**Server Management**

**Assignment & Answer Sheet**

For Learner Use:

|  |  |
| --- | --- |
| Surname of Learner | Naidu |
| Name of Learner | Kian |
| Learner ID | 0110105463084 |
| Student Number | KNPMB070 |
| Date of Test Given | 23/08/2021 |
| Location / Branch | iStudent Academy, Durban |

For Assessors Use:

|  |  |
| --- | --- |
| Name of Branch | Durban |
| Name of Facilitator |  |
| Name of Assessor |  |
| Assessor Number |  |
| Mark Allocation | 130 |
| Mark Obtained |  |
| Competency Status (C / NYC) |  |

|  |  |
| --- | --- |
| Unit Standards MICT Seta | 114043, 114053, 114054, 114065, 114066, 114073 |

|  |  |  |  |
| --- | --- | --- | --- |
| Candidates Signature | C:\Users\KIAN\AppData\Local\Microsoft\Windows\INetCache\Content.Word\(KNPMB070)Kian Naidu.jpg | Date of Submission | 13/09/2021 |
| Assessors Signature |  | Date Marked |  |

**Instructions to Learner:**

* Read all Questions Carefully
* Use proper grammar
* Provide *Screenshots* if instructed by question.
* Marks will be deducted for plagiarized work.

**Question 1 (60 marks)**

Explain in clear and great detail, in your own words the following technologies and the importance thereof.

1. Central store for Administrative Templates(4) explain 4 valid points.
2. Network printing
3. Implementation of Group Policies
4. Server Virtualization
5. Implementation of AppLocker
6. PKI Infrastructure
7. DNS Zones / Zone Transfers
8. Virtualized Domain Controllers
9. RODC & Server Core
10. Managed Service Accounts
11. Branch Cache
12. Dynamic Access control
13. Distributed ADDS Deployments
14. ADDS Replication
15. AD RMS

|  |
| --- |
| 1. Central store for Administrative Templates   The central store is a location for .admx files and anyone with permissions to create or edit Group Policy Objects (GPOs) can access. A central store ensures that whenever someone edits a GPO that the settings in administration templates are always the same. The central score also allows for centralized location of storing files, so when Microsoft releases .admx files for newer operating systems you will only need to update the .admx files in a single location instead of all locations. When setting up a central score it must be done manually, and then also updated manually on a domain controller.   1. Network printing   This allows multiple computers to print using single/multiple printers so that the workload is shared amongst many computers. This can be done through wired or wireless connections to connect the computers to the printers to transfer information between them for the print jobs. Network printing usually has a print server as this allows the printer network to operate more efficiently and reduce the data load.  This allows for print jobs to happen faster as the print server is dedicated and has more processing power than the printers. This streamlines communication and saves time in a company setting.   1. Implementation of Group Policies   A group policy is a hierarchical infrastructure which allows a network admin in charge of Microsoft’s Active Directory to implement specific configurations for both users and computers. A group policy is mainly a security tool and can be used to apply security settings to users and devices. Group policies are collectively called group policy objects (GPOs) and are based on a group of individual policy settings. GPOs are administrated from a central interface known as the Group Policy Management Console. A group policy can be managed with the command line interface such as gpresult and gpupdate.   1. Server Virtualization   The process of dividing a physical server into more than one unique virtual server by using a software application. Each virtual server is able to run it’s own OS independently from each other. Server virtualization allows for cheaper operating costs and increased application performance. There is 3 types of virtualization: full virtualization, Para-Virtualization and OS level virtualization.  Full virtualization uses a hypervisor, Para virtualization uses the entire network working together as a single unit. OS-level virtualization does not need a hypervisor and instead the virtualization capability, which is a part of the physical server OS.   1. Implementation of AppLocker   Applocker advances the app control features and functionality of software restriction policies. Applocker has extensions that allow you to create rules that allow or deny certain apps from running based on the identities of files and Applocker also specifies which user or group can run restricted apps. Applocker allows you to define rules based on file attributes such as the digital signature of the file, file name or even file version. You can also assign a rule to a security group or just an individual user. With Applocker you may also create exceptions so that all processes may run except the one you want to be disabled.  Applocker reduces administrative overhead and reduces a company’s cost of managing computer resources.   1. PKI Infrastructure   A set of roles/policies needed to create, manage, use store and revoke digital certificates and manage public key encryption. This allows you to facilitate secure electronic transfer of information for communication over a network. A PKI infrastructure allows users/servers to securely exchange information using digital certificates. PKI is a 2-key asymmetric encryption and the two keys are called the public key and the private key which are mathematically linked so that only the receiver can decrypt the information sent by a device. A devices private key is used to encrypt the information and the mathematically linked public key is used by the receiving device to decrypt the information so data can only be read by the devices that have the public key.   1. DNS Zones / Zone Transfers   A portion of the DNS namespace that is managed by a specific admin or company. A DNS zone is an admin space that allows for easier control of DNS components such as authoritive name servers. A DNS zone can contain multiple subdomains and multiple zones can exist on one server. A domain name space is a hierarchical tree with the DNS root domain at the top. A DNS zone starts at a domain within a tree and could also move down into the subdomains so that multiple subdomains can be managed by a single person.   1. Virtualized Domain Controllers   A server computer that responds to security authentication requests within a computer network domain. It is a network server that’s in charge of allowing hosts to access resources in a domain. It also authenticates users and stores user account information so that it can verify that the users that log on can access information they are privileged to. A domain controller also enforces security policy for a domain to ensure that no user can use something that is not allowed by company policy. A virtual domain controller is controlled by software such as Hyper-V as resources are allocated to it accordingly and it is completely run by virtualization methods and has no physical components.   1. RODC & Server Core   A Read Only Domain Controller (RODC) is a server that hosts am active directory databases read only partitions and can also respond to security authentication requests.  RODC was designed to be used in branch offices that cannot support their own domain controllers. It allows you to deploy a DC in remote sites where physical security is somewhat ideal. The benefits of an RODC is that it allows for faster login times on remote sites and gives secure access to resources on the network. The limitations of RODC are that you can only install one RODC per AD site, per domain. A domain admin should also need to run the installation. By default RODCs do not store passwords so this could be seen as a disadvantage to the standard DC. To install a RODC you will need to input various commands into the powershell module.   1. Managed Service Accounts   Managed service accounts allow you to run programs with an account that does not require a password while still having the security of a strong password. Passwords are managed by AD for you and are randomly generated and strong passwords. Passwords are cycled regularly which helps to keep accounts more secure. Managed server accounts also support deployment to server farms, which means that the accounts can be deployed to multiple servers.   1. Branch Cache   This is a bandwidth optimization feature that enhances network application responsiveness when users try to access content from a central office. A copy of the content that is retrieved from the web server is cached within the branch office. If someone else requests the same content, the user can download it directly from the local branch network instead of re-downloading the content again.  BranchCache works in two types of modes: Distributed or Hosted Mode. Distributed allows clients to request cached information from one another, while Hosted Mode centralizes the cache on a BranchCache server.   1. Dynamic Access control   This allows users to apply access control and restricted permission depending on conditional rules for accessing files and folders dynamically.  DAC lets you create classifications or tags that can apply on the shared file resources such as giving it a tag based on the department.  There is a central access rule that can have conditions involving user groups, user claims, device claims, and resource properties. These can be combined into a central access policy which can act as an additional layer of security for a company.   1. Distributed ADDS Deployments   Allows for the distribution of AD DS services to be deployed to multiple devices. AD DS Deployments allow admins to manage and store information about resources from a network as well as app data in a distributed database. This helps admins manage network elements which are both computing devices and user and reorder them into a custom ordered structure. AD DS also integrates security by authenticating logons and controlling access to directory resources.   1. ADDS Replication   This is a method of transferring/updating AD objects from one DC to another DC. The connections between these domain controllers are built based on their locations within a forest and site. Each site in AD has one or more subnets which identify the range of IP addresses associated with the site. Connections are configured between sites to make sure that the AD objects have actually been replicated between the sites.   1. AD RMS   Active Directory Rights Management Services is a server software for information rights management that is shipped with windows server. It uses encryption and a form of selective functionality denial for limiting access to documents and web pages. Companies can use this technology to encrypt their information stored in documents, and using the policies embedded in the documents, prevent the protected content from being decrypted except by authorized users. This authorization only lasts for a specified amount of time before access is revoked. Specific operations such as editing, copying or deleting can be allowed or disallowed by authors for individual pieces of content, then the RMS admins can deploy these RMS templates that group these rights together into predefined rights that can be applied to multiple devices |

**Question 2 (20)**

1. Provide legible and well explained **detailed screenshots** of each and every step on how you Install and Configure a Domain Controller. There should be a minimum of 5 written steps (own Words) and 5 screenshots.(10)

|  |
| --- |
| 1.Go to Server Manager  2. Select add roles and features and in the add roles and features wizard select next.    3. Select the role based or feature based installation and then click next    4. On server selection click on the server you want to install the roles and features on then click next    5. On server roles select the roles you want to install on the server, the minimum requirement to promote the server to a domain controller is AD DS. Ensure that AD DS is ticked at minimum.    6. Select next then confirm your selection in features and click next to install them.  Once the installation is complete close the window  7. Back on server manager select the flag notification icon and under Post-deployment configuration select  Promote this server to a domain controller.  8. Under the AD DS Services Configuration wizard, make sure the add a domain controller to an existing domain is selected and that your domain choice is correct then select next  9. In the domain controller options tab select the DNS server and GC checkbox and ensure that the RODC checkbox is not ticked. Type in your password then click next  10. On the DNS options tab, click next.  11. On the Additional options tab click next.  12. On the paths tab click next.  13. On the prerequisites check click next.  14. On the installation tab click install and once the services are installed you can close the AD DS Services wizard.  15. Refresh server manager and in the dashboard select AD DS and observe that your server is there.  Once done you have successfully created a domain controller. |

1. Explain the relevance and importance of a fully functional domain controller in a business environment.(10)

|  |
| --- |
| 1. A domain controller authenticates users’ identities by checking the stored credentials and ensuring that they match. A DC also makes sure that only trusted users are able to connect to the company resources.  2. A domain controller stores user account information which is used to validate the correct usernames and passwords.  3. Security policy enforcement ensures users follow the companies set policies that are made per user so that there is no violation of the company policies such as restricting flash drive access per user and disable any user accounts immediately after they leave the company.  4. Allows for shared computer resources since you can set access privileges that require specific login, so anyone can use any computer in the company to do their work.  5. Lower cost and centralized management as you have the ability to set login and security information configuration for all devices from a central hub which saves costs and resources instead of doing it individually for all devices. |

**Question 3 (9)**

Name and explain in full, three transitional technologies used in to effectively manage IPv6 Traffic on IPv4 Infrastructure.

|  |
| --- |
| Teredo (IPv6) Tunneling – Gives full IPv6 connectivity for hosts that are able to run IPV6 that are on the IPv4 internet but have no native connection to an IPV6 network. Tunneling allows for the transport through encapsulation of one protocol within another protocol. This tunneling encapsulates IPV6 packets within IPv4 packets. This allows for communication without the need to upgrade IPv4 infrastructure  Dual-Stack IPv4 and IPv6 – Deploys IPv6 directly from the networks infrastructure. It allows devices to run IPv4 and IPV6 in parallel, allowing hosts to simultaneously reach IPv4 and IPv6 content.  IPv6 Translation – This technology allows the translation between the packet header formats in IPv6 and IPv4. This is meant to translate packets with IPv6 addresses to those with IPv4 addresses so that IPv6 only hosts are able to communicate with IPv4 only hosts. |

**Question 4 (10)**

Provide legible and well explained **detailed screenshots** of each and every step on how you implement DNS. There should be a minimum of 5 written steps (own Words) and 5 screenshots.

|  |
| --- |
| 1. Select Server manager.    2. Click the option manage on the top-right then select add roles and features    3. On the add roles and features wizard, on the before you begin tab click next.    4. On the installation type tab select role based or feature based installation then click next.    5. On the server selection tab select your server then click next    6. On the server roles tab select DNS Server then click next.    7. On the features tab click next then on the DNS Server tab click next.  8. On the confirmation tab click on install then next. Once installed you can close the wizard and your DNS Server has been successfully created. |

**Question 5 (12)**

Explain these concepts, and the importance thereof:

1. WSRM
2. FSRM
3. Health Policy
4. Quotas and File Screening

|  |
| --- |
| 1. WSRM   Windows System Resource Manager enables the allocation of system resources such as the CPU and memory (RAM) as well as applications. WSRM can also allocate resources among multiple applications that are on a server according to the policies that are put in place. WSRM prevents apps with memory leak from affecting normal healthy applications and protects healthy applications.   1. FSRM   File Server Resource Manager allows you to manage and classify data that is stored on file servers. FSRM automatically classifies files and performs tasks based on these classifications.  FSRM has the following features: Quota management, File classification Infrastructure, File screening, Store reports and File management.  FSRM set quotas on folders which allow you to limit the space allowed for a folder and can automatically be applied to new folders. FSRM can create reports that monitor the storage usage of files and trends in disk usage so you can see how your data is classified.   1. Health Policy   A health policy ensures that your computer is healthy and there is nothing that performs abnormally. A health policy can ensure that the systems anti-virus is kept up to date and the virus definitions are regularly updated and kept current so that there is little risk of data breach. A health policy also keeps the devices drivers up to date to ensure the best and most current functionality. Network access protocol is also kept updated as it is a set of rules that determine how data is sent between different devices on the same network and the health policy is in place to keep the NAP up to date.   1. Quotas and File Screening   Quotas allow you to limit the space allowed for a folder and can automatically be applied to new folders that are created as well as its subfolders that are on a file server.  File screening helps control the types of files that a user can store on a file server. File screening can limit the extension that can be stored for your shared files. As such an example is that you can create a file screen that restricts files that have a jpeg extension to be stored on a file server. |

**Question 6 (10)**

Authentication Methods

1. Explain what is a Multi-site Failover Cluster?

|  |
| --- |
| This is a group of clustered nodes that are distributed through multiple sites in a region or even separate regions connected with a low latency network and storage. Cluster nodes can be connected a local SAN storage while replicated to a local SAN storage. Replication is done by identical software defined storage on each site. Software defined storage will replicate volumes or logical unit number (LUN) from the main site to a disaster recovery site. A failover cluster is configured with pass-through storage. All these clusters work together to provide increased availability and scalability so that if one node were to fail there would always be another node that would be available. The clustered roles are proactively monitored to make sure that they work correctly, and if they do not they are restarted or moved to another node. Failover clusters also provide cluster shared volume (CSV) functionality that can provide consistent and distributed namespace that clustered roles can use to access shared storage from all nodes. |

1. Explain how one can maintain a Failover Cluster

|  |
| --- |
| You can add nodes from an existing always on failover cluster instance (FCI) and this is accomplished using SQL server setup program. Other tasks such as changing the IP address resource, recovering from certain FCI scenarios are done by using the Failover Cluster Manager snap-in, which is the management snap-in for windows server failover clustering (WSFC). You can also tune the heartbeat settings of the failover cluster and check that the nodes in the cluster are healthy and working correctly. You can also remove a node from an existing failover cluster instance from an FCI by running SQL server setup on the computer that you want to remove from the FCI. |

**Question 7 (9)**

Explain in full, how to implement a Windows Server Backup and restore strategy. Approximately 8 – 10 steps in your own words.

|  |
| --- |
| 1. Open server manager  2. Select on manage then Add roles and features  3. In the add roles and features wizard, select next and configure your installation type and destination server.  4. In the features tab ensure that windows server backup is ticked then select next.  5. In the confirmation tab select install and close the wizard.  6. Go back to server manager and select the tools option and then below select the windows server backup option.  7. On the action tab of the new window that popped up select the backup you want such as backup once.  8. In the backup once wizard select your method of backup then click next.  9. Under the select backup configuration tab choose custom or full server backup then click next.  10. Under the specify destination tab select the location where you want the backup to be stored and click next.  11. Specify the remote location if it is on a shared folder and click inherit then next.  12. On the confirmation tab select backup and the backup will be successfully created. |

***The End!***