Network server system management

Mahmudov Elvin

Abstract

It is important that every system built in the network communicates with each other. When systems are built, each system in the network performs other tasks, and all systems must be connected to create a complete system. A network administrator is needed for connections and then a system administrator is needed to manage the systems. However, network and system problems can be resolved and network and system management becomes easier. When setting up physical or virtual servers, it is important to write the system correctly. Virtual systems are built on top of the system written on the physical server, and the system becomes more complex. As systems become more complex, their management becomes more complex

Keywords: Sistem Administration, configuation management, server virtualization, log and event management.

Network server system management refers to the process of effectively managing and maintaining network servers, a central component of an organization's information technology infrastructure. This process is crucial to ensuring that a business's data, applications and other network services are delivered in a secure, accessible and high-performance manner. A more comprehensive description of network server system management is provided below. Network server system management has a major impact on the success of the organization as it is a key component of the organization's IT infrastructure. This process plays a vital role in ensuring reliability, security, performance and business continuity. Therefore, skilled system administrators, automation tools and following best practices contribute to the successful execution of this process. System management refers to the function of carrying out the duties and responsibilities required to ensure the efficient and safe operation of an organization's information technology infrastructure. A systems administrator typically maintains network servers, workstations, and other IT components and ensures the uninterrupted operation of these systems. Here are the key components of system administration:

Sistem Administration

Server management refers to the effective management and maintenance of servers that form a central part of an organization's network infrastructure. These servers perform many functions such as hosting applications, data storage, user access, database services and more. Server installation is the physical installation of new servers and their integration into the network. After operating system selection and installation, hardware and software configurations should adjusted. During update and maintenance processes, server operating systems and applications should kept up to date, and at the same time, performing regular maintenance operations and checking the hardware is important for the servers. Security management is the implementation of firewalls, antivirus software, security patches and access controls to ensure the security of servers. Special attention paid to the protection of sensitive data. In capacity planning, it is necessary to monitor the resource usage of the servers and estimate future needs and make a plan when capacity increase or new servers need to be added.

Network Management

Network management refers to the process of ensuring that the network infrastructure, which is an important component of an organization's information technology infrastructure, operates effectively and securely. This process includes a series of activities from establishing, configuring, updating and monitoring the network infrastructure. In network design and planning work, the network must designed and planned in accordance with the requirements. This includes network topology, device positioning, and security strategies. In network configuration, it is the installation and configuration of network devices (router, switch, firewall, etc.). This process includes IP addresses, subnets, VLANs, and other network settings. In security management works, ensuring network security, using firewalls, VPNs, security protocols and security policies are preliminary tasks. Wireless network management is the planning, configuration and management of wireless networks and ensuring security and access control. Network management plays a

fundamental role in ensuring data communication, security and business continuity of organizations. Good network management increases the reliability of the network, speeds up troubleshooting processes and ensures that documentation about the network kept. It also helps organizations keep pace with rapidly changing technology and provides a competitive advantage.

Backup and Recovery

Backup and recovery are important IT processes used to prevent loss or disaster of data and systems and to ensure business continuity. These processes help organizations protect their data and restore it quickly when necessary. Data protection is the protection of data lost due to user errors, hardware failures, software problems or malware. Disaster preparedness is the protection of data in the event of natural disasters, fires or other disasters. In Full Backup, all data backed up. It is often time consuming and storage space intensive. Data recovery is the restoration of stored data, this process is fast and data focused.

System recovery does not involve using server or system backups or quickly rebuilding servers after a disaster. Disaster recovery plans use detailed plans and procedures to ensure post-disaster business continuity. Backup and recovery are critical to ensuring organizations' business continuity and data integrity. A good backup and recovery strategy helps organizations prepare for data loss or disaster. These strategies include making regular backups, storing backups securely, and performing regular recovery tests. It is also important to create well-planned disaster recovery plans to ensure a quick return to normal business processes after a disaster.

Server virtualization is an IT technology and method that converts physical servers into virtual servers and enables multiple operating systems to run on the same physical hardware. This technology enables more effective use of server resources, rapid deployment and flexibility. Server virtualization increases the efficiency of the IT infrastructure while also providing cost savings. It also puts an end to servers' dependence on physical hardware and enables better sharing of resources. There are 2 types of Hypervisor in virtual servers. Type 1 Hypervisor runs directly on the physical server and does not require any operating system. Type 2 Hypervisor runs on a host operating system and provides more flexibility. The virtual machine managed via VM. Virtual machines are managed through VM creation, configuration and management processes. Resource management in a virtual machine is the effective management and sharing of CPU, memory, storage and network resources. Resource allocation between virtual machines is important.

Log and event management is a critical process for maintaining the security and effectiveness of an organization's information technology infrastructure. This process is concerned with collecting, analyzing, monitoring logs, and detecting and handling incidents. Log management is the creation of log records of IT components such as computers, servers, network devices, and applications. These logs are used to record system activities and user interactions. Log collection is the collection, secure storage and management of log data in a central location. Log collection tools and software used for this process. In log analysis, the aim is to analyze log data and detect unwanted events and security violations. This used to identify malicious activities or errors. Automation and alarm, on the other hand, log analysis tools generally create automatic alarms, indicating situations when certain conditions met. This supports a rapid response. In reporting and compliance, log reports used to meet compliance requirements and provide data to managers. For example, PCI DSS or HIPAA compliance.

Incident Management

Incident Detection is the detection of events that meet certain conditions through log analysis and event management systems. This used to identify malicious activities or security threats. Incident response is the determination and implementation of procedures to respond to specific events. For example, closing the vulnerability or stopping the attack. Incident investigation involves examining the events in detail and understanding how the event occurred. This helps prevent and prevent future incidents. In incident records and documentation, each event recorded and these records are documented. This is important to meet legal requirements and support the investigation of incidents.

Log and event management plays a critical role in protecting organizations' data security and detecting and

addressing attacks. Logs and events help organizations monitor anomalies in their networks and systems, enabling early detection and rapid response to malicious activity. Therefore, a good log and event management strategy is important for IT security and can help comply with various regulations and compliance requirements.

References

1. Network Management: Principles and Practice by Mani Subramanian, pages 144-223
2. The Practice of Network System Administration" by Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, pages 225
3. Network Management: Concepts and Practice" by J. Richard Burke, pages 156-265
4. Principles of computer systems and Network Mangement by Dinesh Chandra Verma
5. Client/server Computing Architecture, Applications, and Distributed Systems Management By Bruce R. Elbert, Bobby Martyna 1994
6. Virtualization: A Manager's Guide" by Dan Kusnetzky provides an excellent overview of virtualization technologies, including hypervisors.7. Vechetek, L. (2019). Use post-deployment information to improve IT implementation efficiency, pages 1-167
7. The Art of Virtualization" by K. A. Arun and S. Arunraj covers various aspects of virtualization, including hypervisor technology, pages 1-49
8. The Practice of System and Network Administration by Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, pages 57-349
9. Windows Server 2016 Inside Out by Orin Thomas and William R. Stanek, pages 15-178
10. PowerShell for Sysadmins: Workflow Automation Made Easy, pages 1-89