V20PCA107 - IT INFRASTRUCTURE MANAGEMENT 2.0

UNIT - III_WEEK - 8

Bare Machine

In IT infrastructure management, a "bare machine" refers to a physical computer or server that has no operating system (OS) or any software installed on it. It's essentially a "bare metal" system, which means it's just the hardware without any software layer, like an operating system or hypervisor, managing the resources.

Here's how a bare machine fits into IT infrastructure management:

1. **Bare Metal Servers**: These are physical servers that are dedicated entirely to one user or tenant. Unlike virtualized environments where multiple virtual machines (VMs) share the same physical hardware, bare metal servers provide full access to the underlying hardware, offering better performance and control.
2. **Installation of OS and Software**: Managing a bare machine involves installing an operating system (like Linux, Windows Server, etc.) and configuring the necessary software stack. This can be done manually, through automated scripts, or using provisioning tools.
3. **Provisioning and Automation**: Tools like PXE (Preboot Execution Environment), Kickstart (for Red Hat-based systems), or Windows Deployment Services (WDS) can be used to automate the installation of an operating system on a bare machine. These tools help in managing multiple servers efficiently, especially in data centers.
4. **Cloud and Virtualization**: In a cloud environment, you might hear about "bare metal" instances, which are cloud services that provide dedicated physical servers. These are often used when performance, security, and resource isolation are critical.
5. **Configuration Management**: Once the OS is installed, configuration management tools like Ansible, Puppet, or Chef can be used to manage the

software and settings on the bare machine. This includes installing packages, applying security patches, and ensuring the system adheres to the desired configuration state.

6. **Monitoring and Maintenance**: After setup, the bare machine must be monitored for performance, security vulnerabilities, and hardware issues. Tools like Nagios, Zabbix, or Prometheus are often used to monitor these systems in real-time.

In summary, a bare machine is the foundational layer in IT infrastructure, requiring careful management and configuration to ensure it operates efficiently and securely.

Bare Metal Recovery (BMR) in IT Infrastructure Management

Bare Metal Recovery (BMR) is a crucial process in IT infrastructure management that involves restoring a system from scratch, including the operating system, applications, and data, onto a completely new or bare hardware platform. This process is essential for disaster recovery, hardware failure, or system migration.

1. Introduction to Bare Metal Recovery

- **Definition**: BMR is the process of restoring a complete system, including the OS, applications, and data, to a new or freshly wiped hardware platform.
- **Purpose**: Used to recover from catastrophic failures, migrate systems to new hardware, or quickly provision new servers.

2. BMR Components and Tools

- **Backup Software**: Tools like Symantec Backup Exec, Acronis True Image, and Veeam Backup & Replication.
- **Boot Media**: CD/DVD, USB, or network boot (PXE) containing the BMR software.
- **Backup Storage**: Local disks, NAS, SAN, or cloud storage where backups are stored.

3. Planning and Preparation

- **Identify Critical Systems**: Determine which systems require BMR capabilities.
- **Regular Backups**: Schedule regular full system backups to ensure up-to-date recovery points.
- **Documentation**: Maintain detailed documentation of system configurations, applications, and backup procedures.

4. Backup Process

- **Full System Backup**: Includes the OS, applications, system settings, and data.
- **Incremental/Differential Backups**: Capture changes made since the last full backup to reduce backup time and storage requirements.
- **Offsite Storage**: Store backups in multiple locations, including offsite or cloud storage, for added redundancy.

5. Recovery Process

- **Boot into Recovery Environment**: Use boot media to start the recovery process on the bare metal server.
- **Locate Backup**: Access the backup storage location to retrieve the necessary backup files.
- **Restore System**: Follow the BMR software instructions to restore the OS, applications, and data.
- **Post-Recovery Configuration**: Configure network settings, verify system integrity, and ensure all services are running correctly.

6. Testing and Validation

- **Test Recoveries**: Regularly perform test recoveries to verify that the BMR process works and backups are valid.
- **Validation**: After recovery, validate the system's functionality, data integrity, and application performance.

7. Challenges and Best Practices

- **Hardware Compatibility**: Ensure compatibility between backup images and new hardware. Use universal restore features if available.
- **Downtime Minimization**: Plan BMR processes to minimize downtime, especially for critical systems.
- **Security**: Secure backup storage locations and ensure data encryption during backups and recovery.

8. Disaster Recovery Planning

- **Integrate BMR into DR Plan**: Ensure BMR processes are part of the overall disaster recovery strategy.
- **Recovery Objectives**: Define RTO (Recovery Time Objective) and RPO (Recovery Point Objective) for systems requiring BMR.
- **Documentation and Training**: Document BMR procedures and train IT staff on the recovery process.

9. Automation and Orchestration

- **Automate Backups**: Use backup software to automate regular full and incremental backups.
- **Scripted Recovery**: Develop scripts to automate parts of the BMR process, reducing manual intervention and potential errors.

10. Monitoring and Maintenance

- **Backup Monitoring**: Monitor backup jobs for success or failure and address issues promptly.
- **Regular Maintenance**: Regularly update backup software and firmware on backup storage devices.
- **Capacity Planning**: Ensure sufficient storage capacity for backups and adjust retention policies as needed.

Bare Metal Recovery is a critical capability for ensuring business continuity and quick recovery from catastrophic failures. By implementing robust BMR processes, leveraging appropriate tools, and regularly testing recovery procedures, organizations can minimize downtime, protect data integrity, and ensure rapid restoration of critical IT services.

Data Retention

Data retention involves storing data for a defined period, typically for purposes such as legal compliance, ensuring business continuity, and supporting data analytics.

How to Manage Data Retention

As organizations accumulate data, the associated costs for storing, maintaining, and protecting it increase. Data retention describes the policies and processes you implement to keep data that is still useful or must be kept for regulatory or compliance reasons, while discarding data that is no longer required.

What Is Data Retention?

Data retention is the act of storing data for future use. A data retention policy is an organization's system of rules for managing the information it generates and collects. This includes identifying the information and deciding how it is stored, the period for which it is stored, and how it is deleted afterwards.

The primary factors that should be considered when defining your data retention policy are your business requirements and the use case for the data, the costs of storing it, and any regulatory or compliance concerns that may surround it.

What are the risks of retaining too much data?

Storing data that no longer has any usefulness can have detrimental effects on your organization. As your data inventory increases, it compounds the following negative effects on your business:

- **Increased clutter:** Large amounts of data are more likely to become disorganized, requiring additional infrastructure and tools to store and manage.
- **Regulatory burdens and security risks:** This disorganization can lead to sensitive data being accidentally disclosed. Additionally, while historical personal data about your customers is rarely useful for ongoing business operations, it is a popular target for theft. This leaves you open to regulatory and civil legal repercussions.
- **Costs and labor:** Additional infrastructure and tools increase the costs of retaining data, as do the labor and resources required to maintain its availability while keeping it protected.

In addition to these business factors, there are legal requirements that specify the timelines some categories of data can be kept for. Some require the immediate deletion of data after it has been used, while others demand that data be kept indefinitely.

By building a comprehensive retention policy, all of these concerns can be recognised and addressed in a single document. You can then share this document within your organization and your users, ensuring that stakeholders are aware of how all of your data is handled, and acting as the basis for automated data retention actions.

How to build a good data retention policy

Regardless of which industry your business operates in, you must implement a data retention policy to protect your valuable data assets and remain compliant. The processes that your data retention policy establishes should accomplish the following objectives:

- Improve the speed and efficiency of managing and accessing data
- Reduce costs by cutting down on storage infrastructure.
- Eliminate potential failure points and vulnerabilities inherent in huge data systems
- Limit liability and ensure compliance with industry guidelines and government regulations

- Communicate how the above is achieved in clear language so that it can be precisely implemented and communicated with your users

The following practices should be considered necessary when deciding on your data retention policy and its implementation.

Introduction to Computer Security

- **Definition**: Computer security, also known as cybersecurity, is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money, or interrupting normal business processes.
- **Importance**: Essential in safeguarding IT infrastructure, protecting data, and ensuring operational continuity.

2. Fundamental Concepts

- **Confidentiality**: Ensuring that sensitive information is accessed only by authorized individuals. Techniques include encryption and access control.
- **Integrity**: Ensuring that data is accurate and has not been tampered with. Hashing and digital signatures are commonly used.
- **Availability**: Ensuring that information and resources are available when needed. This involves maintaining up-to-date systems and providing reliable backups.
- **Authentication**: Verifying the identity of users or systems. Common methods include passwords, biometrics, and multi-factor authentication.
- **Authorization**: Determining if a user has permission to perform a specific action, often implemented through access control lists (ACLs) or role-based access control (RBAC).

3. Types of Threats

- **Malware**: Malicious software such as viruses, worms, Trojans, and ransomware designed to damage or disrupt systems.
- **Phishing**: Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communications.
- **Man-in-the-Middle (MitM) Attacks**: An attacker intercepts and possibly alters the communication between two parties without their knowledge.

- **Denial-of-Service (DoS) Attacks**: Attacks aimed at making a system or network resource unavailable by overwhelming it with traffic.
- **Advanced Persistent Threats (APTs)**: Prolonged and targeted attacks in which an intruder gains access to a network and remains undetected for an extended period.

4. Security Technologies

- **Firewalls**: Network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.
- **Antivirus Software**: Programs designed to detect and remove malware.
- **Intrusion Detection and Prevention Systems (IDPS)**: Tools that monitor network or system activities for malicious activities and respond automatically.
- **Encryption**: The process of converting data into a code to prevent unauthorized access. Examples include AES, RSA, and SSL/TLS.
- **Virtual Private Networks (VPNs)**: Secure connections between a user's device and the internet, protecting the data that travels across the connection.
- **Public Key Infrastructure (PKI)**: A framework for creating, managing, and distributing digital certificates for secure communications.

5. Security Policies and Procedures

- **Security Policies**: Formalized rules and practices that govern how an organization manages and protects its information.
- **Incident Response Plan**: A predefined process for detecting, responding to, and recovering from security incidents.
- **Disaster Recovery Plan (DRP)**: A strategy for recovering IT systems, data, and operations after a catastrophic event.
- **User Training and Awareness**: Educating users on best practices for security, such as recognizing phishing emails and using strong passwords.

6. Compliance and Legal Considerations

- **Regulatory Requirements**: Understanding and adhering to laws and regulations such as GDPR, HIPAA, and PCI DSS.
- **Auditing and Monitoring**: Regularly reviewing systems and processes to ensure compliance and identify potential security gaps.

- **Data Protection Laws**: Regulations that dictate how organizations must protect and handle sensitive data.

7. Emerging Trends and Challenges

- **Cloud Security**: Protecting data and applications hosted on cloud platforms. This includes managing security in a shared responsibility model.
- **IoT Security**: Securing the growing number of Internet of Things devices, which are often less secure than traditional IT devices.
- **Zero Trust Architecture**: A security model that assumes threats are present both inside and outside the network and requires strict verification for anyone trying to access resources.
- **Artificial Intelligence (AI) in Security**: Using AI and machine learning to detect and respond to security threats faster and more accurately.