KN University Network Design

COIT13236 – Cyber Security Project

Document Title	Cloud Integration Plan
Document Type	Technical Artefact
Document Status	Completed
Document Version	V_2.01
Group No	02
File name	group02-cloud-integration-plan.docx
Created By	Narayan Parajuli (12144248)
Create Date	05/08/2024
Reviewed By	Krishan Himesh Abeyrathne (12217274)
Reviewed Date	15/08/2024

Table of Contents

Cloud Integration Plan

Cloud Integration Plan:

A Cloud Integration Plan frames how an association will communicate its ongoing IT systems and applications with cloud administrations. The target of KN University Network is to ensure reliable communication and interoperability between on-premises structures and cloud-based resources, updating exercises, flexibility, and versatility.

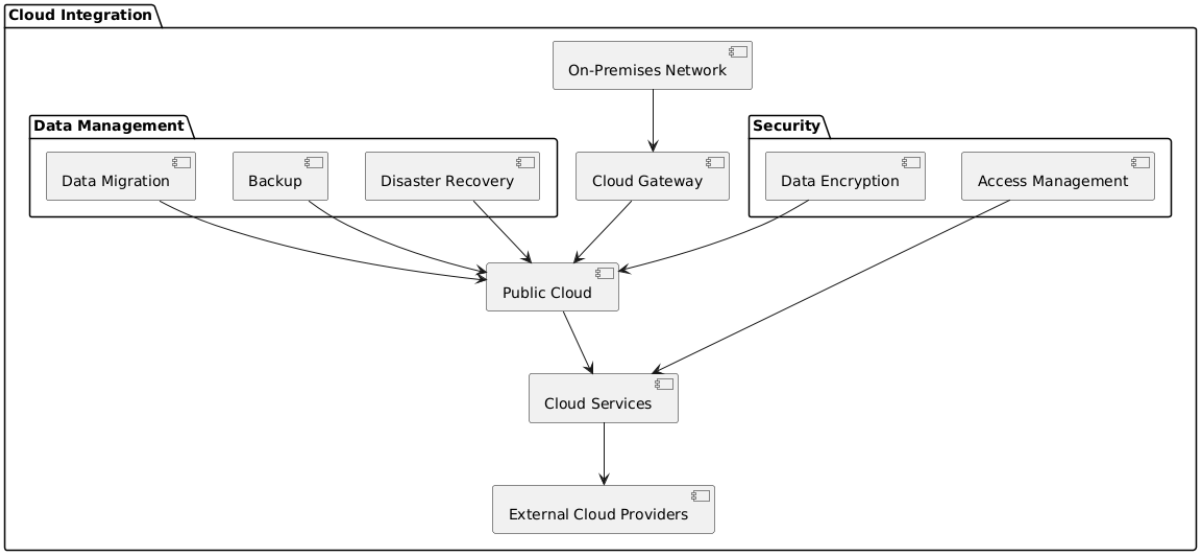

Fig: Cloud Integration Plan

With an emphasis on data management and security to work on the college's network, the diagram frames a favoured cloud integration method for KN University. The cloud is utilized for storing university information to further develop access and versatility. Regular cloud backups ensure that data might be immediately reestablished, and a cloud-based disaster recuperation system keeps on working in case of a crisis. To protect delicate information, university data is scrambled prior to being put away in the cloud. To ensure that main approved people can get to information and cloud administrations, severe access controls are set up. The public cloud and the college's on-campus network are associated safely, considering consistent data integration and transfer. The essential stage for overseeing and storing data is the public cloud, with advantageous cloud administrations accessible for additional capability. By shaping networks with outside cloud providers, the college acquires more access to specific assets and capabilities.

KN College looks to make a more versatile, secure, and strong IT environment that can oblige the growing necessities of its staff, workforce, and students by trying this cloud reconciliation idea. This project will further develop data availability, facilitate disaster recuperation, and assurance that classified information is protected as per industry best practices for cloud security.

Components:

Cloud Service Providers:

There are different cloud service providers in the market i.e. Azure Cloud, IBM Cloud, Google Cloud etc. For this project, Azure Cloud will be used for the demonstration as well as for other purposes.

Cloud Integration Strategy:

1. Hybrid Cloud Model: The Hybrid Cloud Model integrates on-premises system with public cloud administrations to lay out a bound together computing environment. This approach works with information and application portability, improves disaster recovery capacities, and supports managerial consistence by overseeing delicate data inside while including the cloud for less basic functions.
2. Cloud Gateway: A Cloud Gateway is a development or administration that works with secure accessibility between a relationship's on-premises network and public cloud services. It acts as an entry point that manages and gets the data in cloud of KN University.
3. API Management: API management includes using a concentrated gateway to control and get API demands, implement strong measures, and handle API versioning. It consolidates consistent noticing, thorough documentation, and rate confining to guarantee viable use and integration.

Security and Consistence:

1. User verification: To affirm client identities and further develop security beyond passwords, authentication methods like multi-factor authentication (MFA) is utilized.
2. Access Control Policies: Utilizing ideas like Role-Based Access Control (RBAC) and Least Honor, arrangements that characterize client admittance to assets is created and carried out for KN.
3. IAM Jobs and rights: To diminish unapproved access, IAM roles to clients in view of their work obligations is made and appointed. These jobs have specific freedoms.
4. Directory Services Integration: To oversee identities and synchronize access limitations between on-premises and cloud environments, incorporate with directory services (like Active Directory and LDAP).
5. Data in transit: Encrypt information in transit as it goes among clients and cloud services or among several cloud administrations. Utilize TLS (Transport Layer Security) protocols to ensure that information is protected from manipulation and block attempt while it is being transmitted.
6. Data at Rest: To forestall unwanted access, encrypt stored data utilizing encryption strategies. Ensure the encryption keys are kept safe and aside from the data that is being encoded.
7. Key Management: To control the creation, storing, revolution, and access of encryption keys, set up areas of strength for a key management system (KMS). To safely keep up with keys, utilize third party tools or KMS arrangements from cloud suppliers.
8. Data Masking: To reduce exposure risk and safeguard information convenience for improvement and different purposes, use data masking methods.

Backup and Redundancy:

1. Backup: Keeping up with data backups can help shield against loss from unexpected erasure, corruption, or system failure. Computerized backup plans are laid out and backup is kept securely in cloud storage.
2. Redundant Systems: On the off chance that a primary system fails, redundant system or parts to keep up with continuous activity is used. This covers network redundancy (like a several network paths) and equipment redundancy (like multiple servers).
3. High Availability (HA): To decrease downtime and safeguard administration progression in case of a breakdown, high availability arrangements, like clustering and failover strategies is utilized.
4. Regional Redundancy: To prepare for site-explicit disasters or blackouts, store backups and redundant systems is introduced in a few different geographic areas of university i.e., Adelaide, Sydney and so on.

References

Gartner, Inc. (2021) Hype Cycle for Cloud Computing. Stamford: Gartner. Available at: https://www.gartner.com/en/doc/4482592/hype-cycle-for-cloud-computing (Accessed: 1 August 2024).

Cisco (2024) Cloud Gateways and Integration. Available at: https://www.cisco.com/c/en/us/solutions/collateral/cloud/what-is-a-cloud-gateway.html (Accessed: 1 August 2024).