New Zealand Diploma in System Administration Level 6

NET602: Network Services

Assessment/Aromatawai - Assessment 2 v2
Practical

Credits/Whiwhinga 7

	Submission	FER1	FER2
Result	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Date	Click or tap to enter a date.	Click or tap to enter a date.	Click or tap to enter a date.
Assessor's Signature			

Student Name	Click or tap here to enter text.
Student ID	Click or tap here to enter text.
Student Signature	
Assessor	Click or tap here to enter text.

Assessor's Feedback

Submission

Click or tap here to enter text.

FER1

Click or tap here to enter text.

FER2

Click or tap here to enter text.

Assessment Instructions and Guidelines for Submission

Task Completion

- All tasks must be completed to receive a mark. Submissions with incomplete or missing tasks will be marked as Incomplete and not entitled to further FER.
- Any storage media (flash drive, disk, etc.) submitted must be virus free. Media containing malware or content that cannot be run directly will be marked as a Fail.
- Submissions will be judged based on completeness, correctness and clarity. Please refer to the assessment schedule for more details.

Format

- All written submissions must:
  - Be formatted in size 11 Arial font.
  - Have 1.15 line spacing**.**
  - Include a title page with the candidate's name, class and Aspire2 student ID clearly printed.
- All pages and printouts must include the candidate's Aspire2 student ID in the footer.
- You may need to attach the task cover sheet found on Canvas to the front of the final submission of your task (Please confirm with your tutor).

Submission

- All written work will be submitted via Turnitin in your Canvas LMS course unless otherwise specified.

Due Date

- Refer to your Canvas LMS course for specific due dates.

Competency-based Assessment Resubmission and Re-enrolment

- Students will have an opportunity to provide further evidence twice.
- To be eligible for a FER the student must make a reasonable attempt at the questions/tasks in the assessment.
- *Reasonable* is to be defined as a response that at the very least attempts to address the question/task.
- Where the student does not make a reasonable attempt at ALL questions/tasks they will not achieve and will be required to re-enrol in the paper.
- A fee of $250 is payable for the second FER.
- The need for further evidence from the students will be noted on the assessment as "FER" and dated.
- When the further evidence is deemed adequate the "FER" notation will be crossed out, initialled and dated.
- If a student is still deemed not yet competent after the second FER they will be required to re-enrol in the paper. A fee will apply for re-enrolment and details will be available in the Programme Handbook, and students will be informed of them at the start of the program.

- Additional FER's are at the discretion of the Head of Faculty.

Reconsideration of Assessments and Appeals

- Students have the right to a reconsideration of assessment or appeal if they believe an assessment has been incorrectly marked or graded.
- The request for reconsideration must be made in writing to the Head of Faculty within five (5) working days of the return of the assessment. A fee of $40 per assessment applies.
- Students must be informed that, as a result of the reconsideration of assessment, their result may be unchanged, raised or lowered.
- The reconsidered result will be recorded as the final result. Students retain the right to appeal this result.

Plagiarism

- By submitting your assignment, you agree to the Aspire2 Education policy on 'Academic Dishonesty and Plagiarism'. Assignments completed using unfair means or plagiarised material will receive a FAIL grade.
- All tasks must be done in your own words and referenced using APA 7th edition.

Feedback

- You may request feedback from your lecturer to verify the accuracy of your marks.
- Any feedback and grading results will be available in the Canvas LMS within the timeframe specified by your Programme Handbook.

Assessment Criteria

Course Aims
The objective of this course is to provide learners with knowledge and skills on the implementation of advanced networking principles and protocols.

Graduate Profile Outcome (GPO)
• GPO1(2 Credits) Plan and use services, technologies, and tools to automate the deployment and management of devices, applications, and infrastructure by way of scripts to automate standard systems procedures. • GPO3(5 Credits) Investigate and implement advanced network security solutions to protect and secure assets, troubleshoot, and mitigate threats and attacks, and to meet best practice and organizational requirements.

Learning Outcomes/Tīpako
LO2. Implement and manage secure network solutions using automated system procedures according to best practice.

Task Mapping/Mahere Mahi		Learning Outcome/Tipako
1.1, 1.2	Second Domain Controller Integration and User Authorization.	LO2
2.1	Deploying Print Management Solution via Group Policy Object.	LO2
3.1, 3.2	Implement and Managing MFA for network access.	LO2
4.1, 4.2, 4.3, 4.4	Manage the remote access via VPN.	LO2
5.1, 5.2	Implementing Server Backup.	LO2
6.1, 6.2	Implement and Managing Intrusion Detection System (IDS).	LO2
7.1	Update Existing Network Diagram.	LO2

Student Undertaking

I have read and understood the assessment instructions given above. I understand that I will be given zero marks and will be reported to the disciplinary committee if I am found cheating or engaging in any academic misconduct.

Student Name: Click or tap here to enter text.

Student Signature: X _____

Aspire2 Student

Date: Click or tap to enter a date.

Case Scenario

As the designated network administrator for TechCo Solutions, you have been tasked to implement and manage a secure on-premises network solution for the company. The company has a specific operational strategy requirement to maintain its data, infrastructure, and network services within its current building, aligning with its unique business requirements, and emphasizing the importance of a well-managed and secure on-premises network.

This project aims to establish and maintain a secure and well-managed network infrastructure that ensures authorized user access, protects sensitive data against potential threats, and optimizes operational maintenance processes. To achieve these objectives, you have chosen to adopt an automated system procedures approach, utilizing PowerShell scripting as the primary tool for automation to complete the selected tasks below.

Business Requirements

As proof of concept, you are required to complete Tasks 1–7 in a simulated virtualised lab environment.

- **Data Security:** Establish a secure and encrypted communication channel for remote access to safeguard sensitive information.
- **Operational Strategy:** Maintain data, infrastructure, and network services within the current building, emphasizing the importance of an on-premises network solution.
- **Scalability:** Address scalability concerns to accommodate increased data volume and evolving user requirements, aligning with imminent business expansion plans.
- **Efficiency:** Optimize IT infrastructure for enhanced efficiency, streamlining network processes to support overall business operations.
- **User Management:** Implement solutions that enhance user management processes, providing a seamless experience for employees accessing network resources.
- **Fault Tolerance:** Implement high availability and fault tolerance mechanisms, especially concerning critical components like domain controllers, to minimize downtime in case of failures.
- **Security Oversight:** Integrate advanced security measures to monitor and detect suspicious activities, enhancing the overall security posture of the network.

The following is the current network infrastructure diagram of TechCo Solutions. Refer to this diagram to complete all the required tasks.

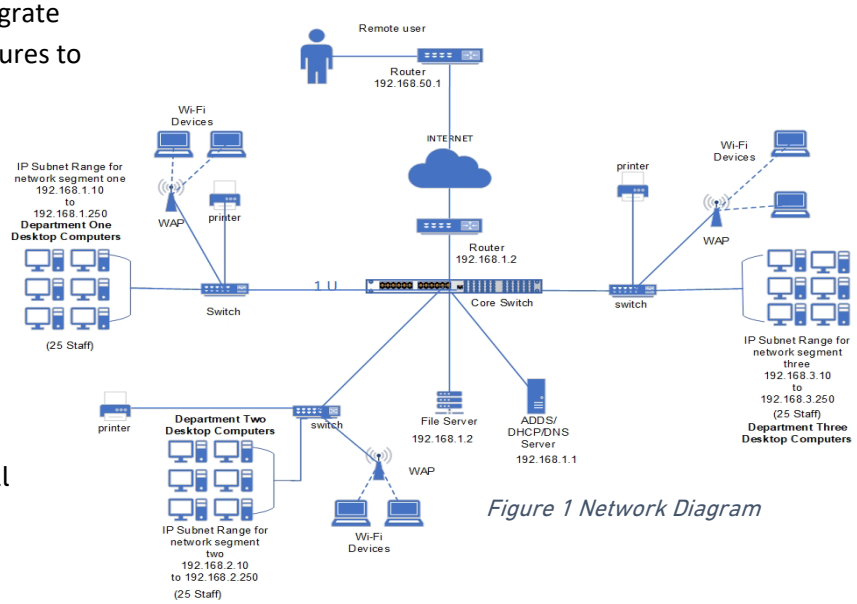

Figure 1 Network Diagram

Task Instructions

Most of the tasks below require you to have your work verified by your tutor. Your tutor will complete a task verification checklist as you progress through the assessment. Once the checklist is complete, your tutor will sign off and you must submit the form as part of your final assessment submission.

Task/Mahi 1: Second Domain Controller Integration & User Authorization

TechCo Solutions has experienced increased user load and is concerned about the existing domain controller's capacity to ensure uninterrupted services to network resources. To mitigate potential service disruptions and facilitate load balancing, the company is seeking to implement a second domain controller. Additionally, there is a need for an automated process to enhance the efficient management of user accounts. The task involves integrating a second domain controller into the existing network and creating user accounts through a PowerShell script using an automated system procedure.

The tasks to be completed are as follows:

Task 1.1

Create a PowerShell script to set up and integrate a second domain controller into the existing network infrastructure to enhance load distribution, ensure high availability and establish fault tolerance.

- Domain name – *techco.co.nz*
- Conduct testing to validate both the configuration and functionality of the second domain controller.
- Document your key steps, including relevant screenshots.
- Ask your tutor to verify your work.

Task 1.2

To streamline the onboarding and offboarding processes and ensure timely access control updates, the IT manager has requested you automate the approach the manage the active directory user accounts. You are required to:

- Create a PowerShell script to automate user creation in Active Directory.
- New users will be provided in a CSV file according to the table below:

Last Name	First Name	Group
Smith	Mary	Management
Lo	Lan	Account
Warner	Shreya	IT
Tang	Eric	IT
Singh	Harmandeep	Management
Jackson	William	Account

- Test the script in the test environment to ensure the script is functioning.
- Document your key steps, including relevant screenshots.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 2: Deploying Print Management Solution via Group Policy Object

Task 2.1

TechCo Solutions employs various printers across different departments, resulting in inconsistent print management practices. To simplify and standardize the print management solution deployment, the company aims to utilize a centralized printer management server and deploy client versions of the printer management application via Group Policy Object (GPO).

In order to simplify and standardize the process of installation and sharing printers across the organisation's network, you have decided to centralize the printer management and share the client version of the printer management application to end-user machines using GPO to ensure proper access control and consistent printer configurations across the organization.

Tasks:

- Set up and configure a printer management system/server to centrally manage printers and their configurations.
- Identify and procure the client version(s) of the printer management application that are compatible with end-user machines.
- Package the client application for deployment via GPO.
- Conduct testing to verify that the client version of the printer management application is installed on targeted machines and ensure that the deployed application functions correctly and provides access to the centrally managed printers.
- Capture screenshots of all the key processes.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 3: Implementing & Managing Multi-Factor Authentication (MFA) for Network Access

You need to secure network access to the organization's internal resources. The organization is concerned about the risk of unauthorized access and wants to implement MFA to enhance the security of user logins to the network. To achieve this, you are tasked with both implementing MFA and automating the deployment process to client machines. It is essential to adhere to best practices and security guidelines to ensure a robust and secure MFA implementation.

Task 3.1

You are required to implement MFA for network access and automate the process of deploying MFA for employees by completing all the following tasks:

- Set up the MFA platform on a server and automate the deployment of MFA to the client machines.
- Set up user enrolment and configuration. You are required to specify a secure password policy and use it in the user enrolment.

User 1

- Username: `user1`
- Password: `secured password`
- Enrol user in the authentication app.

- Test the MFA setup with a client machine to ensure proper user authentication functionality and troubleshoot any issues as needed.
- Make sure to screenshot and document all key steps taken during the implementation and troubleshooting.
- Ask your tutor to verify your work on your task verification checklist.

Task 3.2

The manager of TechCo Solutions has reported that a new employee is facing difficulties receiving notifications from MFA when attempting to log in. Consequently, the new employee is unable to access their work device. Your responsibility is to troubleshoot the MFA configurations on a client machine and MFA Admin App.

- Check and troubleshoot the MFA configuration on client machines and MFA Admin App.
- Address the root cause of the issue once it has been identified.
- Test the MFA services on the client machines by logging in as the created user to verify that the MFA is functioning properly.
- Document your key steps during the troubleshooting process and resolve the problem, including relevant screenshots.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 4: Manage the remote access via VPN

TechCo Solutions requires secure remote access to protect sensitive data for employees who are working remotely to access the company's resources. Before the implementation, you would like to evaluate the effectiveness of the VPN in enhancing network security and providing secure remote access. You are conducting a proof of concept to evaluate network management and security in a virtualized environment. Your tasks are as follows:

Task 4.1

- Set up and configure a member server of the domain to act as a VPN server.
- Provide a specific IP range for 40 remoter users.
- Clearly define the subnet and ensure adequate address space.

Task 4.2

- Set up a secure VPN connection using an industry practice encryption technique.
- Ensure that the connection is only accessible to authorized employees based on their respective user groups.
- Additionally, set the default idle timeout for VPN connections to 15 minutes.

Task 4.3

Enable access to the following network resources and services through the VPN tunnel:

- Allow VPN Connection:
  - Allow inbound VPN traffic to the virtual AD server from the VPN clients' IP range.
- Allow file sharing for a shared folder:

    - Allow inbound traffic to TCP port 445 for the VPN clients' IP range to access shared folders on the virtual AD server.
- All other access should be restricted for security purposes.

Task 4.4

- Test the VPN connectivity to verify the setup and configuration.
- Make sure to screenshot and document all key steps from Task 4.1 to Task 4.4 taken during the implementation and troubleshooting.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 5: Implementing Server Backup

Task 5.1

TechCo Solutions seeks to enhance data security by automating server backup deployment using PowerShell Script. The objective is to establish a robust backup system for critical data on a designated server while adhering to industry best practices.

- Create a complete backup policy using PowerShell Scripts to automate the backup process for the company. The backup policy will cover aspects such as managing data volumes, implementing robust security measures, specifying backup targets and establishing schedules to ensure regular and reliable backups.
- Ask your tutor to verify your work on your task verification checklist.

Task 5.2

As proof of concept, your task is to utilize the PowerShell Script created in Task 5.1 to set up and configure Windows Server Backup. The specific requirements include:

- Configure Windows backup using the PowerShell Script.
- Conduct thorough testing of the backup system to verify that backups are completed and stored in a network folder to enhance accessibility and security.
- Simulate recovery scenarios to validate the system's ability to restore data accurately and reliability for a specified folder.
- Document the key steps of configuration, testing and debugging, including relevant screenshots.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 6: Implementing and Managing Intrusion Detection System(IDS)

TechCo Solutions has become increasingly concerned about potential cybersecurity threats. To strengthen the network security posture, the company has decided to deploy an Intrusion Detection System (IDS). The goal is to monitor network activities, detect suspicious behaviour, and respond promptly to potential security breaches.

As proof of concept, set up and configure IDS to monitor and detect suspicious activities. You are required to complete the following tasks:

Task 6.1: IDS Deployment and Configuration

- Research and select a suitable IDS solution for TechCo Solutions. Justify your selected IDS solution.
- Install and configure the selected IDS on designated servers or network devices.
- Document the IDS deployment processes, including configurations and settings.
- Capture screenshots of key processes during the installation and configuration of IDS and rules.
- Ask your tutor to verify your work on your task verification checklist.

Task 6.2: Integration, Testing, and Documentation

- Integrate the IDS with the existing network architecture of TechCo solutions.
- Develop and implement alert rules aimed at identifying and monitoring network activity using TCP, UDP and ICMP protocols within the network infrastructure.
- Conduct thorough testing of the alert rules within the IDS to ensure reliable detection of network anomalies.
- Document your key steps, including relevant screenshots.
- Ask your tutor to verify your work on your task verification checklist.

Task/Mahi 7: Update Existing Network Diagram

Task 7.1

Having implemented various changes to enhance the current network infrastructure, such as integrating a second domain controller, deploying MFA, establishing VPN, and implementing additional security measures, your responsibility as the network administrator is to create an updated network diagram that reflects these enhancements.

- Incorporate all the implemented changes made to the TechCo Solutions network infrastructure.
- Use appropriate symbols and labels to denote the components, their interactions, and the flow of data.
- Ensure the diagram provides a comprehensive overview of the updated network infrastructure post-implementation of the specified tasks.

Evidence and Judgement Statements

Learning Outcomes	LO2. Implement and manage secure network solutions using automated system procedures according to best practice.
Documentation	The student has provided all the required documentation, including a completed task verification checklist signed off by the tutor. **Note:** All the documentation must be submitted with suitable screenshots. Steps must be explained properly where necessary and comments should be provided if any selection must be made from a given batch of options.

Task	Task Description	Evidence Criteria	Judgement
1.1	Create a PowerShell script to set up and integrate a second domain controller into the existing network infrastructure to enhance load distribution, ensure high availability and establish fault tolerance. • Domain name – techco.co.nz	• The student creates a PowerShell script to set up and configures the second domain controller on the Windows Server virtual machine with the domain name given. • The script includes a minimum of three comments explaining the purpose and functionality of the distinct code segments. • The student conducts thorough testing to validate the configuration and functionality as a second domain controller using different test scenarios. • The student submits the script and relevant screenshots.	• The student has set up and configured the second domain controller using the PowerShell script successfully. • The student has tested the second domain controller is functioning accordingly.
1.2	Create a PowerShell script to automate user creation for Active Directory. New users will be provided in a CSV file from your tutor according to the table provided. Test the script in the test environment to ensure the script is functioning. Document your key steps, including relevant screenshots.	• The student creates users for Active Directory using PowerShell with the details provided in the task requirements. • The student tests the script to verify the user creation is working correctly. • The student submits the script and relevant screenshots.	• The student has created the user account and removed the users from the Active Directory using PowerShell according to the task instructions. • The student has tested the script to verify the tasks are completed correctly.

Task	Task Description	Evidence Criteria	Judgement
2.1	TechCo Solutions employs various printers across different departments, resulting in inconsistent print management practices. To simplify and Setup and configure a printer management system/server to centrally manage printers and their configurations. • Identify and acquire the client versions of the printer management application compatible with end-user machines. • Package the client application for deployment via GPO. • Conduct testing to verify that the client version of the printer management application is installed on targeted machines. • Ensure that the deployed application functions correctly and provides access to the centrally managed printers. • Capture screenshots of all the key processes. • Ask your tutor to verify your work.	• The student setups and configures the Printer management server accordingly. • The student deploys the client printer management application via GPO. • The student verifies that the client version of printer management application is running properly. • The student tests the deployment of the printer management server can manage centralized printer. • The student submits the screenshots of the configuration and testing process.	• The student has successfully set up and configured the printer management server.to enable sharing and access control. • The student has packaged the client application via GPO deployment. • The student conducted thorough testing to verify installation on targeted machines and ensure proper functionality and access to centrally managed printers. • The student submitted clear documentation and screenshots of all key processes. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.
3.1	You are required to implement MFA for network access and automate the process of deploying MFA for employees by completing all the following tasks: • Set up the MFA platform on a server and automate the deployment of MFA to the client machines. • Set up user enrolment and configuration. You are required to specify a secure password policy and use it in the user enrolment. • Test the MFA setup with a client machine to ensure proper user authentication functionality and troubleshoot any issues as needed. • Make sure to screenshot and document all key steps taken during the implementation and troubleshooting. • Ask your tutor to verify your work.	• The student sets up the Duo platform on the server and on a client machine. • The student creates a user account and completes the configuration for the user. • The student automates the process of deploying the MFA to the client machine using GPO. • The student tests the MFA setup on both the server and client to ensure the function is working successfully. • The student troubleshoots any technical issues encountered and resolves the problem. • The student provides screenshots of key steps.	• The student has successfully set up the MFA platform on a server and automated the deployment of MFA to client machined using GPO. • The student has established user enrolment and configuration with a secure authentication policy according to the requirements. • The student has conducted a thorough testing of the MFA setup on the client machine. • Any issues encountered during testing were effectively troubleshooted. • The student documented all key steps taken during implementation and troubleshooting. • Screenshots were provided for clarity and verification purposes. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.

Task	Task Description	Evidence Criteria	Judgement
3.2	The manager of TechCo Solutions has reported that a new employee is facing difficulties receiving notifications from MFA when attempting to log in. Consequently, the new employee is unable to access their work device. Your responsibility is to troubleshoot the MFA configurations on a client machine and MFA Admin App. • Check and troubleshoot the Duo configuration on client machines and MFA Admin App. • Address the root cause of the issue once it has been identified. • Test the MFA services on the client machines by logging in as the created user to verify that the MFA is functioning properly. • Document your key steps during the troubleshooting process and resolve the problem, including relevant screenshots	• The student checks and troubleshoots the MFA configuration on both the server and client. • The student identifies the root cause of the issue. • The student fixes the identified root cause. • The student tests the MFA on the client machine and makes sure the MFA is properly working on the client machines. • The student documents key steps taken during the troubleshooting process. Included relevant screenshots illustrating the troubleshooting steps and resolution of the issue for clarity and verification purposes.	• The student has successfully troubleshot and identified the root cause of the issue with MFA notifications on client machines and the MFA Admin App. • The student has resolved the problem with MFA notifications and restored access for the new employee. • The student has tested and verified the functionality of MFA, including receiving notifications was working appropriately. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.
4.1	Set up and configure a member server of the domain to act as a VPN server. Provide a specific IP range for 40 remoter users. Clearly defines the subnet and ensures adequate address space.	• The student installs and sets up a VPN server on a member server. • The student specifies the IP range according to requirements.	• The student provides screenshots of key steps. • The student has successfully set up and configured a member server of the domain to act as a VPN server according to the requirements.
4.2	Set up a secure VPN connection using an industry practice encryption technique. Ensure that the connection is only accessible to authorized employees based on their respective user groups. Additionally, set the default idle timeout for VPN connections to 15 minutes.	• The student sets up a secure VPN connection using an industry practice encryption. • The student configures the VPN on the server with proper security settings and tested the connectivity from a remote client machine. • The student allows proper inbound traffic to access the shared folder.	• The student has set up a secure VPN connection using an industry-standard encryption technique • VPN is only accessible to authorized employees based on their respective user groups.

Task	Task Description	Evidence Criteria	Judgement

4.3	Enable access to the following network resources and services through the VPN tunnel:
	• Allow VPN Connection.
	  ○ Allow inbound VPN traffic to the virtual AD server from the VPN clients IP range.
	• Allow file sharing for a shared folder.
	  ○ Allow inbound traffic to TCP port 445 for the VPN clients IP range to access shared folders on the virtual AD server.
	• All other access should be restricted for security purposes.
		• The student accesses the shared folder using VPN connections.
		• The student restricts user access according to the requirement.	

4.4	Test the VPN connectivity to verify the setup and configuration. Make sure to screenshot and document all key steps from Task 4.1 to Task 4.4 taken during the implementation and troubleshooting. Ask your tutor to verify your work.	• The student tests the VPN connectivity, access to network resources and services from a remote client.	• The student has performed thorough testing of the VPN to demonstrate successful connection establishment and access to network resources/services as specified. • The student documented all key steps taken during the implementation and troubleshooting of Tasks 4.1 to 4.4. • Included relevant screenshots illustrating the setup, configuration, and testing processes for clarity and verification purposes. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.
5.1	TechCo Solutions seeks to enhance data security by automating server backup deployment using PowerShell Script. The objective is to establish a robust backup system for critical data on a designated server while adhering to industry best practices. Create a complete backup policy using PowerShell Scripts to automate the backup process for the company. The backup policy will cover aspects such as managing data volumes, implementing robust security measures, specifying backup targets and establishing schedules to ensure regular and reliable backups.	• The student creates a backup policy using a PowerShell script. • The student outlines the key components in the script. • The student adds proper comments in the PowerShell script. • The student provides a proper explanation of the backup policy components ensuring data safety and best practices.	• The student has created a comprehensive backup policy utilizing PowerShell scripts to automate the backup process for TechCo Solutions. • The student has submitted and explained the script that included all the key components required.

Task	Task Description	Evidence Criteria	Judgement
5.2	As proof of concept, your task is to utilize the PowerShell Script created in Task 5.1 to set up and configure Windows Server Backup. The specific requirements include. • Configure Windows backup using the provided PowerShell Script. • Conduct thorough testing of the backup system to verify that backups are completed and stored in a network folder to enhance accessibility and security. • Simulate recovery scenarios to validate the system's ability to restore data accurately and reliability for a specified folder. • Document your key steps, including relevant screenshots. • Ask your tutor to verify your work.	• The student executes the PowerShell script to configure backup. • The student conducts thorough testing of the backup system. • The student simulates recovery scenarios to validate data restoration. • The student provides an explanation and screenshots of the testing process and its results.	• The student has successfully set up and configured Windows Server backup using PowerShell created in Task 5.1. • The student has conducted comprehensive testing of the backup system to ensure that backups are completed and achieved all components specified in the script. • The student simulates recovery scenarios to validate the system's ability to restore data accurately and reliably for a specified folder. • The student documents all key steps taken during the setup, testing, and recovery simulation, including relevant screenshots. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.
6.1	TechCo Solutions has become increasingly concerned about potential cybersecurity threats. To strengthen the network security posture, the company has decided to deploy an Intrusion Detection System (IDS). The goal is to monitor network activities, detect suspicious behaviour, and respond promptly to potential security breaches. As proof of concept, set up and configure IDS to monitor and detect suspicious activities. You are required to complete the following tasks: 1. Research and select a suitable IDS solution for TechCo Solutions. Justify your selected IDS solution. 2. Install and configure the selected IDS on designated servers or network devices. 3. Document the IDS deployment processes, including configurations and settings. 4. Capture screenshots of key processes during the installation and configuration of IDS and rules.	• The student researches and selects a suitable IDS solution. • The student provided proper justification for the selected IDS solutions according to the organisational requirements. • The student installs and configures the selected IDS. • The student provides an explanation and screenshots of the installation and configuration process and its results.	• The student researched and selected a suitable IDS solution with its justification for TechCo Solutions. • The student successfully installed and configured the selected IDS on designated servers or network devices. • The student documented the IDS deployment processes comprehensively, including configurations and settings. • The tutor successfully verified the completion of tasks by the student, ensuring all requirements were met satisfactorily.

Task	Task Description	Evidence Criteria	Judgement
6.2	Integrate the IDS with the existing network architecture of TechCo solutions. Develop and implement alert rules aimed at identifying and monitoring network activity using TCP, UDP and ICMP protocols within the network infrastructure. Conduct thorough testing of the alert rules within the IDS to ensure reliable detection of network anomalies. Document your key steps, including relevant screenshots.	• The student integrates the IDS with the existing network architecture. • The student implements various alert rules to monitor the network activity according to the requirements. • The student tests the alert rule to validate its functionality. • The student provides an explanation and screenshots of the integration, configuration, testing and its results.	• The student has successfully integrated the IDS with the existing network architecture of TechCo Solutions. • The student has developed, implemented and tested alert rules aimed at identifying and monitoring network activity using TCP, UDP, and ICMP protocols within the network infrastructure. • The student conducted thorough testing of the alert rules within the IDS to ensure reliable detection of network anomalies. • Relevant screenshots were provided to illustrate the configuration and testing processes.
7.1	Having implemented various changes to enhance the current network infrastructure, such as integrating a second domain controller, deploying MFA, establishing VPN, and implementing additional security measures, your responsibility as the network administrator is to create an updated network diagram that reflects these enhancements. Incorporate all the implemented changes made to the TechCo Solutions network infrastructure. Use appropriate symbols and labels to denote the components, their interactions, and the flow of data. Ensure the diagram provides a comprehensive overview of the updated network infrastructure post-implementation of the specified tasks.	• The student implements all the changes in the updated network diagram. • The student utilizes suitable symbols and labels to represent network components. • The diagram provides a clear overview of the changes made to the existing network infrastructure.	• The student ensured that the network diagram incorporated all the implemented changes made to the TechCo Solutions network infrastructure. • The student used appropriate symbols and labels to denote the components and their interactions. • Symbols and labels were clear, concise, and consistent, facilitating easy interpretation of the diagram. • The student presented the diagram in a clear and organized manner, ensuring ease of understanding for viewers.