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 – CONCEPTS, PLANNING AND DESIGN, BUSINESS CONTINUITY AND DISASTER, DISASTER RECOVERY PRINCIPLES

Introduction to Virtualized Data Center Architecture (VDC)

A Virtualized Data Center (VDC) is a comprehensive IT environment where physical hardware resources are abstracted and managed through virtualization technologies. This approach allows for efficient allocation and management of resources across multiple virtual machines and applications.

Key Components:

Compute: Virtual Machines (VMs) run on hypervisors which abstract physical server resources into multiple virtual instances. Popular hypervisors include VMware ESXi and Microsoft Hyper-V.

Storage: Virtualized storage solutions like Storage Area Networks (SAN) and Network-Attached Storage (NAS) enable scalable and flexible storage management across the data center.

Network: Virtual networks and VLANs (Virtual Local Area Networks) enable flexible network configurations and isolation within the VDC.

Management: Platforms such as VMware vSphere or Microsoft System Center manage and automate the virtual environment, facilitating tasks like resource allocation, monitoring, and orchestration.

Benefits:

Improved Resource Utilization: Virtualization allows for better use of physical resources by running multiple VMs on a single physical server.

Enhanced Flexibility and Scalability: Resources can be easily scaled up or down based on demand without the need for physical changes.

Simplified Management and Automation: Centralized management tools streamline administration and automate repetitive tasks.

Planning and Design of VDC Environments

Assessment:

Begin by evaluating the current infrastructure to understand what resources you have and what you need. Assess future requirements by considering growth, new applications, and changing workloads.

Design Considerations:

•**Scalability:** Ensure that the VDC can handle future growth. This includes planning for additional VMs, storage, and network capacity.
•**Performance:** Design should address the performance needs of applications, including compute power, I/O throughput, and network bandwidth.
•**Redundancy:** Incorporate redundant components and failover mechanisms to ensure high availability and minimize service disruption.
•**Security:** Implement security measures such as firewalls, access controls, and network segmentation to protect data and applications.

Capacity Planning:

Use tools and methodologies to forecast future resource requirements based on current and anticipated workloads. Plan for peak usage to avoid performance bottlenecks.

Business Continuity in VDC Environments

Business Continuity involves ensuring that critical business functions remain operational despite disruptions. In a VDC, this means planning for redundancy and resilience.

Strategies:

•**Redundancy:** Deploy redundant hardware and software components to avoid single points of failure. For example, use dual power supplies and network connections.
•**High Availability:** Design systems so that they remain operational even when components fail. Techniques include clustering and load balancing.
•**Backup:** Regularly back up data, configurations, and virtual machines to protect against data loss and enable recovery.

Implementation:

•**Load Balancing:** Distribute workloads across multiple servers or resources to prevent any single resource from becoming a bottleneck.
•**Disaster Recovery Plans:** Develop and document procedures to restore services after an incident, including steps for data recovery and system restoration.

Disaster Recovery Principles

Disaster Recovery (DR) is about restoring normal operations after a major disruption, such as hardware failure or natural disaster, ensuring minimal downtime and data loss.

Key Components:

•**Recovery Point Objective (RPO):** Defines the maximum period of acceptable data loss. For example, if the RPO is 1 hour, data should be recovered to a point no more than 1 hour before the failure.
•**Recovery Time Objective (RTO):** Specifies the maximum allowable downtime. For example, if the RTO is 4 hours, services should be restored within 4 hours of a disruption.

DR Strategies:

•**Site Recovery:** Implement failover solutions using remote data centers or cloud-based recovery sites to ensure that services can continue if the primary site fails.
•**Data Replication:** Use technologies to replicate data in real-time or on a scheduled basis to backup sites, ensuring that recent data is available for recovery.
•**Testing and Maintenance:** Regularly test DR plans to ensure they work as expected and update them based on changes in the IT environment or business requirements.

Summary

Key Concepts Recap:

•Virtualized Data Centers (VDCs) offer improved efficiency and flexibility in managing IT resources.
•Proper planning and design are crucial to accommodate growth and ensure performance.
•Business continuity and disaster recovery strategies are essential to minimize disruptions and ensure resilience.

Best Practices:

•Continuously monitor the VDC environment to ensure optimal performance and availability.
•Regularly review and update disaster recovery plans to reflect changes in the infrastructure and business needs.
•Implement proactive measures, including regular backups and redundant systems, to enhance reliability.

THANK YOU