SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT, Cyber Security including Blockchain Technology)

19SB731 – CLOUD COMPUTING & VIRTUALIZATION

IV YEAR/ VII SEMESTER

UNIT 4 – VIRTUALIZED DATA CENTER ARCHITECTURE VDC ENVIRONMENTS

TOPIC – MANAGING VDC, CLOUD ENVIRONMENT AND INFRASTRUCTURES, INTEGRITY AUTHENTICATION, NON REPUDIATION, AVAILABILITY

Managing Virtualized Data Centers

Managing a VDC means overseeing the entire virtual environment that integrates physical hardware and virtual resources. This includes ensuring efficient use, performance, and security of these resources.

Objectives:

- **Optimize Resource Allocation:** Efficiently distribute computing, storage, and network resources to meet varying demands.
- **Maintain System Performance:** Monitor and adjust to ensure that all systems perform optimally and efficiently.
- **Ensure Security and Compliance:** Implement security measures to protect data and ensure adherence to regulations.

Challenges:

- **Resource Contention:** Multiple virtual machines (VMs) sharing the same physical resources may compete for resources, which can affect performance.
- **Performance Management:** Keeping track of and managing the performance of virtualized systems can be complex due to the dynamic nature of virtual environments.
- **Security Threats:** Ensuring security in a virtualized environment requires managing vulnerabilities and ensuring compliance with various standards.

Cloud Environment and Infrastructure

Cloud Computing Basics:

•**Public Cloud:** Services are offered over the internet by third-party providers. These services are scalable and cost-effective but shared with other customers.

•**Private Cloud:** An exclusive cloud environment dedicated to a single organization. It provides more control and security but can be more expensive.

•**Hybrid Cloud:** Combines both public and private clouds, allowing for greater flexibility and optimization of existing infrastructure.

Infrastructure Components:

•**Compute:** Virtual machines (VMs) or containers that provide processing power for applications. Managed by orchestration tools like Kubernetes for containerized applications.

•**Storage:** Different types of storage solutions, including:

- ❑**Object Storage:** For storing large amounts of unstructured data, such as files and backups.
- ❑**Block Storage:** For high-performance needs like databases.
- ❑**File Storage:** For sharing files across multiple systems.

•**Networking:** Virtual networks that allow communication between VMs and with external systems, including virtual private networks (VPNs) and load balancers.

Considerations:

Choose the appropriate cloud model based on your organization's needs and regulatory requirements.
Understand the cost implications and potential benefits of different cloud services.

Integrity and Authentication in VDCs

Data Integrity:

•**Hashing Algorithms:** Use cryptographic algorithms to create a hash value for data. Any changes to the data will alter the hash value, helping detect tampering.
•**Digital Certificates:** Ensure data integrity during transmission by using encryption and certificates to verify that data has not been altered.
•**Integrity Checks:** Regularly verify data to ensure it has not been corrupted or tampered with.

Authentication:

•**Multi-Factor Authentication (MFA):** Requires users to provide multiple forms of verification (e.g., password, SMS code) to access systems. This enhances security by making it harder for unauthorized users to gain access.
•**Single Sign-On (SSO):** Allows users to log in once and access multiple applications or systems. This simplifies the user experience and reduces the need for multiple passwords.

Implementation Tips:

Regularly update and review authentication methods to address new security threats.
Ensure all systems enforce strong data integrity and authentication measures.

Non-Repudiation

High Availability (HA):

•**Clustering:** Group multiple servers to act as a single unit. If one server fails, others in the cluster continue to provide services, minimizing downtime.

•**Failover Mechanisms:** Automatically switch to a backup system or resource when the primary system fails. This ensures continuity of service.

Redundancy:

•**Component Redundancy:** Use redundant components like power supplies and network paths to avoid single points of failure.

•**Geographic Redundancy:** Distribute critical systems and data across different locations to protect against localized failures or disasters.

Disaster Recovery (DR):

•**Replication:** Continuously or periodically replicate data to backup locations to ensure data is not lost in case of a failure.

•**Testing and Maintenance:** Regularly test disaster recovery plans to ensure they work effectively and update them based on changes in infrastructure or business needs.

Best Practices:

Continuously evaluate and improve HA and DR strategies to address evolving risks and technological advancements.
Ensure that all critical systems have well-documented and tested recovery procedures.

Summary

- **Key Points Recap:**

•**Managing VDCs:** Effective management involves optimizing resource allocation, maintaining system performance, and ensuring security.
•**Cloud Environments:** Understand different cloud types (public, private, hybrid) and their components to leverage cloud benefits effectively.
•**Security Aspects:** Focus on data integrity, authentication, non-repudiation, and availability to secure and maintain VDCs.
•**Availability:** Implement high availability and disaster recovery strategies to ensure continuous operation and minimize downtime.

Best Practices:

•Regularly review and adjust management practices based on current and future needs.
•Stay updated with the latest technologies and best practices in cloud computing and virtualization.
•Engage in ongoing training and development to ensure compliance and effective management of VDCs.

Actionable Steps:

•Continuously monitor and optimize VDC resources and security measures.
•Develop and test disaster recovery plans to ensure preparedness for potential disruptions.
•Stay informed about industry trends and advancements to keep your VDC management strategies current and effective.

THANK YOU