CONESTOGA
Connect Life and Learning

Student Name:	Aagam Sanjay Shah
Deliverable:	Assignment
Course Name:	NTWK8181-24F-Sec1-IT Environmental Planning

Date Assigned:	24/11/2024
Date Due:	01/12/2024
Rules:	• Individual. • Cheating is not allowed. • Plagiarism counts as cheating! • That FAILURE to submit work in the course can result in a grade of 'F' or 'I' for failure to complete the course!

Table of Contents

Question 1: Plan Requirement

1) Why must a plan be required for a change to the central database server, specifically upgrading the core software on that database system? What role does your plan fulfil in relation to other groups/teams that depend on this central database server?

Explains why a plan is needed for a core software update

Central Database Server handles the critical data of the organization, Every organization make sure that their data is upto date and running without any issues to manage the daily exercises and its operations. To update the core software on the server, it is necessary to take backups, higher authority approvals and check the compatibility connectivity with other applications and their dependencies. To perform any critical update or activity on critical infrastructure of the organization plan is required how to perform and what will be steps/phases to perform the same. It requires coordination with group/teams, software-server vendors, and other stakeholders approvals too.

Why plan is needed? :

To keep the infrastructure well planned so that in case any issue arises the administrator or the activity handlers are ready to take the appropriate actions without wasting time or extending the downtime.

Updating core software helps in increasing the performance of the applications, services, connectivity, reducing space constraints and other benefits.

Planning of the core software update gives better idea of what has to be performed in which order or phase, if also gives brief idea of any additional resources required to achieve the task.

Plan is required to reduce the activity failure chances, It helps to evaluate the downtime requirement, impact on other applications, services and operations of the organization. By planning the activity risk is evaluated and makes easy to monitor the same.

To check Core Software dependency on other applications, services, It helps to check the compatibility of the software with other applications and its functionality such as version updates.

If something goes wrong in the activity of core software update, quick rollback or restoration of data actions can be placed and performed as it is considered a kind of risk/disruption while planning the activity.

Provides details on plan rollout.

This can be planned and rolled out as well as performed in different ways.

Taking backup as the first steps towards safeguarding the data from any loss by any actions performed on the critical server.

Each Team, Departments, Managers, Administrators are informed about the plan of actions with its details at regular intervals, so that every individual team or members can take their backups and save the data to avoid any impact due to this upgrade.

Testing is necessary to check the impact and time required to perform the activity, observe the compatibility of other applications, connections, services and so on.

Plan rollout helps in troubleshooting the issues before the update on production server, like best practices are teams perform update on UAT servers before performing on Production servers.

Provides details notification for the plan.

Notification of the plan can be done through different channels in the organization, such as Emails, SMS, Meetings, instructions from Managers or support teams, higher authorities, application notifications, and so on.

As the plan activity begins, the Downtime of services, operations unavailability is informed prior to the activity is starts.

The notification provides the details of the activity such as Downtime, Rollback time, monitoring time, different phases, impacts, strategies, timelines and

support details in case any issue is faced or observed by stakeholders or users in the organization.

Question 2: Backup and Recovery

2) Building on question 1, please explain how you would incorporate backup and recovery procedures within the upgrade plan? What are some of the requirements that should always be included?

Provides details on incorporating back-up and recovery procedures.

Backups are taken as per organization policies, criticality, dependencies, and best practices to safeguard the data from any kind of circumstances.

Backup Procedures

There are different kinds of backup taken such as: Full Backup, Incremental Backup, Partial backup, and Differential backup.

Like every organization, admins have a habit of taking backups at different intervals and saving at different locations as per their practices and purposes.

As a Best practice to perform the planned update of the critical software server database, it is necessary to take the full backup before performing the activity.

So that backup can be validated where the data is safe and compatible, check the data to avoid any corruption.

Some of the requirements that should always be included are Additional Hardware Requirements, Storage Requirements, and a few other needs.

Recovery procedure

In case of any circumstances of issue faced, the data can be recovered easily and further review the cause of the issue. It is also helpful to perform rollback of the planned activity. This can happen in situations like applications are not compatible, performance issues, disasters, etc.

The recovery phase helps to make things back to the situation as it was before performing the upgrade of the infrastructure. This helps to make the operations and services available as it was earlier and allows the organization to perform its routine operations.

Provide an explanation on the key requirements that those procedures must address.

Key requirements of the procedures are as followed

Backup of the data, infrastructure to be verified and backup taken at regular intervals. Also, we need to check the availability of data, compatibility, and whether data is corrupted or not. Additional space requirements can be the requirement to address the performance of the new update.

Multiple backups to be taken and saved on different locations such as on local data center, disaster recovery sites, on cloud platforms and on remote storage locations to safeguard the same from any impact or loss.

Question 3 : AD Major components

3) You are asked by your supervisor to list three major components that are required to be updated during an active directory migration from an on-site resource to a cloud-based resource. Please identify those three components and explain why they are important.

The 3 major components while updating an active directory migration from on-site resource to a cloud-based resource are as followed:

1. **Users, resources, roles, OU structure, dependency, connections.**
2. **Group object policies**
3. **Compatibility with Cloud Resources and on-site resources. Example: Single Sign-on**

Explanation on Major component 1 migration

1. Users, resources, roles, OU structure, dependency, connections.

Users roles, accessibility, authentication, authorization and their permissions to be synced with Cloud Resources and other dependent applications.

Migrations take place at different levels at different phases based on the accessibility and dependency with other servers and applications and resources in the organisation.

Their resource accessibility, such as applications, printers, share drives, Emails and other services with their accountability, need to be captured and migrated with On-cloud resources, as they have to be synced with on-premise Active Directory resources and cloud resources.

Explanation on Major component 2 migration

2. Group Object Policies

Group Object Policies are an important part of the organization; it is also a part of security measures placed by admins throughout the organization on different computers, OU, and groups.

All the policies placed at the OU level, user level, computer level, and domain level have to be synced with the Cloud platform.

Example: AWS cloud provides IAM to perform the Active Directory features.

Group object policies are to be audited at regular intervals to make sure the activity in placed as well as to check if any security measures are not compromised. GPOs are used to manage the user's and computer accessibility throughout the organizations. Each users and resources are given different permission and rights of accessibility at different level same has to be synced with Cloud resources this helps to reduce the impact of the unavailability of resources that can either be on-premise active directory resource or on-cloud resource.

Explanation on Major component 3 migration

3. Compatibility with Cloud resources and onsite resources

It should be compatible with cloud resources and onsite resources as it should not create dependency on either of the resources. Active Directory is a core

component of an organization, it helps to authenticate and authorize the users on daily basis to perform smooth accessibility in an organization to its users and resources. Each applications and resources should be compatible with Active directory and cloud resources. It should support other protocols, services, such as Single Sign-On, Multi-Factor Authentication and so on.

For example, Employee attendance is captured with the Active Directory's list of users and its services; if that is not available, it has a significant impact on the work efficiency of the organization.

Example: Single Sign-On → Users and applications need to access the applications, services, and web applications by single sign-on feature; this has to be compatible with the on-cloud resources.

Question 4: Problem areas

4) Building on Question 3, please explain three potential problem areas that need to be considered within the plan. How will these problem areas affect the migration, and what potential mitigation could be included to reduce their impact.

Explains problem areas

1. Latency in data synchronization

As on-premise data can be easily handled monitored and changes can be made by administrator in case of any impact or troubleshooting required to perform the same. Whereas, On-cloud migration the third party involvement is necessary and prompt actions are required.

For Example: Banking organisation or a Stock Broking organisation can't afford any delay in data synchronization, in this case the on-cloud and on-premises has to be in sync every time and it should be available.

2. Version Incompatibility of applications.

As On-premise applications runs on hardware that are purchase on upfront cost, which are usually not frequently upgraded neither updates. This leads to incompatibility of the application and resources. This can be addressed by updating the version of the connected application to the newer versions as per

the market and organizational standards to increase the performance and security.

3. Hardware, security issues

Sometimes, upgrading to new versions leads to firmware incompatibilities, which require additional resources to support the upgrade to meet the requirements. New hardware brings better performance as well as addresses new security measures this bring additional cost to the organization but it can be observed as one time expenditure rather than loosing data due to such issue.

Explains mitigation strategy for identified problem areas.

Migitgation Strategy to identify problem area are:

Rather than performing activity on production servers and databases, it is necessary to perform the same planned activity on UAT environments to observe the risk, issue, and compatibility.

This will help in identifying problems and monitoring the situation after and before the upgrade. It also allows us to perform rollback actions, which will reduce tasks and overhead actions.