three DRaaS Models — In-House Own Data Center with Cloud, Hybrid Cloud, and Multi-Cloud.

2.1 In-House Own Data Center No Cloud

Architecturally, traditional DR consists of backing up and recovering from an organization's own data center or from a second site they own or a site that is hosted/co-located. The systems will still be hosted on-site and, depending on the model/service chosen, some or all of the data and systems will be replicated to a contingency site. Figure 1 shows how traditional systems can be replicated to a contingency site for DR, and how they then would replicate to the primary facility once the situation is returned to normal.[4]

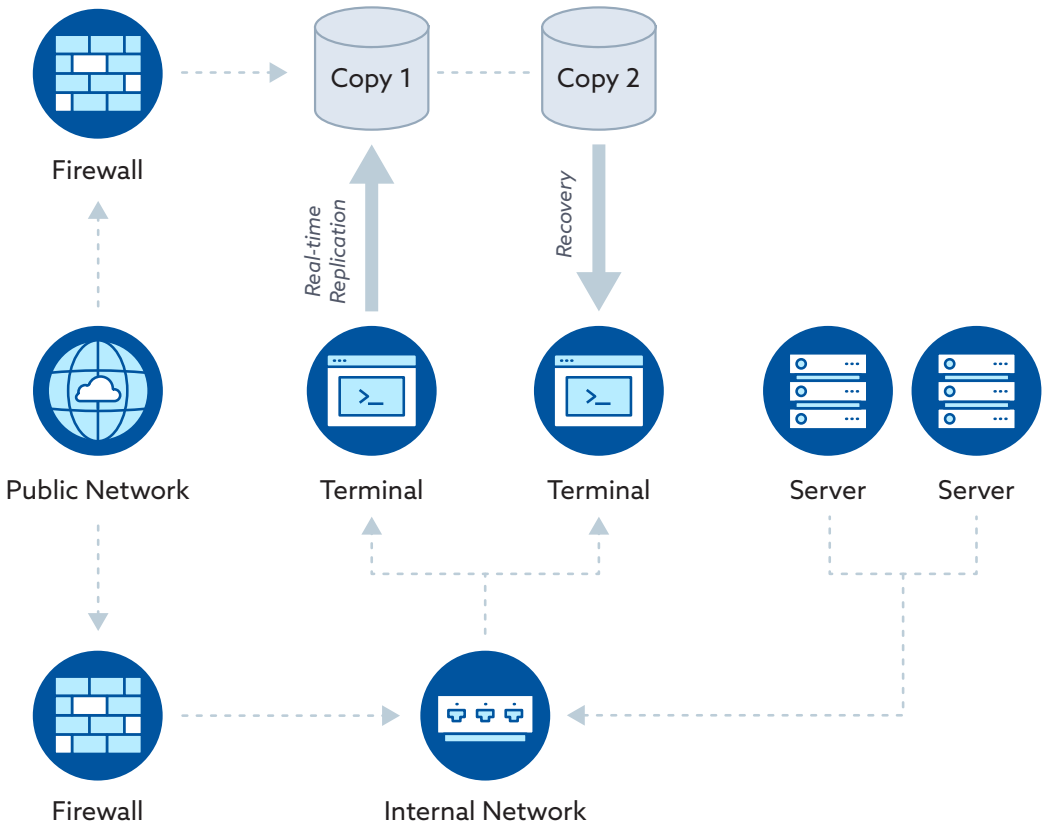


Figure 1: Traditional System to CSP Replication and Recovery

3 See Appendix 1 and 2 for NIST and ISO Cloud Architecture Definitions.

4 Cloud Security Alliance 2012, SecaaS Category 9, BCDR Implementation Guidance, https://cloud-securityalliance.org/artifacts/secaas-category-9-bcdr-implementation-guidance

The advantages of this architecture are that

- physical control over backup is kept in-house; and
- third-party access is limited and controlled.

The disadvantage of this architecture is that

- significant capital investment in hardware, software, and human resources is required.

2.2 In-House Own Data Center with Cloud

This architecture retains a copy of data in local storage (i.e. on-premise), and the organization also replicates the data to a CSP's datacenter. Using a CSP for data storage enables the organization to utilize the benefits of the high availability and durability that the CSP guarantees without investing in additional hardware, software, and human resources.

This architecture is ideal for archiving data that is not immediately required. For example, the audit logs from various systems can be stored locally for inspection but can be archived to cloud storage once the exercise is complete in case future retrieval is required.

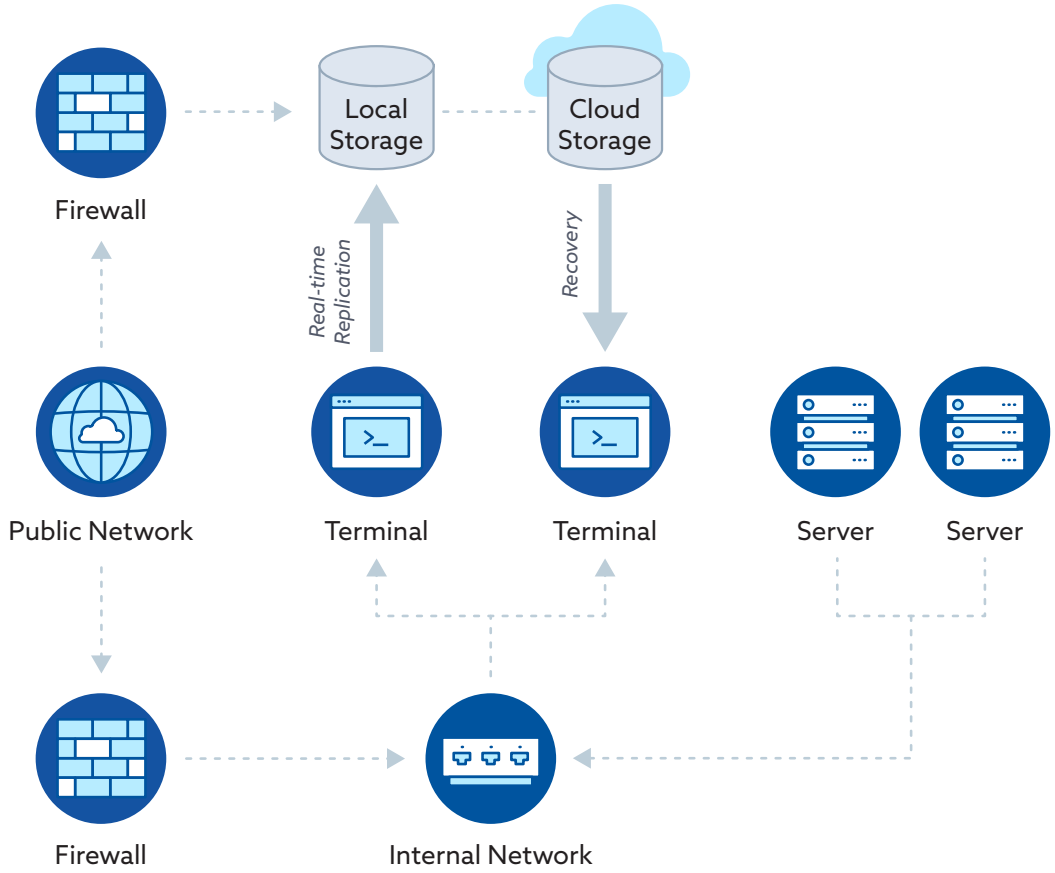


Figure 2: Data Center to Cloud Disaster Recovery

The advantages of this architecture are that

- backing up can be less expensive in the cloud when compared to an in-house environment;
- backing up is also easier as the service provider assumes many responsibilities;
- backups are performed outside the office network making them less Ransomware vulnerable;
- cloud backups help lower the risk of common data backup failures caused by improper storage, physical media damage or accidental overwrites; and
- backed up data is accessible from anywhere.

The disadvantages of this architecture are that

- physical control over data is moved outside the customer's confines;
- expenses can increase substantially as the amount of data backed up increases;
- multiple customers backing up simultaneously can slow the backup process; and
- multiple customers restoring simultaneously can slow the restoration process.

2.3 Hybrid Cloud

The Hybrid Cloud approach can prove to be advantageous for an organization's Disaster Recovery Strategy. Businesses have the opportunity to use the private cloud infrastructure for real-time replication and use public cloud storage for recovery. They can do this by making use of privately managed infrastructure as well as the public cloud.

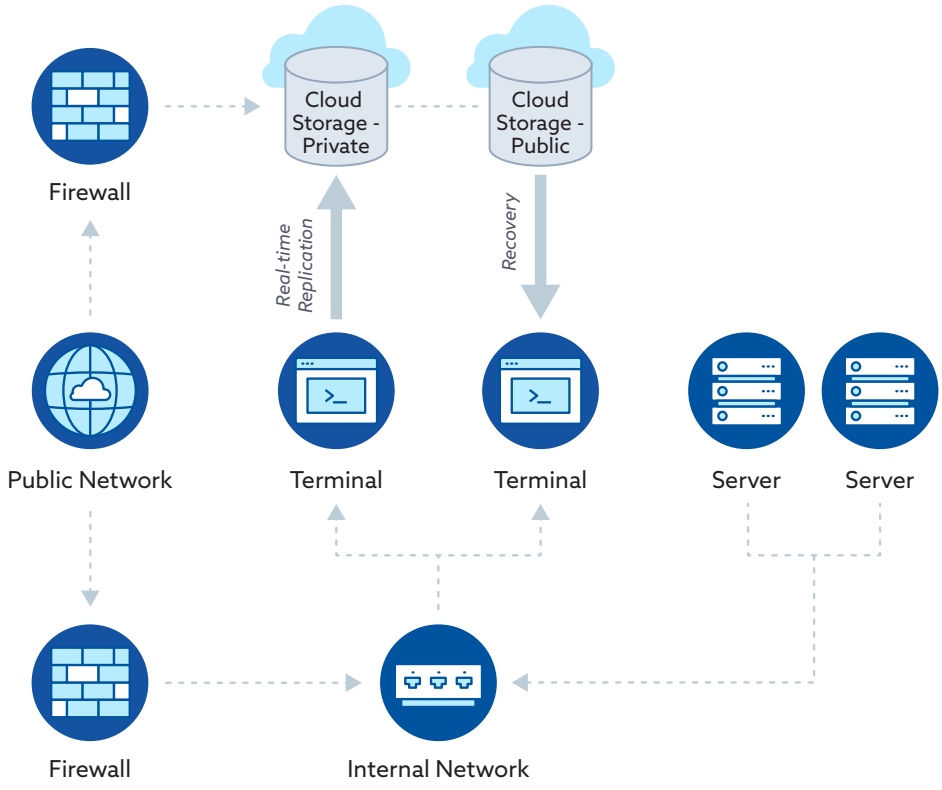


Figure 3: Hybrid Disaster Recovery

While the Hybrid Cloud retains the advantages and disadvantages listed in section 2.3 above, important additional considerations with respect to the Hybrid Cloud are

- minimization of vendor lock-in: cost, availability, performance;
- optimization of geographical dispersion: data governance restrictions, disaster risk management; and
- maximization of application use: taking advantage of containers and microservices modular architectures.

2.4 Multi-Cloud

Using Multi-Cloud Disaster Recovery enables the customer to replicate resources to a second cloud provider in another geographic region. This ensures that there is limited risk that both cloud providers will undergo a major outage at the same time.

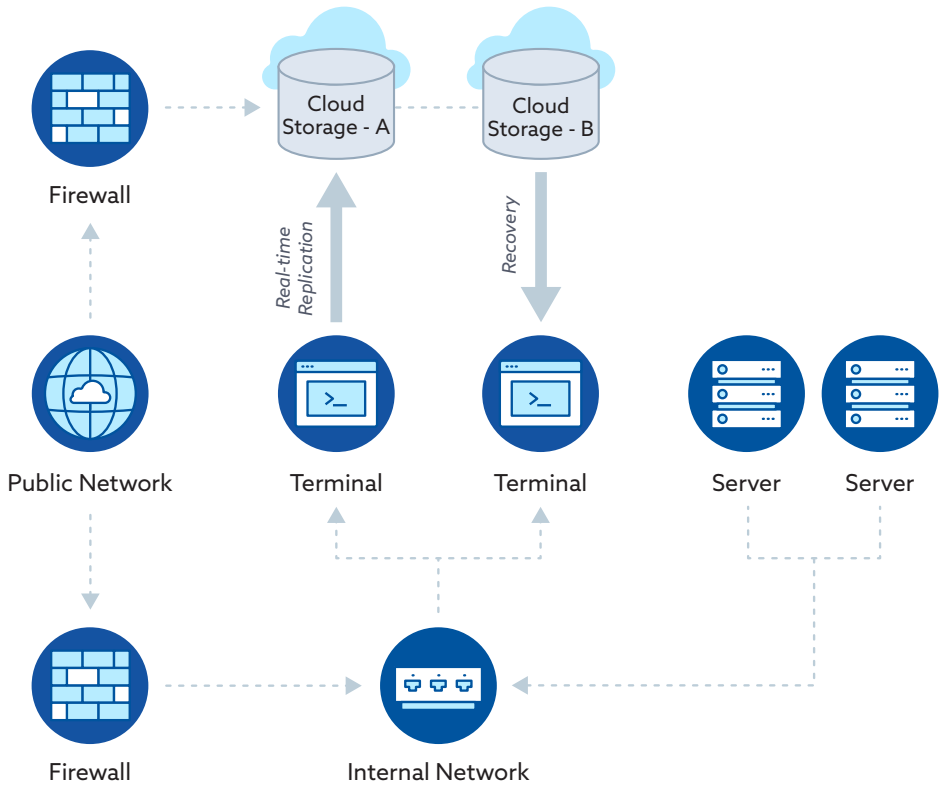


Figure 4: Multi-Cloud Disaster Recovery

While the Multi-Cloud approach retains many of the advantages and disadvantages listed in section 2.3 and consideration in 2.4 above, there are challenges in using Multi-Cloud DR:

- Each cloud provider has its own management portal and different services that require different skill sets.
- For example, for IaaS implementations, different cloud providers use different on-disk formats for their VMs. Microsoft Azure uses the VHD format while AWS uses the AMI format.

- As a general rule, each cloud provider's DR services are not designed to deal with multiple cloud providers. However, some third-party DR solutions are able to bridge multiple clouds making it far easier to implement a multi-cloud DR strategy.
- If an organization wants to implement a multi-cloud DR plan it's best to begin with a smaller scoped POC before expanding to the rest of the organization.
- Like all DR plans, regular testing is a must.

3. Services

Backup and Disaster Recovery, whether performed as a service or in-house/on-premise can be performed using a variety of methods as follows:

3.1 Object-Level Storage for Backups

Object-based storage is a backup strategy that generates a backup of data as a single object. The object is stored using the metadata,[5] which eliminates the tiered file structure used in file storage, and puts everything in a flat space address known as a storage pool. Most of the larger CSPs provide object-level storage via Infrastructure-as-a-Service (IaaS) offerings that can be used for DR, as shown in Figure 5. Often, small-to-mid-sized businesses (SMBs) will leverage this model to store locally executed backups remotely instead of using backup tapes, offsite storage vendors, and couriers.

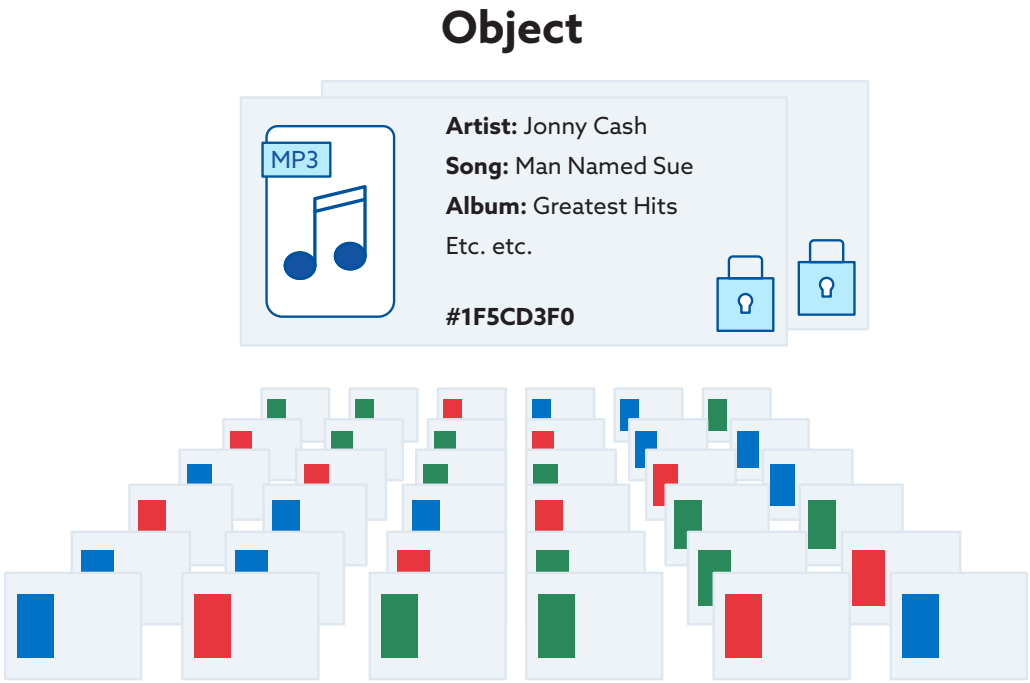


Figure 5: Object-Level Storage for Backups

The diagram above shows how the objects are stored in the cloud computing environment. Each object in the diagram represents a file and each file is stored in its separate object.

5 Google Cloud, Object Metadata, https://cloud.google.com/storage/docs/metadata

3.2 Block/Volume-Level Storage for Backups

Cloud consumers may use block/volume-level storage for DR purposes when leveraging IaaS computer services. Block-level replication is likely more bandwidth efficient than object-level replication, so it will often require a smaller link to the CSP and be either more feasible, lower cost, or both. Many IaaS vendors support backup and DR using block/volume-level storage. These blocks are backed up using replication within the available zone. In IaaS architecture, block storage replication works like the RAID infrastructure in the datacenter. RAID protects the storage environment both logically and physically to prevent it from corruption or deletion, which might occur due to human error, software malfunctioning, or electrical spike. An example of this service infrastructure is shown below in Figure 6.

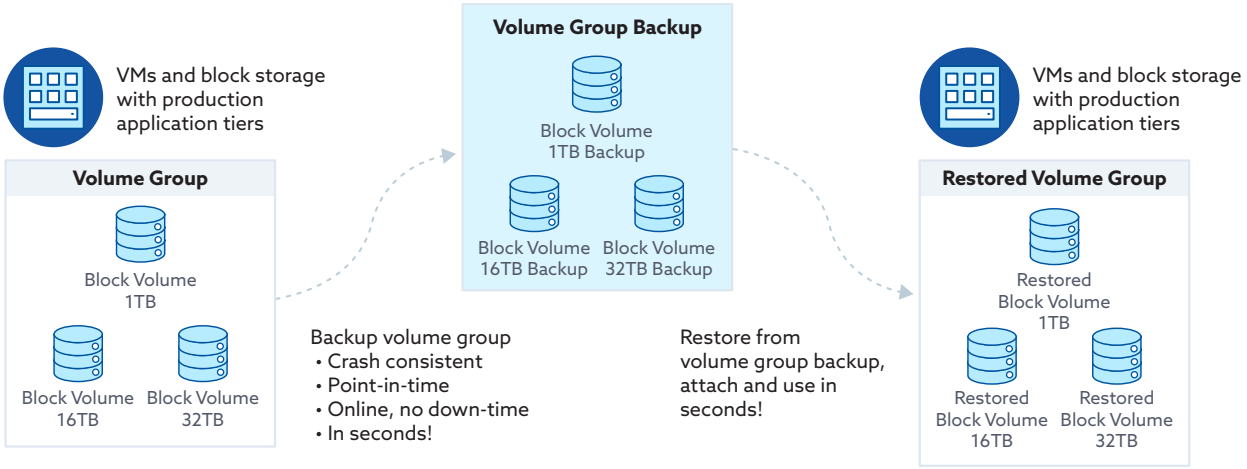


Figure 6: Block/Volume-Level Storage for Backups

The diagram shown above represents the block/volume storage structure in the oracle cloud known as a volume group feature to create block volume backup. The model works by generating the volume backup in multiple groups that generate multiple volume blocks. The collection of multiple volumes in one block and this procedure create a collection of multiple and consistent volume backups. It also generates clones of the backups. In case of any disaster, the entire group can be restored from the cloud.

3.3 PaaS – Replicated Database Instances

In PaaS, centralized DBs (Databases) are connected with replicated DB instances, which helps various systems simultaneously backup. Most of the companies are using PaaS as replicated DB instances. Replication of DB over the cloud is costly, but this system helps load balancing and cost-effectiveness. For example, by installing an instance of the DB software on an IaaS O/S instance, the client may utilize any database software and version, rather than relying on the existing PaaS offerings. In this instance, the client would be responsible for managing replication via technologies such as mirroring or log shipping. These databases in the cloud also can be provided via an IaaS style implementation. Figure 7 given below nicely represents the replication of the database system, the load

balancer layer, and the container layer. The user request moves to the database, which generates the two instances — one locally and one for the replicated DB — which stores data on the cloud.

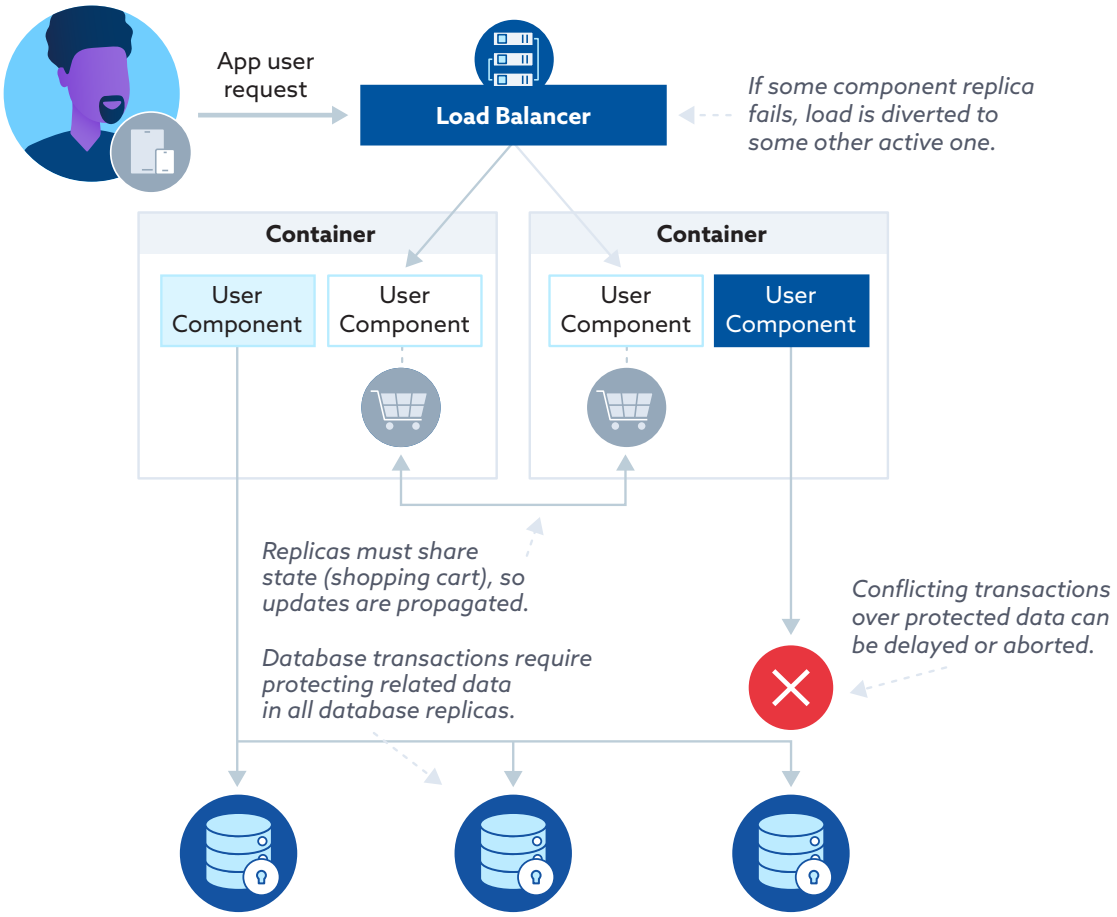


Figure 7: PaaS – Replicated DB Instances

3.4 IaaS – Replicated OS Instances

IaaS is a cloud service for Backup and DR, which allows the customer to automatically provision servers, storage, and network access via an interface or to use some application based on charges. It provides the complete infrastructure, which is the best fit for the changing needs of the organization. The environmental infrastructure of IaaS is based on the Virtual Machine (VM), which is connected with cloud systems. This system works in three layers. The physical layer consists of VMs, the second layer consists of the management of APIs, and the last layer consists of storage, which allows the user to store data on the cloud using different techniques.

IaaS provides a range of services to accompany the infrastructure components, including detailed billing, monitoring, log access, security, load balancing, clustering, and storage resiliency, such as backup, replication, and recovery. These services are increasingly policy-driven, enabling IaaS users to implement greater automation and orchestration for essential infrastructure tasks. IaaS customers

can access resources and services through a wide area network (WAN), as shown in Figure 5 below, such as the internet, and can use the cloud provider's services to install the remaining elements of an application stack.

For example, the user can log in to the IaaS platform to create virtual machines VMs; install operating systems in each VM; deploy middleware, such as databases; create storage buckets for workloads and backups; and install the enterprise workload into that VM. Customers can then use the provider's services to track costs, monitor performance, balance network traffic, troubleshoot application issues, manage disaster recovery, and more.

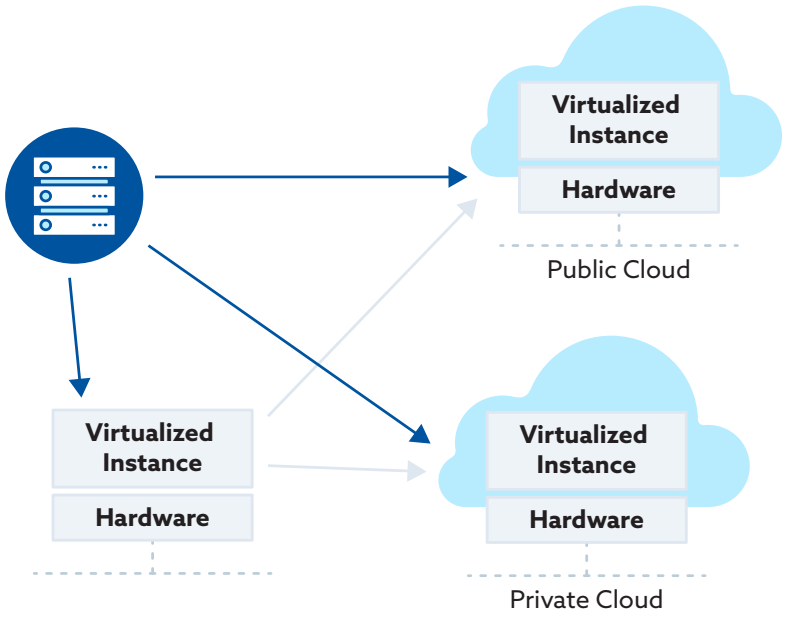


Figure 8: IaaS – Replicated OS Instances *(On Slides)*

3.5 PaaS – Application Failover

Platform-as-a-Service (PaaS) is a type of cloud computing service provided by the service provider to its clients with a complete environment hosted on the cloud, which consists of development environments, managed custom applications, and software deployment processes. This model works in the hidden layer of infrastructure, which keeps away the developers and users. This model is also known as serverless computing and function-as-a-service (FaaS), in which the cloud allows the customer to run allocated resources.

Platform-as-a-Service (PaaS) environments offer businesses scalable application containers that can operate across a multitude of infrastructures. In contrast to IaaS, PaaS offers greater built-in resilience for applications because it creates a further abstraction away from guest operating system environments. PaaS provides a greater homogeneity level, but often at the cost of requiring applications to be modified for operation within the specific PaaS environment.

Due to the greater abstraction, PaaS has the added benefit of more easily deploying across cloud service and deployment models. Some IaaS environments force a specific guest operating system architecture upon the user, making it difficult to share a single image across multiple service providers. The PaaS abstraction allows a single application image to operate on all these IaaS, thus allowing cloudbusting, on-demand scaling, service provider redundancy, and geographic independence. These attributes enable greater business continuity levels and disaster recovery at much lower costs than traditional DR using redundant owned or leased data center environments.

Many PaaS environments can naturally load balance and scale across PaaS node instances that are geographically dispersed. As with any redundant application architecture, load balancing, DNS, and identity management services need to be able to failover accordingly. Assuming these services are also highly available, the interoperable nature of PaaS means that the application will be accessible. Figure 9 below illustrates the behavior of a system during failover.

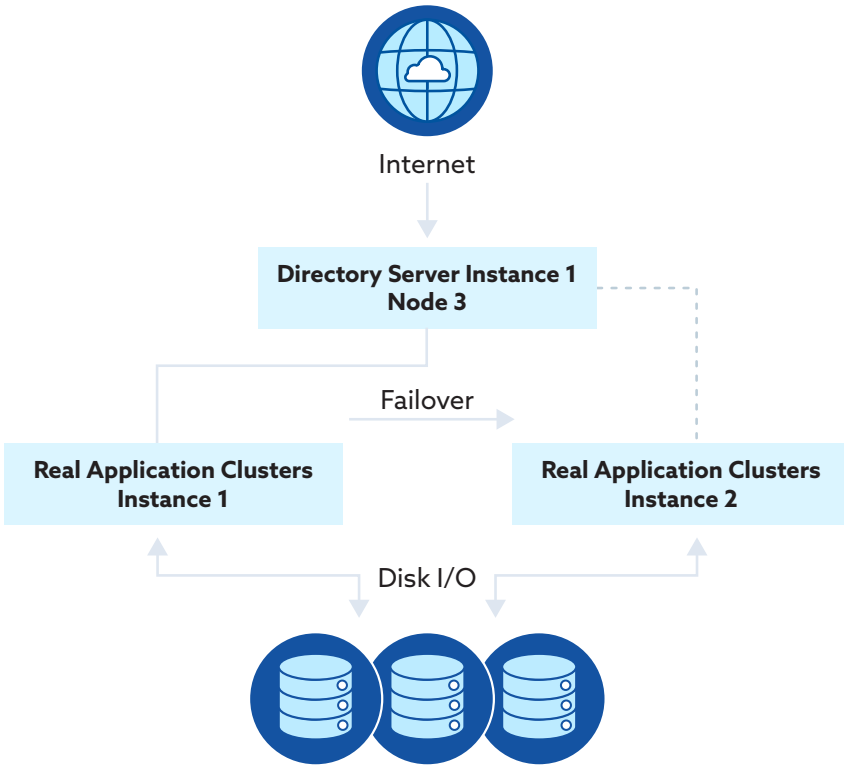


Figure 9: PaaS – Application Failover

3.6 SaaS – Replicated File-Level Storage for Clients/ Hosts Backups

CSPs typically have automated methods to back up and sync data to offsite locations as shown in Figure 10. The only requirement for an administrator or user is to install and configure the solution for the backup jobs; backups are conducted at specified intervals. These solutions are convenient and cost effective. However, the need for a consumer to test the backups is extremely important. The backup process should be tested every six months.

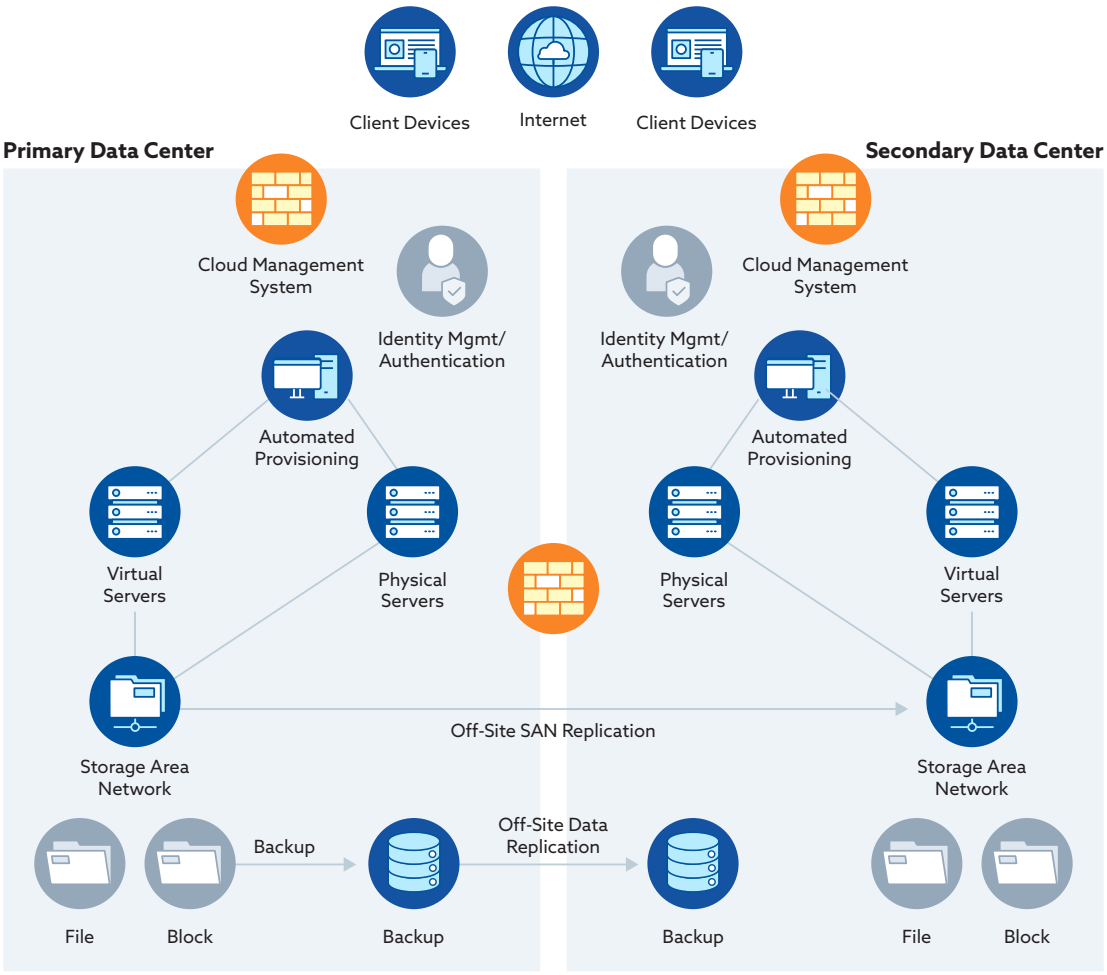


Figure 10: SaaS – Replicated File-Level Storage for Clients/Hosts Backups

In the above architecture, the model describes the replicated file-level storage both on-site and off-site. The primary data center is connected with the cloud management system which connects with the virtual servers and physical servers. The backup process first begins from the off-site data back-up, which is then replicated in both forms as block and file to the cloud repository.

3.7 Cloud-Based Systems Recovery

For businesses whose systems are already hosted in the cloud, it is recommended that they leverage the inbuilt DR capabilities provided by the CSP. Most CSPs will offer, at a minimum, automated replication, and the ability to automatically (or at least quickly) failover systems, even when using an IaaS-based solution. This option means that the customer must contractually specify the resources required at the DR site, define the level of ramp-up if DR is invoked, and understand the repercussions of failing over to another location, including its effects on customers and partners. The big benefit of the RaaS solution is that there is little or no actual implementation or architectural work required of the consumer as given in Figure 11. Requirements of the customer are limited to contractual design, scaling, and testing.

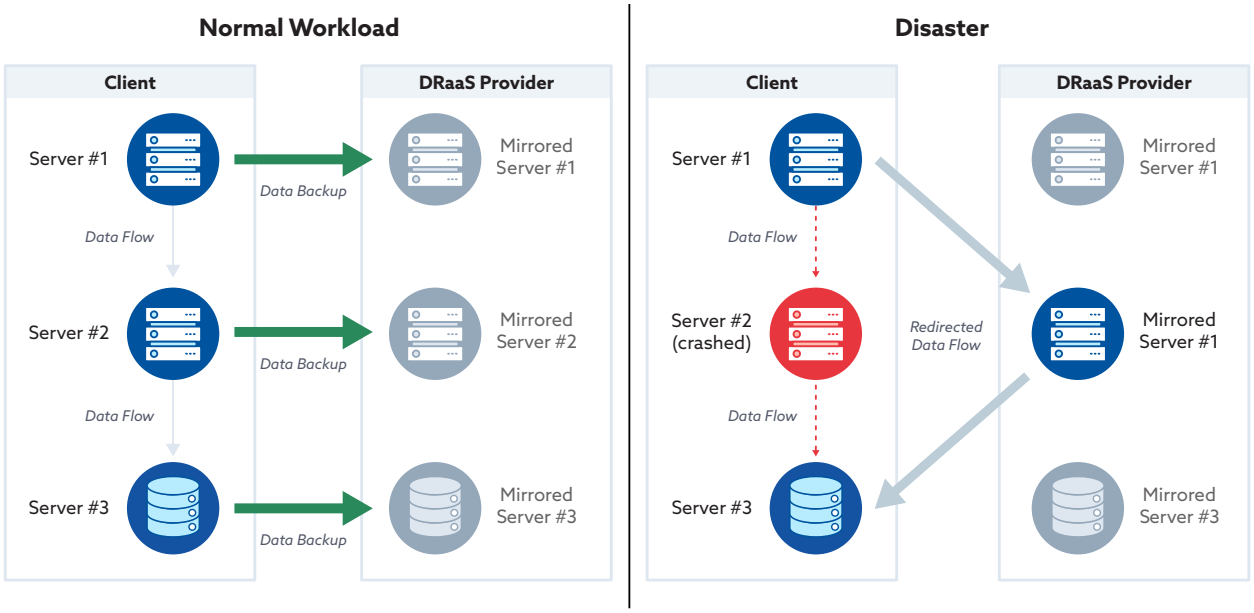


Figure 11: Traditional Systems Recovery as a Services

3.8 DR and Backup as Cloud Service

Authenticated, secure backup, and disaster recovery are possible only by using cloud services. This service is hosted on the cloud server which periodically synchronizes with the host computer to generate the backup segment as given in Figure 12. The cloud server operates in two services mode, replication mode, and failover mode. In the normal case, replication mode is synchronized with the host computer to compare and check the resources; if the system runs smoothly, this service only generates the backup files, while in the case of a disaster, the cloud server automatically moves from replication mode to failover mode to fully support the host.

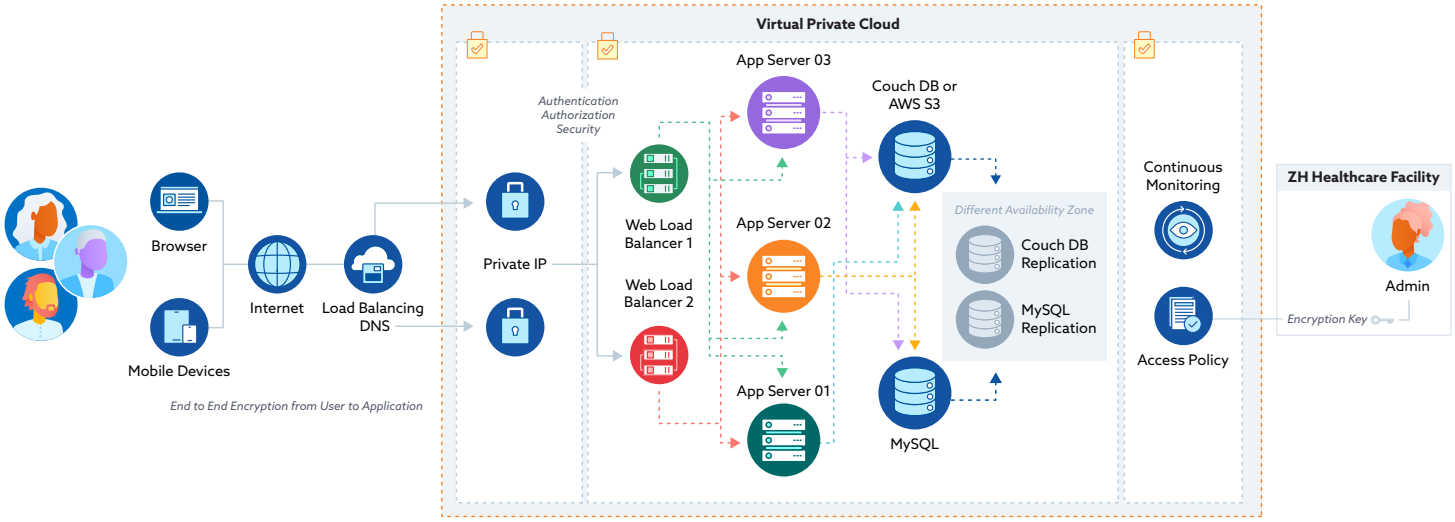


Figure 12: Cloud-Based Systems Recovery

3.9 DR and Backup for Physical Environmental Level

With this type of service, the DR represents the physical level replication and monitoring of data, which is the most used service strategy at the machine level. This service uses replicas of failover sites by using the same characteristics as the main datacenter to operate the IT system.

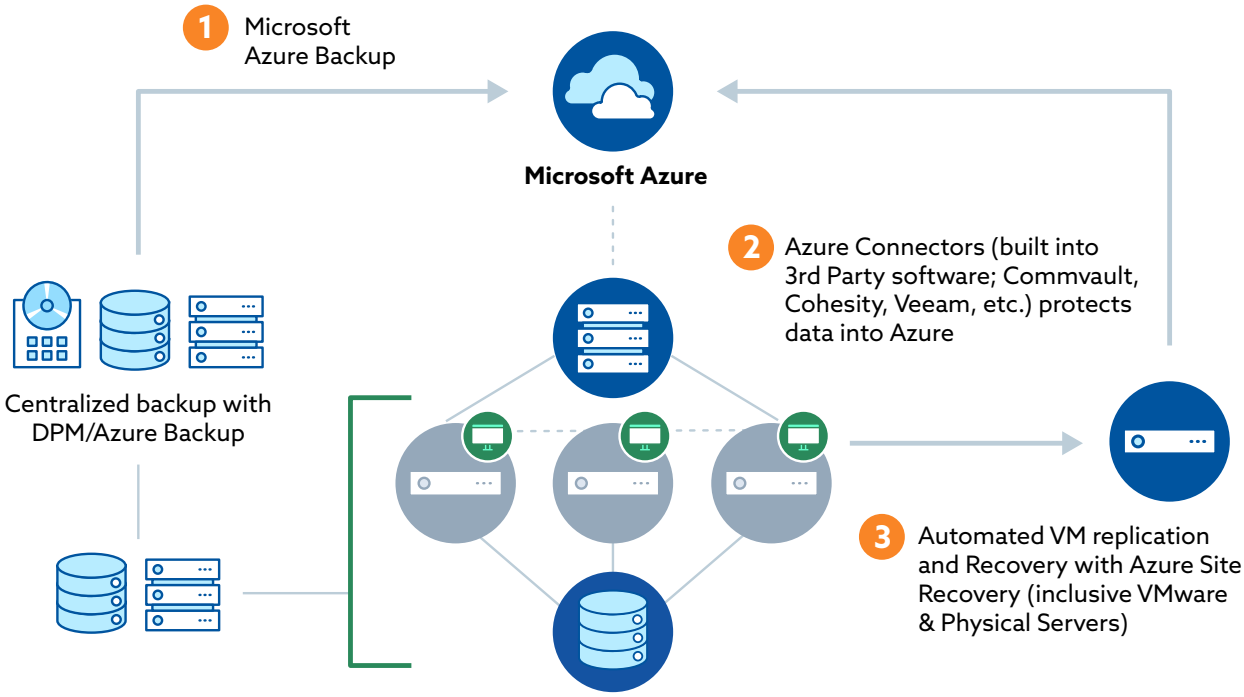


Figure 13: Backup and DR in the cloud

3.10 SaaS – Replicated File-Level Storage for File Shares

Much like replicating file-level storage for client systems, an organization may engage in using a CSP to the backup user or organizational file shares via a software client/agent. This solution works best for SMBs, as large enterprises will have a much larger data footprint, thus adding costs and time for the backups to execute. Figure 14 below describes the replicated file-level storage sharing methodology.

There are two domains connected with the two nodes which are further connected with the two data sources. The data is stored on the two data sources which are shared as a replicated database system. In the event that one DB is down, the shared files are also available on replicated DB, which will be up and used.

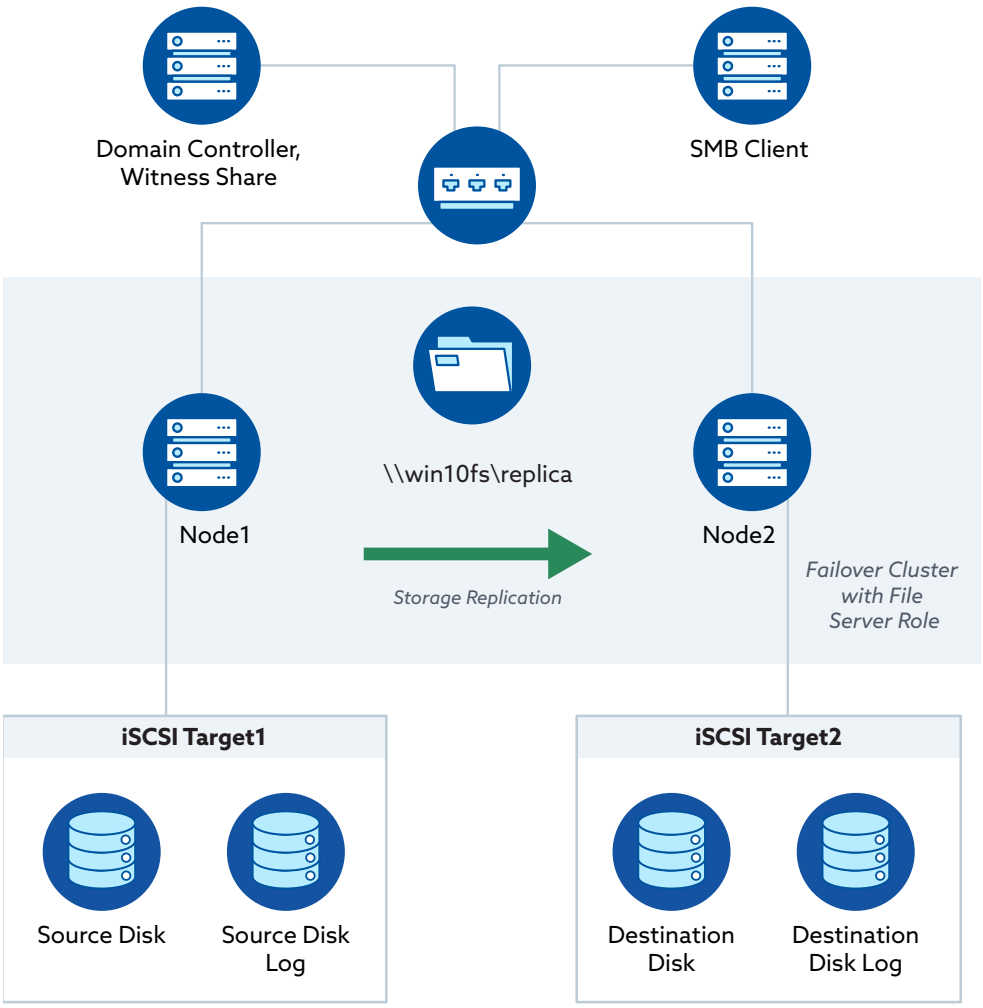


Figure 14: SaaS – Replicated File-Level Storage for File Shares

3.11 SaaS – Data Export

To negate vendor lock-in, SaaS cloud consumers should validate that a cloud service provider (CSP) provides data export functionality. Consumers may use this functionality to export data to another geographic location and/or CSP, to ensure continuity in the event of an outage. Furthermore, consumers can use this model, as given in Figure 15, to ensure that proper and agreed-upon recovery time objectives (RTO) and recovery point objectives (RPO) are met. For portability and interoperability purposes, the consumer should ensure that the SaaS CSP provides a consistent standard for data export and one that is compatible with the customer's and other cloud vendor's solutions.

Data export processes can be optimized by leveraging open standards such as ASCII, as well as by leveraging data dictionaries. A common data model, data dictionaries, or master data management (MDM) will allow the consistent and automated exporting of information between geographically separate systems. This expectation is predicated on the expectation that the CSP's and the consumer's systems have data import capabilities as well.

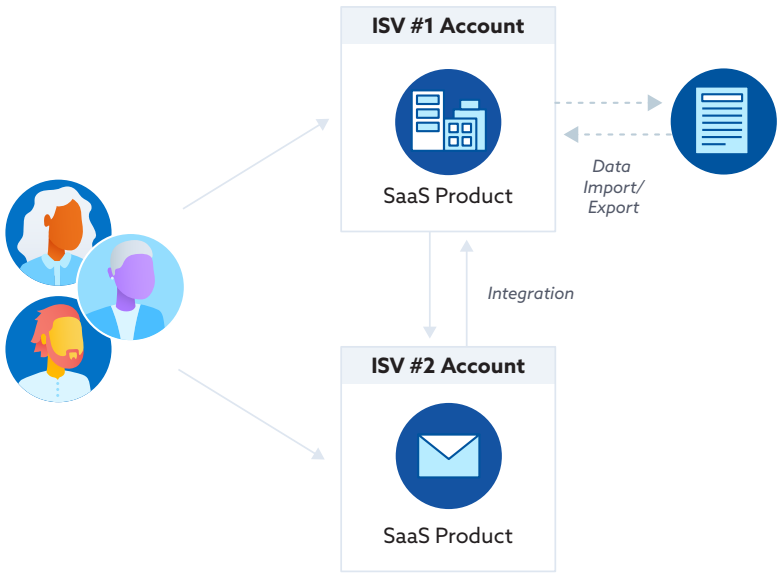


Figure 15: SaaS – Data Export

3.12 IAM – Leveraging Federated Identities

Federated identity management allows organizations like enterprises and service providers to securely exchange user information across partners, suppliers, and customers. By utilizing standards-based methods, identity federation can reduce costly repeated provisioning, security loopholes, and user inconvenience, which are often the consequences of rigid, proprietary, tightly-coupled application architectures. Organizations that have deployed federated identity management

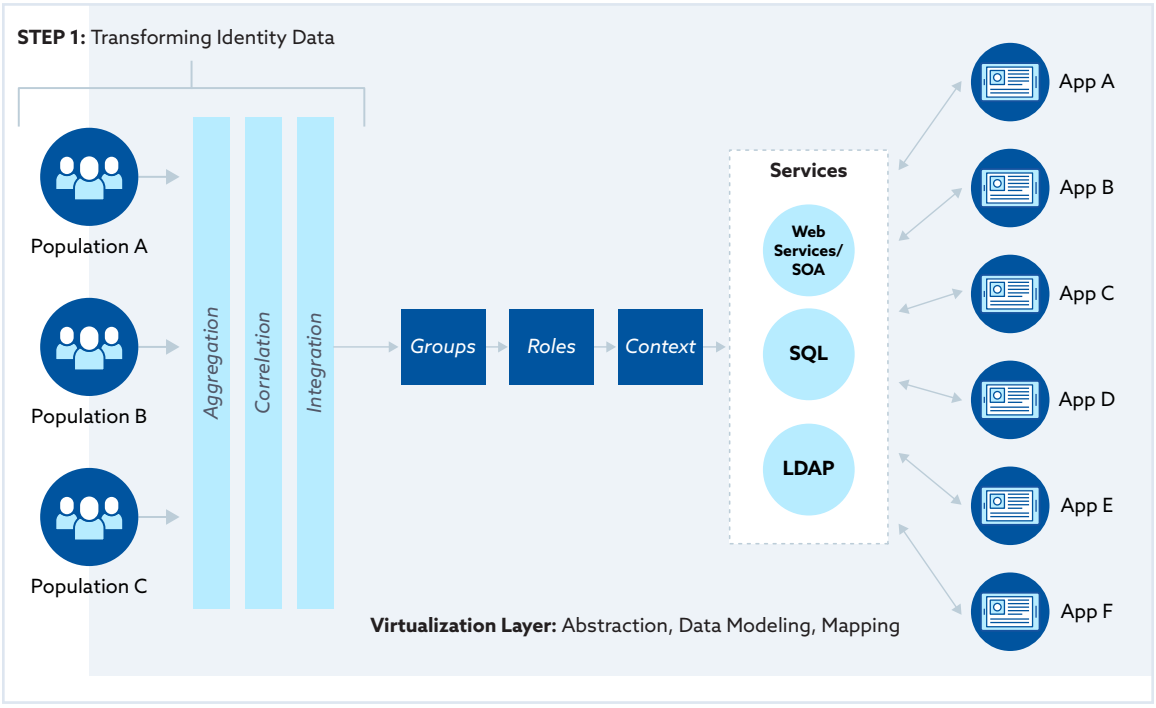


Figure 16: Leveraging Federated Identities

software remove barriers from logging in, improve collaboration with partners, enhance customer service, accelerate partnerships and alliances, reduce costs associated with integrating to outsourced services, and free themselves from large vendor-specific, all-encompassing systems. Figure 16 elaborates on the leveraging of federated identities which are based on three layers: aggregations, creation, and integration. The data from different sources, gathered by these layers are sent to the services for identification.

3.13 Recovery as a Service

Recovery as a Service (RaaS) is sometimes known as Disaster Recovery as a Service. DRaaS, effectively, is a catchall term for performing DR in the cloud. It usually refers to a considerably more complete service than the other options mentioned and may include replication to the CSP, alerts of issues, and potentially automated failover options, including component and whole site failover. This service also often includes error reporting, compression, replication, etc. It is very helpful for small as well as large scale organizations to back up data and recover systems immediately in case of failure where dedicated, off-site, disaster recovery infrastructure is not applicable. Figure 17 describes the model useful for the implementation of disaster recovery. The architecture of the model is based on the replicated DB, over the cloud system. The cloud service periodically performs the backup according to the system settings.

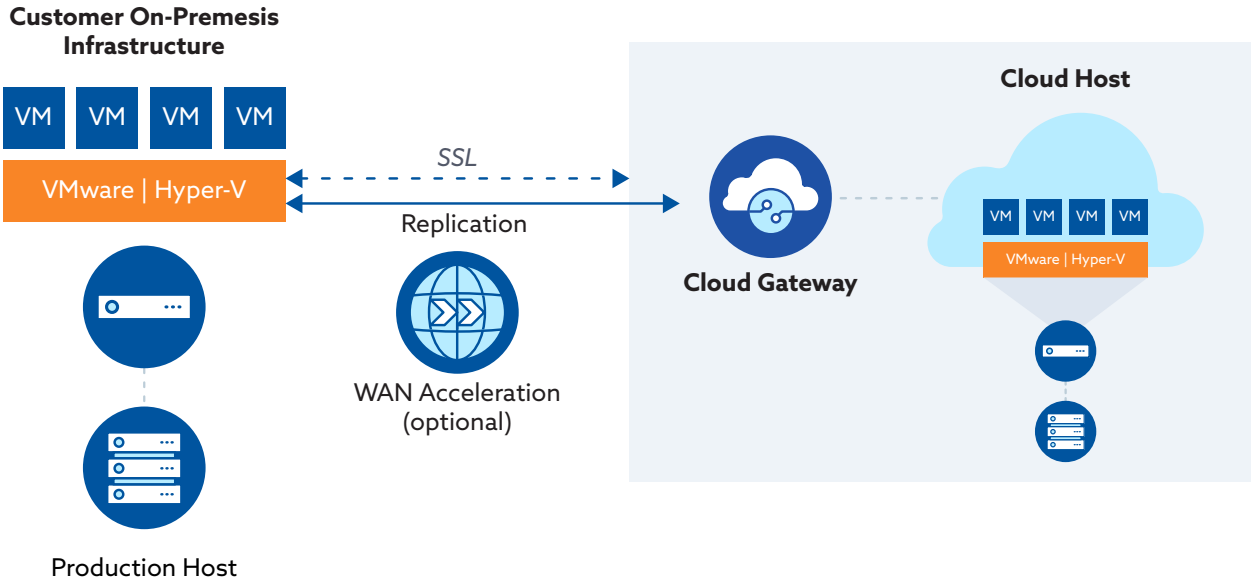


Figure 17: DRaaS Disaster Recovery as a Service

3.14 Traditional Non-Cloud Systems Recovery as a Service

For comprehensive DR as a Service (RaaS) should be considered. RaaS providers typically offer a total solution. The CSP will work with the client/the user, potentially even hosting hardware at the local site and offer fully or partially automated failover services for requirements from individual systems to the whole site. The CSP also will work with the client on the failback process, which is often overlooked and is as critical as the initial failover process in terms of enabling the business to return to normal once the disaster has been resolved.

From an architectural perspective, shown in Figure 18, RaaS will look similar to a combination of the solutions incorporating replication of systems and data, with additional wrappers for better monitoring and assistance with failover.

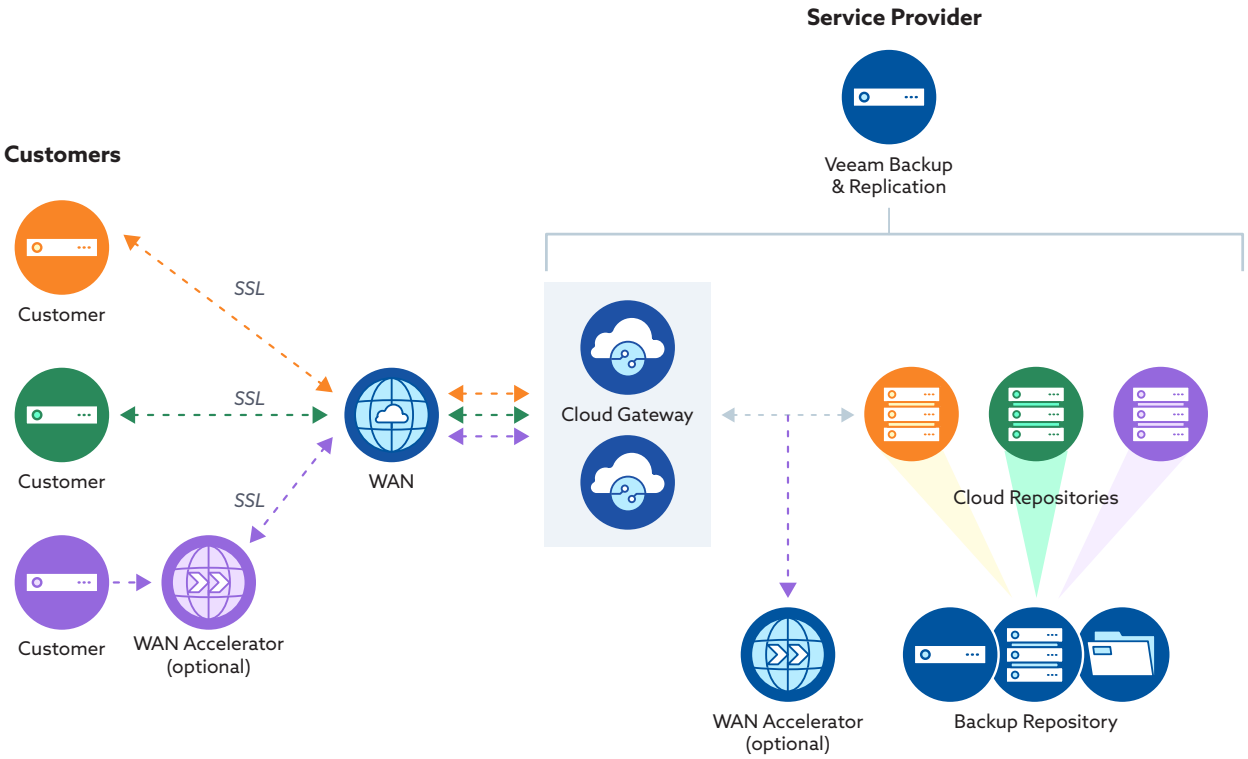


Figure 18: Disaster Recovery as a Service (DRaaS)

3.15 Disaster Recovery and Backup using Distributed Metadata

One or more representations are generally applicable to the management services with distributed metadata in virtual machine and cloud computing, while physical machines rely on the data centers. As shown in Figure19, some cloud computing services maintain systems metadata, which can be used for DR. For such services, a management layer works above the cloud and physical environment (such as VM) to maintain metadata and differentiate between the physical DR and cloud-based DR.

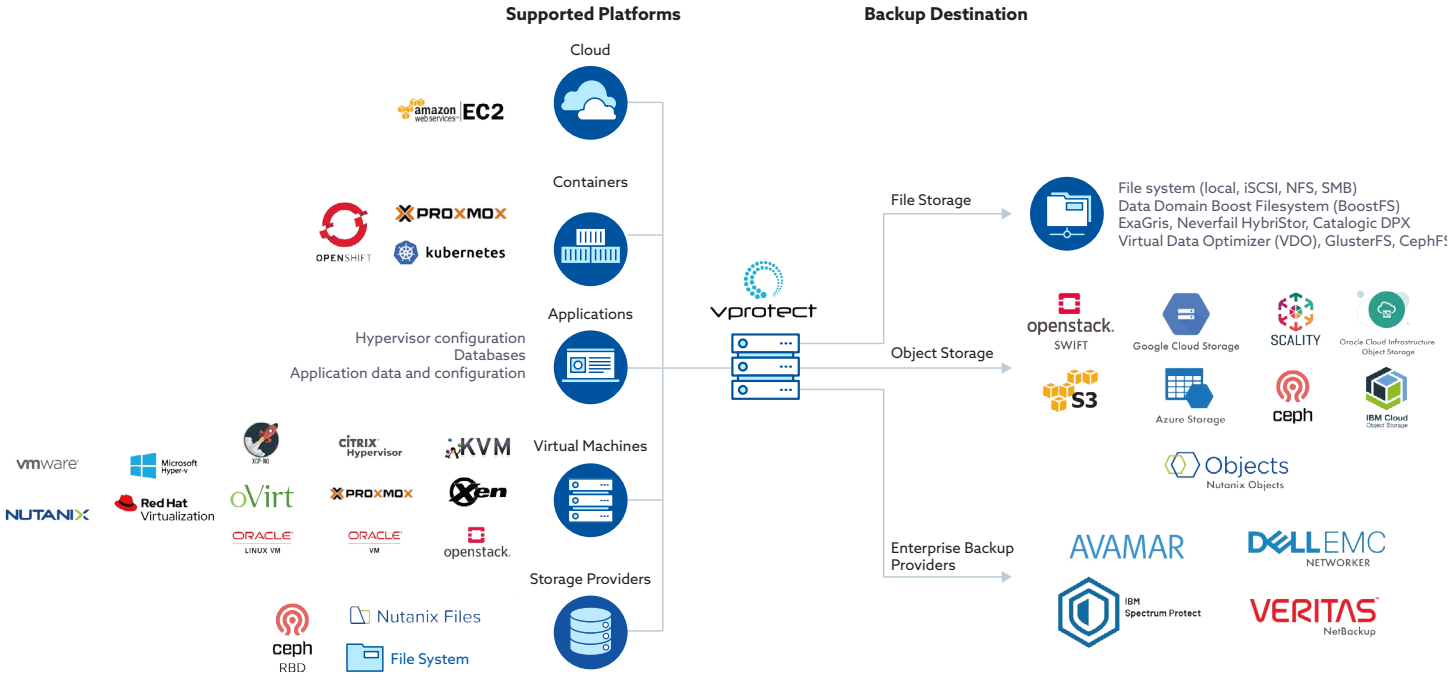


Figure 19: Disaster Recovery and Backup

3.16 Disaster Recovery in the Cloud

Figure 20 describes the involvement of the third party. The cloud-based system can be highly resilient; however, single cloud environments are usually much less resilient than regular infrastructure. This is due to the inherently greater fragility of virtualized resources working in highly complex environments. This usually applies to compute, networking, and storage, because those allow users unauthorized access and cloud providers can leverage extra resiliency techniques for their structures and applications that run on top of IaaS.

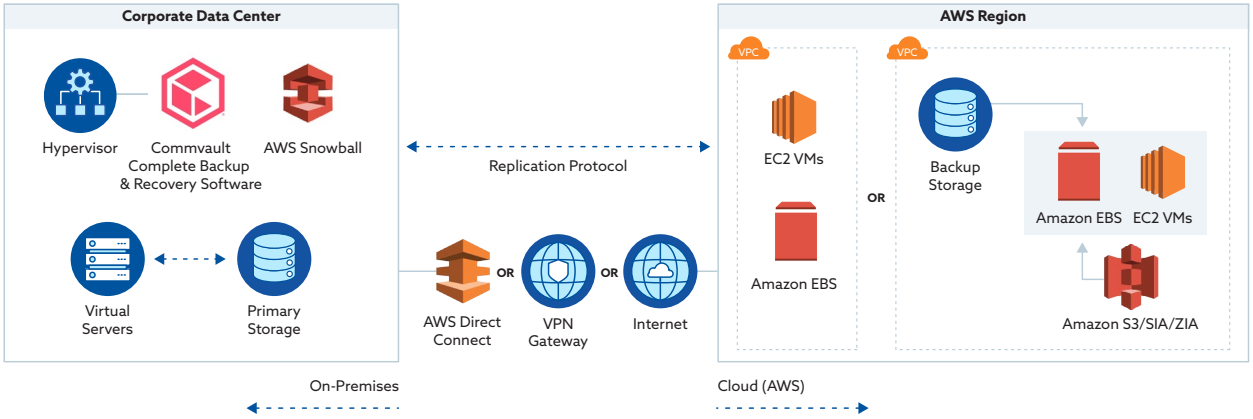


Figure 20: Disaster Recovery

4. Best Practice Considerations

Besides the architectures and services offered, there are other considerations that should be addressed to ensure that DRaaS Services (Backup and Recovery) are secure.

4.1 Replication of Files and Data

Data replication is NOT the same as data archiving or backing up data. Unless snapshots and journaling are used, replication will replicate only whatever is "live" so deletions/errors/corruptions will be replicated to the local Highly Available (HA) instance and the remote DR instance(s). To provide reliable DR, backups, whether as snapshots to disk or more traditional backups to tape, should also be implemented.

Replication, from a DR perspective, copies an entire logical object to the DR site for system/application/data recovery purposes. Depending upon the solution used, it may provide off-site backup functionality as well. Replication can be done in multiple ways, including file-level synchronization, file copies, byte, or block level.

Files are usually replicated or synchronized across different geographic locations for continuity purposes. Note that synchronization is more bandwidth-efficient than complete file replication; the entire file is not copied over, just the modifications. The all or nothing nature of file-level replication can lead to higher bandwidth requirements and a loss of efficiency. However, this solution can be easier to implement.

Block-level replication replicates only block level changes on the storage device and is the most efficient in bandwidth requirements. However, block-level replication may not be compatible with systems that need to be live at the DR site, especially if immediate failover is required. An example would be a database, where it is likely best to rely on built-in replication technologies, such as mirroring. An organization should determine data to be replicated for DR to minimize bandwidth and off-site storage requirements.

When it comes to replicating data for DR, it is critical

- to determine if systems/applications for which data is being replicated include any dependencies (if data in system X is from xx time, then data in system Y must also be from xx time);
- to determine the mode of DR (if systems are being replicated as live systems, or if only data is being replicated, and the DR systems will be "turned on" if DR is invoked);
- to determine the rate of system change, and how much bandwidth will be required;
- to determine how near to "real-time" the replication must be; and
- to determine which CSP-supported technologies for which replication can be performed.

4.2 Service Level Agreements (SLAs)

A key area to consider when managing backup and recovery relationships with third parties is the service level agreement (SLA). Customer and provider requirements, along with the capabilities, are aligned and agreed upon in the SLA.

The client should ensure that:

- cloud and non-cloud services are integrated into SLAs;
- performance requirements such as RTO/RPO (Recovery Time Objective/Recovery Point Objective) for all systems, whether cloud or non-cloud apps/data/systems are established;
- bandwidth requirements for things like replication to the CSP and client access to hosted services are cited;
- system requirements for recovery workstations are detailed;
- declaration of DR procedures, workflow, and allocation of responsibilities are provided; and
- procedures and requirements for failover and failback are specific.

4.3 Data Privacy

Data privacy is at the forefront of every organization's concern. Firstly, data breaches of consumer information can lead to severe damage to their fundamental rights and freedoms. Secondly, organizations that collect information without authorization, process this information carelessly, or fail to provide proper protection open themselves to fines, penalties, and legal redress. GDPR, arguably the most well-known law, provides for fines up to 20 million euros or 4% of a company's global annual revenue for the preceding year. Companies can even be banned from processing personal data in the future.

- Know from where the data originated and is hosted.
- Know where data is replicated.
- Identify all data privacy laws applicable to data.
- Know the rules governing the movement of data, such as the European Union data privacy laws covering personally identifiable information.
- Know the legal restrictions on the use of encryption (e.g., requirements that keys be disclosed).
- Obtain Cloud Service Provider (CSP) certifications related to any relevant regulations while still guaranteeing resilience and failover.

4.4 Data Protection/Encryption

Data processed in the cloud or on-premise, at some point, will be encrypted then decrypted, possibly multiple times. It is essential to understand the requirements for data handling to ensure that the encryption levels are adequate for the data's sensitivity and the length of time that the data must remain secure.

- Understand the requirements for data handling.
- Encrypt data in transit to and from the CSP and between the CSP's sites.
- Encrypt data in transit between guests within the CSP's datacenter(s).
- Encrypt data at rest.
- Employ secure algorithms and key lengths.
- Use trusted cryptographic implementation (e.g., FIPS 140.3).
- Put in place and maintain secure key management processes.
- Ensure that adequate data confidentiality, integrity, and availability (CIA) protections are in place surrounding the virtual or shared servers, including when data is being processed.
- Know the value of data to attackers and how long this value lasts.

Server-Side Encryption

Server-side encryption ensures cloud consumers that information uploaded by end-users is protected once the data is within the walls of the CSP. This solution is a final safeguard for those organizations that require protection for their data at rest (DAR).

Depending upon the offering consumed, the customer will have differing levels of control in this area. For example, in an IaaS solution, the customer likely will be able to use whichever encryption method they want. Still, in a SaaS solution, the encryption level will be defined by the CSP.

Client-Side Encryption

For cloud consumers located in heavily regulated jurisdictions, or for those in heavily regulated industries, the use of client-side encryption is recommended to ensure the confidentiality and integrity of their information. This can be done via data at rest (DAR) encryption solutions.

Transport/DIM Encryption

CSPs should support the use of transport layer security (TLS) and secure sockets layer v3 (SSLv3) protocols for secure communications. TLS is recommended, as this has superseded SSL. When consumers upload content via electronic data interchange (EDI) methods, the CSP should allow for the use of secure shell (SSH) technologies. FTP is widely considered obsolete.

4.5 Segregation of Duties (SOD)

Proper segregation of duties helps ensure that no one person has undue influence over completing any task. Segregation of duties increases the chance that errors and unauthorized acts, either intentional or accidental, will be prevented or discovered.

- All backup and recovery task combinations must be identified and documented.
- A risk assessment and evaluation considering impact and likelihood and assignment of a high, medium, or low rating must be performed.

- A risk assessment to verify that all backup and recovery job roles created from the individual task combinations are constructed conflict-free must be performed (This helps ensure that CSP staff, such as network administrators and DBAs, cannot perform unauthorized acts, either accidentally or intentionally).
- All roles must be documented to ensure that everyone is aware of their responsibilities.
- A secure separation between the various cloud-based services to ensure that those running DR (Disaster Recovery) processes cannot access SIEM (Security Information Event Management) or DLP (Data Loss Prevention) systems, and vice versa must be ensured.
- Access and authorizations must be considered before the assignment and reviewed before granting.
- SOD must be reviewed periodically to evaluate changes in access and authorization and any system and process changes.
- Access and authorizations must be terminated promptly upon change of assignment or system or termination of employment.

4.6 Access Controls

Access control goes hand in hand with the Segregation of Duties (SOD). Access should be granted using the principle of least privilege. It is a practice that limits access rights to the minimum permissions needed to perform the required work. Even though a task or access to an asset may be allowed per SOD, it may still not be in line with the individual's responsibilities, and therefore access may not be granted.

- Customers of the CSP can access only their systems and data.
- Access to live data and backup is not allowed.
- Access is restricted to particular assets (data, servers, etc.)
- Access to , view, and run backup and recovery but without access to delete services
- Permissions can be set to create administrator accounts, allowing a user to create and edit other accounts.
- Administrators cannot edit their permissions.

4.7 CSP Resilience

The resilience of the cloud customer is embedded in the resilience of the cloud provider. While the cloud customer's data may be backed up and recoverable if the CSP's operations are unavailable to perform the recovery then both the customer and backup sit idle until the CSP restores its operations.

CSP should have a holistic approach to determine resilience readiness level and define measures to mitigate identified risks. CSP should have

- a strategy and vision for resiliency;
- a resiliency program that keeps pace with the organizational changes across the enterprise;
- applications that are available in active-active mode;
- agreed-upon levels of resilience, contained in the SLA, both for

- systems within the data center and for the data centers themselves; and
- resilient and secure supporting services, such as third-party links to the CSP, including locally hosted CSP infrastructure.

4.8 Metadata Retention, Separation, and Protection

In addition to cloud consumer's actual data and systems hosted in the cloud, there is metadata that the CSP will capture, log, and record while running and hosting systems.

- The CSP must have retention policies that are commensurate with the sensitivity of the metadata.
- The CSP must provide metadata retention, separation, and protection per national and local laws.

4.9 Licensing

When an enterprise moves to the cloud, one of the biggest challenges besides migrating non-cloud technologies to the new environment is their licenses.

- Adjust the licensing models for legacy applications for virtual deployments.
- Determine the vendors' (of applications and systems) licensing requirements for DR deployments and their solutions.
- The CSP should offer guidance or support regarding licensing concerns or issues (especially if they have existing customers running the same applications) and examples of how they have addressed licensing challenges.
- Evaluate potential cloud-native replacement software.

4.10 Migration

When an enterprise moves wholly or partially from DR in on-premise setup to a cloud or hybrid cloud environment, the following actions should be taken:

- Update the applications and services; the more current the application/service is, the less likely it will be to virtualize it or move it to a cloud-based service.
- Should the enterprise move, it may be that the more current the application/service is, the easier it will be to move.
- If the business is completely or heavily virtualized already, moving to cloud-based DR will be considerably more manageable.
- Many CSPs offer a service where the client can directly copy the virtual machine files to the cloud, then spin them up in the cloud.
- Perform any reconfiguration (IP address, hostname, etc.) to allow application/services to run and be replicated, should this be required when DR is invoked.
- Establish RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives).
- Test RTO/RPO to determine RTR (Real-Time Recovery) and RPR (Real Point Recovery).

4.11 Failover

Cloud consumers need to be aware of what failover functionality a CSP's environment offers and how to automate that task. Many IaaS and PaaS providers should have this functionality available at an additional cost.

Once a consumer has added automated failover capabilities to their environment, it is extremely critical that they occasionally test this functionality to ensure that it works properly.

The failover process will vary considerably depending upon the service model implemented:

SaaS – When utilizing a SaaS-based system, CSP handles the failover, including ensuring data is consistent across the system's components and making requisite external changes, such as updating DNS records as part of the service offering.

PaaS – The CSP will provide failover for the platform, applications, and data residing on it. Areas such as re-pointing other application components and other parts of the system will either be the customer's responsibility or need to be included in the contract.

IaaS – This is the most flexible option for the customer, wherein the onus for implementation and management resides with the customer. The CSP will replicate all data and O/S instances, but bringing DR systems online, ensuring consistency of replicated data, etc., will be the customer's responsibility.

4.12 Clustering

Systems are clustered when they are joined in a pool of hardware and software resources that act as one endpoint. Clustering allows for the failover of hardware and/or software within this pool for continued operations. Clustered systems are usually constrained to one geographic location, so location-based failures (e.g., power outages/fluctuations) may affect a clustered solution.

Given the virtual nature of cloud-based services, implementing relatively complex cluster solutions within this environment may not be as worthwhile as in the "physical" domain. Hosting the service on multiple IaaS instances, utilizing horizontal scaling and high availability technology likely provides more resilience than a traditional cluster.

Should clustering be used:

- Backup the passive nodes as the active nodes are working.
- The backup applications should be cluster-aware.
- Selected backup frequency based on available resources and customer requirements.
- Use concurrent cluster node backups to speed up the backup process.

4.13 Services Already Hosted in the Cloud

Ensuring that services work correctly in performance and scale, and functional terms are critical considerations. Understanding the location of the CSP's DR site(s) is also vital, as it may impact both performance (latency issues) and regulatory compliance, in addition to survivability concerns.

If a client's services are hosted already with a cloud provider who has multiple data centers in their legal jurisdiction/region, or if there are no regulatory or business reasons why their data cannot move, then setting up DR for their services will, in most cases, be relatively simple and primarily concerned with contractual issues.

Many of the challenges often faced, such as available bandwidth for replicating data, especially when there is a high rate of data change, will be taken care of by the CSP and their highly scalable infrastructure and services.

See also 4.15 Traditional On-Premises Infrastructure to the Cloud and 4.16 Cloud Service to Cloud Service.

4.14 In-House "Traditional" Non-Cloud Services

Disaster Recovery for traditional, non-cloud hosted systems, when provided as a cloud service, has many of the same issues and concerns as any other DR solution relying on data replication to a remote DR site.

An added challenge when using a CSP over more traditional approaches to DR is that the CSP will only host virtual servers and may place limitations on the operating systems it will support. These limitations likely are driven by the underlying hardware establishing O/S limitations, even when IaaS services are used.

When assessing any project's challenges and efforts to move DR to the cloud ensure that

- the system/application can be virtualized;
- the vendor supports virtualization;
- all non-standard physical components (dedicated PCI cards, USB/parallel port dongles, etc.) are included in the assessment; and
- licensing issues with virtualizing applications are accounted for.

4.15 Traditional On-Premises Infrastructure to the Cloud

A CSP may offer services that provide DR capabilities for on-site IT systems. The architecture will depend on the RPO (Recovery Point Objectives) and RTO (Recovery Time Objectives) of the cloud customer. The overall principles will be the same as traditional DR, and will consist of

- configuring the relevant local systems to replicate data;
- configuring systems and storage at the CSP to be replicas of the live systems, likely with considerably lower specifications;
- defining the required specifications at the CSP should DR be invoked and ensuring that the CSP has enough elasticity to provide the increase and scale within the required DR timelines;
- replicating systems and data to the CSP. (It is imperative to replicate systems and data, not just data. While it is very possible, and in some cases reasonable, to just replicate data in order to have off-site copies, this is analogous to storing tapes off-site. Such a plan can be used to support DR but does not in itself provide DR capabilities. Planning and attention should be paid to the rate of data change, and therefore bandwidth required, between the customer and the CSP to replicate systems for DR.);
- working with any third parties to ensure the cloud-hosted systems can access the third party, if DR is invoked, as per locally hosted systems;
- testing access to the systems in the CSP from any relevant locations, including third parties, customers, and employees;
- testing the actual DR systems themselves to ensure they work as expected and process correctly;
- performance testing (There are often concerns regarding the performance of virtualized systems. Performance tests should be carried out to confirm to the business that the chosen solution will perform as designed, should DR be invoked.);
- ensuring any legal/licensing concerns are addressed;
- ensuring all applications/systems are supported in a cloud/virtual environment; and
- potentially designing alternative solutions for applications/systems that will not function in cloud virtual environments. Work with vendors of these systems on potential solutions to enable virtualized/cloud-based DR.

4.16 Cloud Service to Cloud Service

Even clouds can have outages and cloud service providers, while guaranteeing uptime, do not automatically guarantee backup availability and recovery times. Backup and recovery need to be negotiated and the commitment recorded in the service level agreement.

- If DR is required when using cloud services to provide the Infrastructure/Platform/Software as a Service for production environments, ensure that services are backed up and/or replicated to another site.
- Many CSPs offer DR capabilities for systems they host via replication to another datacenter either by default as an extra service or by combining the two. Some platforms replicate all data to an additional data center by default, but not the whole system in a live state. Maintaining live systems at the DR site may be added as other services, usually incurring additional fees.
- When hosted in the cloud, DR is considerably more straightforward in architecture than when hosted locally. The CSP will manage replication, bandwidth requirements, storage, networking, DR hosts/systems, etc.

- Regulations control data movements in and out of specific legal boundaries. For example, personally identifiable information held in the EU about EU residents must not leave the EU. Choosing a CSP with multiple data centers in the same legal boundary may be a requirement.
- Ensure that the frequency of backups matches the requirement for up-to-date data required for operations as well as compliance.
- For recovery of more targeted information, the CSP should have a tool that allows identification, location, and backup of subsets of data.
- The regular transfer of large data volumes and the proximity of consumers to the source needs to be accounted for.
- Immutable storage prevents changes to be made to backups once they are saved.
- Write new copies of point-in-time (PIT) incremental changes to reduce costs.
- Account for latency and other constraints to ensure user access to and from third parties.
- Establish RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives)
- Test RTO and RPO via testing scenarios to determine RTR (Real Time Recovery) and RPR (Real Point Recovery).

4.17 Ransomware

Ransomware is malicious software that gains access to an organization's systems and data and then encrypts these systems and data rendering them inaccessible without the encryption key. The attacker supplies the decrypt key only if the victim pays a fee (ransom). Ransomware can gain access to systems through such avenues as users interacting with phishing emails or infected websites. Often, the company is unaware as to when the malicious software is introduced; therefore, an investigation is necessary, and it may be required to restore data at a point in time well into the past.

4.18 Requirements, Manual Workarounds/Alternate Processes

Requirements

Regardless of the DRaaS Service offered/chosen, the customer is responsible and needs to set the requirements in areas such as infrastructure quality and location, recovery capability, data loss tolerance, flexible terms, regular testing, and sufficient support.

Manual Workarounds and Alternate Processes

Claims of DRaaS full automation, efficiency, and effectiveness notwithstanding, the variety and complexity of customer environments are such that not everything may be automated immediately or possibly ever given the customer's environment, the cause of the disruption compared to the architecture of the DRaaS solution, and the provider's constraints. Therefore, both the customer and provider must create manual workarounds/alternate processes to ensure the customer is adequately protected during recovery, and must also maintain an ability to rebuild systems should recovery prove impossible based on the situation.

5. Benefits

Below are some of the most significant benefits of taking advantage of DRaaS (backup and recovery) services and modern architectures.

- **Focus** – Instead of expanding the effort to design, implement, and maintain a disaster recovery plan and system, IT can devote their efforts to more revenue-generating activities.
- **Scalability** – As the cloud service provider hosts many customers' infrastructure, this provides the potential for elasticity and effectively unlimited scalability.
- **State-of-the-art** – The diverse customer base and competitiveness of the market ensures that the vendors employ the best infrastructure, software, and systems to meet ever-increasing performance, security, and privacy requirements.
- **Recovery** – Mature vendors offering DRaaS services have access to infrastructure and are experienced in recovery, making disaster recovery plan implementations and recoveries more efficient and effective.
- **Infrastructure** – One of the most critical assets is data. The revenue volume allows the CSP to employ state of the art facilities, construction, fencing, access systems, cameras, and alarms to safeguard data.
- **Updates** – Two major issues today are patching and versioning. The requirements of customers (performance and security) and the efficiency of patching and versioning the same software for multiple customers is a distinct cloud advantage.
- **Resilience** – In serving a large, diverse customer base, vendors need to host multiple infrastructures for hundreds or thousands of customers, so they invest in large-scale, resilient, redundant, and secure systems and facilities.
- **Access** – a DRaaS cloud solution allows a disaster-affected system to be accessed from a location not affected by the disaster.
- **Costs** – While vendors spread costs over a large customer base reducing unit costs, the consumer benefits by paying only for the services they use.
- **Compliance** – Because customers represent diverse fields and geographical areas, it is necessary to comply with numerous regulations, standards, and country-specific requirements.

6. Conclusion/Summary

For both the CSC and the CSP to remain competitive, customers require, and the CSPs must provide, backup and recovery that seamlessly ensures operational resilience in-line with the customer's business and compliance requirements.

Never-ending digital transformation, technological innovation, global expansion, and proliferation of compliance requirements are resulting in complex environments that require backup solutions to

- provide resilience regardless of the environment;
- simultaneously improve the quality of protection while reducing cost;
- be agile in both user-friendliness as well as in adaptation to circumstances;
- back up and recover continuously 24/7/365;
- be automated and granular;
- provide visibility and flexibility regarding data location, quality, and storage cost;
- provide visibility and flexibility concerning data recovery, quality, and cost;
- provide a single DR interface regardless of location; and
- be ready for IoT/IIoT, blockchain, and AI technologies.

This document presents some of the architectures, services, best practice considerations, and benefits that need to be considered when faced with a DRaaS/DR challenging opportunity.

7. References

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017, Chapters 6, 9, 11,13, available @ https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance, SecaaS Implementation Guidance, Category 9, Business Continuity and Disaster Recovery (BCDR), 2012, available @ https://cloudsecurityalliance.org/artifacts/secaas-category-9-bcdr-implementation-guidance

Importance of Disaster Recovery in Cloud Computing, 2020, available @ https://bleuwire.com/importance-disaster-recovery-cloud-computing/

Google Cloud. Disaster Recovery Planning Guide, 2020, available @ https://cloud.google.com/solutions/dr-scenarios-planning-guide

IBM "Hybrid Cloud: The best of all worlds", 2019, available @ https://www.ibm.com/downloads/cas/E97LZYVG

IBM "Private, Public, and Hybrid Cloud Storage Solutions." Larry Coyne, Joe Dain, Eric Forestier, Patrizia Guaitani, Robert Haas, Christopher D. Maestas, Antoine Maille, Tony Pearson, Brian Sherman and Christopher Vollmar. Redbooks. 2018, available @ http://www.redbooks.ibm.com/redpapers/pdfs/redp4873.pdf

Forbes Technology Council. 16 Expert Strategies for Creating an Effective IT Disaster Recovery Plan, 2020, available @ https://www.forbes.com/sites/forbestechcouncil/2020/04/23/15-expert-strategies-for-creating-an-effective-it-disaster-recovery-plan/#11487931b542

Hybrid IT and Disaster Recovery, Christopher Null, 2018, available @ https://www.esilo.com/hybrid-it-and-disaster-recovery-6-things-to-know/

Disaster Recovery as a Cloud Service. Wood, Timothy, 2010, available @ https://www.usenix.org/legacy/event/hotcloud10/tech/full_papers/Wood.pdf

8. Acronyms

AD – Active Directory
ADFS – Active Directory Federation Services
AMI – Amazon Machine Image
BC/DR – Backup and Disaster Recovery
CIA – Confidentiality, Integrity, Availability
CSP – Cloud Service Provider
CSC – Cloud Service Customer
DAR – Data-at-Rest
DLP – Data Loss Prevention
DNS – Domain Name System
DRaaS – Disaster Recovery as a Service
EDI – Electronic Data Interchange
FIPS – Federal Information Processing Standards
FTP – File Transfer Protocol
IaaS – Infrastructure as a Service
IP – Internet Protocol
HTTPS – Hypertext Transfer Protocol Secure
LDAP – Lightweight Directory Access Protocol
O/S or O/S – Operating System
PaaS – Platform as a Service
POC – Proof of Concept
RBAC – Role-Based Access Controls
RPO – Recovery Point Objectives
RTO – Recovery Time Objectives
SaaS – Software as a Service
SAML – Security Assertion Markup Language
SAN – Storage Area Network
SLA – Service Level Agreement
SMB – Small Medium Business
SSH – Secure Shell
SSL – Secure Socket Layer
SSO – Single Sign-On
TLS – Transport Layer Security
VHD – Virtual Hard Disk
VM – Virtual Machine
VPN – Virtual Private Network
XML – Extensible Markup Language

9. Glossary

DRaaS – Disaster Recovery as a Service is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment from which it is possible to regain access and functionality to IT infrastructure after a disaster.

CSC – The Cloud Service Customer is the user of the CSP's cloud computing offering.

CSP – The Cloud Service Provider fulfills the CSC's cloud computing needs.

Community Cloud – See Appendices 1 to 3

Hybrid Cloud – See Appendices 1 to 3

IaaS – Infrastructure as a Service (IaaS) offers access to a resource pool of fundamental[6] computing infrastructure, such as compute, network, or storage.

Multi-cloud/Hybrid Multi-cloud – See Appendices 2 to 4

On-Premise or On-Prem – Refers to computers and software installed at an organization's facility rather than at a remote location or in the cloud.

PaaS – Platform as a Service (PaaS) abstracts and provides development or application platforms, such as databases, application platforms (e.g., a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, the customer does not manage the underlying servers, networks, or other infrastructure.[4]

Private Cloud – See Appendices 1 to 3

Public Cloud – See Appendices 1 to 3

SaaS – Software as a Service (SaaS) is a full application that is managed and hosted by the provider. Consumers access it with a web browser, mobile app, or a lightweight client app.[4]

Shared Responsibility – refers to the concept that the CSC and CSP have varying responsibilities depending on the cloud service level in effect. The CSC has the most responsibility when IaaS is used and the least when SaaS is used.

6 Security Guidance For Critical Areas of Focus in Cloud Computing v4 Domain 1, Page 11.

Appendix 1 – NIST Definitions of Cloud Architectures

NIST Definitions[7]

NIST 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.

NIST 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.

NIST 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.

NIST 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).

7 NIST 2011, The NIST Definition of Cloud Computing, https://csrc.nist.gov/publications/detail/sp/800-145/final

Appendix 2 - ISO Definitions of Cloud Architectures

ISO Definitions[8]

ISO Private Cloud (3.2.32) – deployment model (3.2.7) where cloud services (3.2.8) are used by a single cloud service customer (3.2.11) and resources are controlled by that cloud service customer (3.2.11).

ISO Community Cloud (3.2.19) – deployment model (3.2.7) where cloud services (3.2.8) exclusively support and are shared by a specific collection of cloud service customers (3.2.11) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

ISO Public Cloud (3.2.33) – deployment model (3.2.7) where cloud services (3.2.8) are potentially available to any cloud service customer (3.2.11) and resources are controlled by the cloud service provider (3.2.15).

ISO Hybrid Cloud (3.2.23) – deployment model (3.2.7) using at least two different cloud deployment models (3.2.7).

Appendix 3 - IBM Definitions of Cloud Architectures[9]

Private cloud[10] – A private cloud refers to a cloud solution where the infrastructure is provisioned for the exclusive use of a single organization, either on-premises or off-premises. The organization often acts as a cloud service provider to internal business units that obtain all the benefits of a cloud without having to provision their own infrastructure. By consolidating and centralizing services into a private cloud, the organization benefits from centralized service management and economies of scale. An on-premises private cloud provides some advantages over an off-premises private cloud. For example, an organization gains greater control over the resources and data that make up the cloud. In addition, on-premises private clouds are ideal when the type of work being done is not practical for an off-premises private cloud because of network latency, security, or regulatory concerns.

Public cloud[7] – A public cloud infrastructure is made available to the general public or a large industry over the Internet. The infrastructure is not owned by any single user, but by an organization that provides cloud services to a variety of businesses. Public cloud services can be provided at no up-front cost, as a subscription or as a pay-as-you-go model, and resources can be shared across multiple businesses to reduce costs.

Hybrid cloud[7] – A hybrid cloud deployment typically describes a situation in which a company is operating a mixture of private cloud, public cloud, and traditional environments — regardless of whether they are located on-premises or off-premises. In a hybrid cloud environment, private and public cloud services are integrated with one another. Hybrid cloud enables a business to take advantage of the agility and cost-effectiveness of off-premises, third-party resources without exposing all applications and data beyond the corporate intranet. A well-constructed hybrid cloud can service secure, mission-critical processes, such as receiving customer payments (a private cloud service) and secondary processes, such as employee payroll processing (a public cloud service). The challenges for a hybrid cloud are the difficulty of effective creation and governance, the need to ensure the portability of data and applications in the cloud, and the management of complexity. Services from various sources must be obtained and provisioned as though they originated from a single location, and interactions between private cloud and public cloud components make the implementation even more complicated.

Hybrid multi-cloud architecture – Hybrid multi-cloud refers to an organization that uses multiple public clouds from several vendors to deliver its IT services, in addition to private cloud and traditional on-premises IT. A hybrid multi-cloud environment consists of a combination of private, public and hybrid infrastructure-as-a-service (IaaS) environments all of which are interconnected and work together to avoid data silos. Many enterprise companies are failing to make their various data repositories and systems 'talk to each other' effectively and efficiently, if at all. The result: more data silos that hinder or prevent data movement and sharing. With a modern hybrid multi-cloud architecture in place, you gain access to a single source of truth as it relates to your data. If optimized properly, you can quickly access data that is reliable and accurate. Moreover, data that is unified in one location is accessible whether it resides on-premises or off-premises.

9 IBM, Hybrid cloud: The best of all worlds, https://www.ibm.com/downloads/cas/E97LZYVG

10 IBM 2018, IBM Private, Public, and Hybrid Cloud Storage Solutions, http://www.redbooks.ibm.com/redpapers/pdfs/redp4873.pdf

Appendix 4 – Definitions of Multi-Cloud Architectures

Gartner – The deliberate use of the same type of cloud services from multiple public cloud providers. In this construct, a mobile app may dynamically move, via containers or other technologies between AWS or Azure based on prescribed business requirements. These portable apps are managed and monitored for uptime, reliability, and security via a single dashboard.

IBM – Uses multiple public clouds from several vendors to deliver its IT services, in addition to private cloud and traditional on-premises IT.

A hybrid multi-cloud environment consists of a combination of private, public, and hybrid infrastructure-as-a-service (IaaS) environments all of which are interconnected and work together to avoid data silos.

Cloudflare – 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. A multi-cloud can also be a hybrid cloud, and a hybrid cloud can also be a multi-cloud, but these terms represent two distinct concepts.

Hybrid cloud describes the mixing of two or more distinct types of infrastructure: it combines a private cloud, an on-premises data center, or both with at least one public cloud. Multi-cloud refers to several different public clouds being deployed, and it does not necessarily include a private cloud, although it can.