11/12/2024

CLOUD MANAGEMENT

HOMEWORK #3

JOVITA ANDREWS

Part 1 (30 points):

Describe one of the Azure Security Services listed in

https://learn.microsoft.com/en-us/azure/security/fundamentals/services-technologies?

Solution: One of the key features of Azure Security Services is **Microsoft Defender for Cloud** is a comprehensive cloud workload protection solution that provides robust security management and advanced threat protection across hybrid cloud workloads. This service plays a crucial role in safeguarding Azure resources. Microsoft Defender for Cloud is an essential resource for organizations looking to protection their assets against cyber threats.

Key Features of Microsoft Defender for Cloud is as follows:

- **Security Management:**
  Microsoft Defender for Cloud offers centralized security management, allowing organizations to monitor and control the security posture of their Azure resources from a single dashboard. It provides continuous assessment and actionable security recommendations to help improve the overall security stance.

- **Advanced Threat Protection:** The service employs advanced analytics and threat intelligence to detect and respond to evolving cyber threats. It uses machine learning algorithms to identify suspicious activities and potential security breaches across your cloud workloads.

- **Hybrid Cloud Support:** One of the standout features of Microsoft Defender for Cloud is its ability to protect workloads not just in Azure, but also in other cloud environments and on-premises infrastructure. This makes it an ideal solution for organizations with hybrid or multi-cloud setups.

Benefits:

- **Unified Security Management:** Simplifies security operations by providing a single pane of glass for managing security across diverse environments
- **Continuous Monitoring:** Offers real-time visibility into the security state of your resources, helping to identify and address vulnerabilities quickly.
- **Compliance Assistance:** Helps orgranizations meet various regulatory requirements by providing built-in compliance controls and assessments.
- **Threat Intelligence:** Leverages Microsoft's vast threat intelligence network to provide up-to-date protection against the latest cyber threats.

Part 2 (30 points):

Describe one of the AWS Security, Identity and Compliance Services listed in https://aws.amazon.com/products/security/?nc=sn&loc=2?

Solution:

One of AWS's features is AWS Identity and Access Management (IAM), which helps you grow and manage workforce access and workload in a secure manner while fostering your creativity and agility. AWS IAM is essential to cloud security because it helps businesses effectively and safely control access to AWS resources.

Benefits of IAM:

- **Enhanced Security:** IAM helps ensure users only have access to resources they need, reducing potential attacks surfaces.
- **Centralized Access Management:** Manage and control access to all AWS account resources from a single point making it easier to enforce rules and regulations
- **Scalability:** It is easy to add or reduce users without compromising on security or manageability.
- **Improved Compliance:** Detailed logs and access controls aid in meeting regulatory compliance and security audits helping organizations maintain strict access governance.
- **Increased Flexibility:** With roles and federated access, organizations can seamlessly provide temporary access to resources or integrate existing identity providers.

Part 3 (40 points):

Choose a cloud provider (AWS, Azure, Google) and explore their "well-architected" framework (mentioned in the class slides) by selecting two of the pillars/elements/principles of the framework and describe for each, their main goals and intended benefits.

Note: The following are the links to the well-architected frameworks of AWS, Azure and Google:

AWS Well-Architected Framework

https://aws.amazon.com/architecture/well-architected

Microsoft Azure

https://learn.microsoft.com/en-us/azure/well-architected/what-is-well-architected-framework

Google Cloud Architecture Framework

https://cloud.google.com/architecture/framework

Solution:

I chose the pillars of framework of Google Cloud Architecture Framework:

1. Security, Privacy, and Compliance

- Main Goals: This pillar's main objective is to protect data and workloads by putting strong security procedures in place, protecting data privacy, and adhering to legal and regulatory standards. This entails protecting identity management, access control, data encryption, audit trails, and every other facet of cloud applications and infrastructure.

- Intended Benefits: This pillar reduces the risk of non-compliance with industry and regulatory requirements, improves user confidence, and helps avoid data breaches by optimizing security and compliance. Strong security procedures help businesses satisfy internal and external compliance requirements, safeguard confidential data, and lessen the possibility of unwanted access.

2. Reliability

- Main Goals: Building robust and highly available cloud systems that can continue to function in the face of interruptions or failures is the fundamental goal of this pillar. To guarantee constant operation and little downtime, it entails building systems with fault tolerance, recovery plans, and backup procedures.

- Intended Benefits: Improved user experience, a lower chance of revenue loss, and more assurance in the system's capacity to manage peak loads and bounce back from malfunctions are all advantages of a dependable design. By limiting disruptions and attaining high availability and performance, reliability increases the application's dependability for end users.

These two pillars — Security and Reliability — work together to provide a secure, resilient, and seamless experience for users, helping organizations protect their data and maintain a stable, high-performing infrastructure**.**