Contents

1 EXECUTIVE SUMMARY

This report outlines the comprehensive efforts undertaken by the Yorkshire School System to expand and fortify its IT infrastructure, focusing on virtualization and network integration across multiple enterprise locations. The primary goal was to enhance operational efficiency, facilitate disaster recovery preparedness, and support scalable growth in IT services. Technologies leveraged include VMware vSphere, Windows Server 2019, Windows 10, Active Directory, DFS, WSUS, and Vembu Backup.

The project unfolded in two pivotal phases. Phase I involved the establishment of a second enterprise location with network enhancements, deployment of a new Windows Server 2019 as a domain controller, installation of Windows 10 clients, implementation of Vembu Backup for scheduled domain controller backups, setup of IIS web server with public, private, VLAN-specific pages, and DFS implementation. Phase II extended these efforts with the deployment of WSUS for centralized update management and additional tasks in PowerShell Remote and VMware ThinApp was used to virtualize Visio 7.

Key achievements included successful setup of network port groups and VLAN configurations, deployment of a second domain controller enhancing Active Directory resilience, and secure setup of backup solutions for critical domain resources. The IIS web server was configured to host accessible and secure web pages tailored to different user groups and VLANs. DFS implementation commenced to ensure data redundancy across domain controllers, laying a foundation for robust data management across enterprise sites.

Despite these accomplishments, challenges were encountered, notably the incomplete configuration of printer services intended for operational control and specific paper size support, which requires further attention. Resolving these challenges involved troubleshooting connectivity issues and refining configuration settings to align with operational needs.

In conclusion, this project successfully achieved its objectives by strengthening Yorkshire School System's IT infrastructure with scalable virtualization solutions and robust network management practices. Recommendations for future enhancements include completing printer configurations, refining DFS implementation for optimal data synchronization, and conducting regular performance audits of backup and update management systems to ensure sustained operational resilience and efficiency.

The appendices of this report include detailed problem-solving documentation for encountered challenges, ensuring a comprehensive understanding of solutions applied throughout the project's execution.

2 BUSINESS SCENARIO

The Yorkshire School System recently embarked on a significant project aimed at enhancing its IT infrastructure to support disaster recovery, seamless integration across multiple locations, and efficient management of IT resources. This initiative is crucial as the school system expands its services and ensures continuity in case of unforeseen events.

The project involved several key components. Firstly, the network infrastructure enhancement included the current network, which has the IP range 44.100.10.0/24 and uses the default gateway 44.100.10.1. The new location was assigned the IP range 44.100.60.0/24 and uses the default gateway 44.100.60.1.

Secondly, the domain services were strengthened by deploying a new instance of Windows Server 2019 as a second domain controller. Active Directory was updated with a new subnet/site, and FSMO roles were reassigned to optimize domain services. Thirdly, client services were improved by installing a Windows 10 machine at the new location, configuring, updating, and joining it to the domain.

Fourthly, backup solutions were implemented with Vembu Backup set up for scheduled backups of domain controllers, ensuring backups were stored securely and followed best practices for data conservation. Fifthly, web services were expanded by setting up a Windows Server 2019 to implement an IIS web server. Public, private, and VLAN-specific web pages were configured to accommodate different access levels.

Sixthly, data redundancy and accessibility were ensured by implementing DFS across the two domain controllers, with namespaces and replication configured to ensure data was available and synchronized across sites. Lastly, centralized update management was achieved by deploying a WSUS instance to manage updates for all clients and servers, with GPOs configured to ensure clients pulled updates from the WSUS server.

The applications used in this project included Windows Server 2019, deployed for domain controllers and the IIS web server; Windows 10, installed on client VMs for user access and testing; Active Directory (AD) for managing users, computers, and policies; Distributed File System (DFS) for data redundancy and accessibility; Vembu Backup for scheduled backups of domain controllers; and WSUS for centralized update management.

The Yorkshire School System aimed to ensure robust disaster recovery, data redundancy, and seamless integration across multiple locations. The project was driven by the need to expand services while maintaining a secure, resilient, and scalable IT infrastructure. Specific requirements included setting up a second enterprise location with proper network configuration, enhancing domain services by deploying a second domain controller and updating AD, implementing scheduled backups to secure data and ensure recovery in case of failures, expanding web services to accommodate different access levels, ensuring data redundancy and accessibility through DFS, and centralizing update management to streamline IT operations and maintain system security.

3 PROCEDURES

3.1 Phase One

3.1.1 Add a new VM port group to your ESXi servers representing a second enterprise location

Log into the student virtual cluster

1. Opened Firefox.
2. Entered *studentvc.cit.lcl* in the search bar.
3. Logged in with my student credentials.

Added new NIC

1. Found **ESXi1.2** in the sidebar
2. | Right click | Edit settings | Virtual Hardware | Add New Device | Network Adapter |
3. Selected the new network adapter.
4. | Browse | CNIT24210B | OK
5. Repeated these steps for **ESXi2.1**

Power cycle the ESXi servers

1. Launched web console for **CNIT24200.Group10.juergens.win10** from the sidebar
2. Opened Firefox.
3. Entered the ip address of **ESXi1.2**: *44.100.10.191*
4. Entered login information
5. Entered the ip address of **ESXi2.1**: *44.100.10.192*
6. Entered login information
7. In each ESXi servers respective tab went to | Virtual Machines | Checked checkbox next to Virtual machine | Power off
8. For each ESXi server clicked | Host | Reset | OK
9. In each ESXi servers respective tab went to | Virtual Machines | Checked checkbox next to Virtual machine | Power off

Configured ESXi servers network settings

1. Navigated back to **ESXi1.2**'s web interface
2. Clicked | Networking | Add standard virtual switch |
3. Named it *vSwitch2*
4. Clicked | ADD |
5. Clicked | Port groups | Add port group |
6. Named it *site2 Management*
7. Clicked | ADD |
8. Clicked | Port groups | Add port group |
9. Named it *site2 VM network*
10. Selected vSwitch2 from the Virtual switch drop down menu
11. Clicked | ADD |
12. Selected | Add VMkernal NIC | site2 | IPv4 only |
13. Entered *44.100.60.0* for the Address and *255.255.255.0* for the subnet mask
14. Clicked Create
15. Navigated to **ESXi2.1**'s web interface
16. Clicked | Networking | Add standard virtual switch |
17. Named it *vSwitch2*
18. Clicked | ADD |
19. Clicked | Port groups | Add port group |
20. Named it *site2 Management*
21. Clicked | ADD |
22. Clicked | Port groups | Add port group |
23. Named it *site2 VM network*
24. Selected vSwitch2 from the Virtual switch drop down menu
25. Clicked | ADD |
26. Selected | Add VMkernal NIC | site2 | IPv4 only |
27. Entered *44.100.60.0* for the Address and *255.255.255.0* for the subnet mask
28. Clicked Create

3.1.2 Deploy a new instance of your Windows Server VM template and implement it as a second domain controller at the new location

Deploy New instance of your Windows server template

1. Went to inner virt. enviornment

Created the Server 2019 VM from template

1. Inventory | Detestores | SANdatastoreG10 | VMs | VM templates |
2. right clicked **winServer 2019**
3. Selected new VM from this template
4. Entered *SCDCO2* for virtual machine name
5. | NEXT | 44.100.10.192 | Thin VM Storage Policy | datastore | NEXT | NEXT | FINISH

Navigated to ESXi2.1's IP address

1. Found the new server "SCDCO2"
2. Navigated through VM Hardware| Edit | Network Adapter 1 |Browse | site2 VM network | ok | ok |

Launched SCDCO2's web console

1. Logged in as Administrator

Configured IPv4 settings

1. Change IPv4 proporties:
   (a) IP: *44.100.60.10*
   (b) Subnet Mask: *255.255.255.0*
   (c) Default Gateway: *44.100.60.1*
   (d) DNS: *44.100.10.10*
2. Verified connectivity by pinging 44.100.10.10

Installed Active Directory Domain Services

1. Opened server manager
2. Navigated to | manage | Add roles and features | next | Role-based | Next |
3. Checked Active Directory Domain Services
4. | Next | Next | Next | Install |

Promoted the server to a domain controller

1. Clicked the flag icon
2. Clicked | Promote this server to a domain controller |
3. Selected Add a domain controller to an existing domain
4. Entered:
   (a) Domain: *group10.c242.cit.lcl*
   (b) Entered administrator credentials
5. Clicked | Next |
6. Entered DRSM password
7. Clicked | next | next | next | install |
8. Restarted **SCDCO2**

Defining a new site and Subnet

1. | Tools | Active directory Users and computers |
2. Right-clicked Sites
3. Selected new site
4. Named it site 2
5. Selected |Default|Psite link | OK|
6. Right-click Subnets
7. Selected New Subnet
8. Entered this for prefix: *44.100.60.0/24*
9. Navigated to | Default-First-Site-Name | Servers |
10. Right-clicked SCDCO2 | Move | site 2 | ok |

Transfter FSMO Role

1. Launched Active Directory Users and Computers from **SCDC02**
2. Right-clicked on the domain **group10.c242.cit.lcl**
3. Selected | Operation Masters | Infrastructure | Change | Yes |
4. Ensured the change was successful by running *netdom query fsmo* in the command prompt

3.1.3 Install a Windows 10 VM at the new location

Install a Windows 10 VM at the new location

1. went to the inner vCenter environment
2. Right-clicked **44.100.10.192**
3. New VM | Create a new virtual machine | Next |
4. Named it **site2win10**
5. | Next | Next | Thin storage policy | Next | Next |
6. Added 16 GB of Memory
7. Changed disk size to 35 GB, thin provision
8. Clicked | Next | finish |
9. Opened the web console
10. Accepted the defaults for the windows installer wizard

Configured IPv4 settings for Windows 10 VM

1. Change IPv4 proporties:
    - IP: *44.100.60.120*
    - Subnet Mask: *255.255.255.0*
    - Default Gateway: *44.100.60.1*
    - DNS: *44.100.60.10*
    - Secondary DNS: *44.100.10.10*

Install updates

1. Installed VMware tools
2. Went to settings
3. Selected | update | install | restart |

Join domain

1. Went to settings
2. Searched *domain* in the search bar
3. Entered *group10* in the domain box
4. Entered the administrator credentials

3.1.4 Implement Microsoft Backup

Install Vembu Backup

1. Navigated to the outer vCenter virtualization environment
2. Launched **CNIT24200.Group10.elsner.win10**
3. Downloaded **Vembu** from www.vembu.com
4. Opened the .exe file that was just downloaded
5. Accepted the defaults in the installer wizar.

Install Windows Server Backup

1. Opened **SCDC01** and **SCDC02** and performed the following steps on both
2. Opened **Server Manager**
3. Navigated to | Manage | Add Roles an Features | Next | Next | Next |
4. Checked **Windows Server Backup** and **Windows Server Migration Tools**
5. Completed the installer

Configure Backup

1. Opened BDR Suite web interface
2. Navigated to | Backup | Configure Backup | Windows | Files & Folders |
3. Added Block storage repository
4. Entered

   ```
   \MIDDLESCHOOLPC\TheBackup
   ```

5. Entered the administrator credentials
6. Selected | Create | Next | Confirm
7. Checked the local host to backup
8. Added the user files and domain controller database file locations
9. Configured the schedule to backup once every sunday morning at 2am

3.1.5 Printing

The printing task has not been completed.

3.1.6 Clone the Windows Server VM template and implement an IIS web server

Deploy New instance of your Windows server template

1. Went to inner virt. enviornment

Created the Server 2019 VM from template

1. Inventory | Detestores | SANdatastoreG10 | VMs | VM templates |
2. right clicked **winServer 2019**
3. Selected new VM from this template
4. Entered *IISserver* for virtual machine name
5. | NEXT | 44.100.10.191 | Thin VM Storage Policy | datastore | NEXT | NEXT | FINISH

Navigated to ESXi1.2's IP address

1. Found the newly created server in the sidebar
2. Navigated through VM Hardware| Edit | Network Adapter 1 | Browse | site2 VM network | ok | ok |

Launched IISserver's web console

1. Logged in as Administrator

Configured IPv4 settings

1. Change IPv4 proporties:
    - IP: *44.100.60.200*
    - Subnet Mask: *255.255.255.0*
    - Default Gateway: *44.100.60.1*
    - DNS: *44.100.10.10*
    - Secondary DNS: *44.100.60.10*

Changed server name and add to domain

1. Launced server manager
2. | Computer Name | Change |
3. Entered *IISserver* for computer name and *group10.c242.cit.lcl* for domain
4. Restarted to apply changes

Install IIS

1. Navigated to | Server Manager | Manage | Add roles and features | Role-based | Next | Next |
2. Checked "Web Server (IIS)"
3. Finished the installer by accepting the defaults for the remaining installer wizard
4. Navigated to | Tools | Internet Information Services (IIS) Manager

Create Public Web Page

1. Opened **Server Manager**
2. | Tools | Internet Information Services (IIS) Manager |
3. In **Connections** pane, expanded server node and clicked on **Sites**
4. Right-clicked **Sites** and selected **Add Website**
   - **Site name**: PublicSite
   - **Physical path**:

     `‘C:\inetpub\wwwroot\public‘`
   - **Binding**:
     - **Type**: HTTP
     - **IP address**: *44.100.10.200*
     - **Port**: 80
5. Clicked **OK** to create the website
6. Created the directory

   `‘C:\inetpub\wwwroot\public‘`

Create Private Web Page

1. Opened **Server Manager**
2. | Tools | Internet Information Services (IIS) Manager |
3. In **Connections** pane, expanded server node and clicked on **Sites**
4. Right-clicked **Sites** and selected **Add Website**
   - **Site name**: PrivateSite
   - **Physical path**:

     `‘C:\inetpub\wwwroot\private‘`
   - **Binding**:

- **Type**: HTTP
- **IP address**: *44.100.10.200*
- **Port**: 80

5. Clicked **OK** to create the website
6. Created the directory

   `'C:\inetpub\wwwroot\private'`

7. Restricted access to the private website:
   (a) Opened **IIS Manager**
   (b) Selected **PrivateSite**
   (c) Double-clicked **Authorization Rules**
   (d) Removed default **Allow** rule
   (e) Added new **Allow** rule for Administrators

Create Site-Specific Web Page

1. Opened **Server Manager**
2. | Tools | Internet Information Services (IIS) Manager |
3. In **Connections** pane, expanded server node and clicked on **Sites**
4. Right-clicked **Sites** and selected **Add Website**

   - **Site name**: site1
   - **Physical path**:

     `'C:\inetpub\wwwroot\site1'`

   - **Binding**:
   - **Type**: HTTP
   - **IP address**: *44.100.10.200*
   - **Port**: 80

5. Clicked **OK** to create the website
6. Created the directory

   `'C:\inetpub\wwwroot\vlan'`

7. Configured VLAN-specific access:
   (a) Opened **IIS Manager**

(b) Selected **VLANSite**

(c) Double-clicked **IP Address and Domain Restrictions**

(d) Added **Allow** entry for specific VLAN IP range (‘44.100.10.255/24‘)

Verify Websites

1. Opened a web browser on a client machine
2. Verified access to public site by navigating to *http://44.100.60.200*
3. Verified access to private site by navigating to *http://44.100.60.200/private* (authentication required)
4. Verified access to VLAN-specific site by navigating to *http://44.100.60.200/site1* (ensure client machine is in correct VLAN)

3.1.7 Implement DFS across your two domain controllers

Implement DFS across your two domain controllers

1. Went to inner virt. environment

Ensured DFS Role was Installed

1. Opened Server Manager on both domain controllers
2. Clicked on Manage and selected Add Roles and Features
3. Clicked Next until reaching the Select server roles page
4. Expanded File and Storage Services, then File and iSCSI Services
5. Checked both DFS Namespaces and DFS Replication
6. Clicked Next and Install. Repeated this step on both domain controllers

Created a DFS Namespace

1. Opened DFS Management from Server Manager under Tools
2. In the DFS Management console, right-clicked Namespaces and selected New Namespace
3. Specified one of the domain controllers to host the namespace in the New Namespace Wizard
4. Clicked Next, entered the namespace name

   `group10.c242.cit.lcl\dfs`

5. Chose Domain-based namespace and clicked Next

6. Confirmed and clicked Create

Added Folders to the Namespace

1. In the DFS Management console, expanded the new namespace
2. Right-clicked the namespace and selected New Folder
3. Entered the folder name
4. Clicked Add to specify the path to the shared folder on both domain controllers

Added Folder Targets

1. Right-clicked the folder in the namespace and selected Add Folder Target
2. Specified the path to the corresponding shared folder on both domain controllers
3. Clicked OK to add the folder target

Reconfigured Folder Redirection and Profiles

1. Opened Group Policy Management on one of the domain controllers
2. Edited the GPO that handles folder redirection
3. Navigated to User Configuration -> Policies -> Windows Settings -> Folder Redirection
4. Right-clicked on each folder to be redirected and selected Properties
5. Changed the target folder location to the DFS namespace path
6. Clicked OK to apply the changes

Updated User Profiles

1. Ensured user profiles referenced the DFS namespace by updating the profile paths in Active Directory Users and Computers
2. Opened Active Directory Users and Computers
3. Right-clicked a user and selected Properties
4. Went to the Profile tab
5. Changed the Home folder path to the DFS namespace
6. Applied the changes

Implemented DFS Replication

1. In the DFS Management console, right-clicked Replication and selected New Replication Group

2. Chose Multipurpose Replication Group and clicked Next
3. Specified a name for the replication group and added both domain controllers as members
4. Clicked Next and chose Full Mesh topology
5. Clicked Next to configure replication settings

Configured Replicated Folders

1. In the Replication Group Wizard, specified the folders to replicate
2. Specified the path to the folder on both domain controllers
3. Clicked Next and configured the replication schedule and bandwidth

Completed the Replication Configuration

1. Reviewed the settings and clicked Create to complete the replication group configuration
2. The replication group synchronized the specified folders between the domain controllers

Configured Client Access Based on Site

1. Opened Active Directory Sites and Services
2. Expanded the Sites container and created a new site for each physical location
3. Assigned the appropriate subnets to each site
4. Moved the domain controllers to their respective sites

Updated DFS Namespace Referral Settings

1. In the DFS Management console, right-clicked the namespace and selected Properties
2. Went to the Referrals tab
3. Checked the box for Clients fail back to preferred targets
4. Clicked Edit Settings for each folder target
5. Set the Target Priority to First among all targets for the local site and Last among all targets for remote sites

3.2 Phase Two

3.2.1 Clone the Windows Server VM template and implement a Windows Server Update Services (WSUS) instance

Clone the Windows Server VM Template Created the Server 2019 VM from template

1. Went to inner virt. environment
2. Inventory | Datastores | SANdatastoreG10 | VMs | VM templates
3. Right-clicked **winServer 2019**
4. Selected New VM from this template
5. Entered *WSUServer* for virtual machine name
6. | NEXT | 44.100.10.191 | Thin VM Storage Policy | datastore | NEXT | NEXT | FINISH

Added Second Virtual Hard Drive

1. Navigated to ESXi1.2's IP address
2. Found the newly created server in the sidebar
3. Navigated through VM Hardware | Edit | Add Hard Disk | New Standard Hard Disk
4. Entered 80 GB for disk size, selected Thin provision, and clicked OK

Configured IPv4 Settings

1. Launched WSUServer's web console
2. Logged in as Administrator
3. Changed IPv4 properties:
    - IP: *44.100.10.201*
    - Subnet Mask: *255.255.255.0*
    - Default Gateway: *44.100.10.1*
    - DNS: *44.100.10.10*
    - Secondary DNS: *44.100.60.10*

Changed Server Name and Added to Domain

1. Launched Server Manager
2. | Computer Name | Change |
3. Entered *WSUServer* for computer name and *group10.c242.cit.lcl* for domain

4. Restarted to apply changes

Install and Configure WSUS Installed WSUS Role

1. Opened Server Manager
2. Clicked on Manage and selected Add Roles and Features
3. Chose Role-based or feature-based installation and clicked Next
4. Selected the WSUS server from the server pool and clicked Next
5. Checked Windows Server Update Services and clicked Next
6. Clicked Next through the wizard until the Role Services page
7. Checked WID Database and WSUS Services, then clicked Next
8. Specified the path for the WSUS content folder on the new virtual hard drive W:
9. Clicked Next and Install

Completed WSUS Post-Installation Tasks

1. Opened Server Manager
2. Clicked the notification flag and selected Launch Post-Installation tasks
3. Waited for the tasks to complete

Configured WSUS

1. Opened Windows Server Update Services from Server Manager | Tools
2. Ran the WSUS Configuration Wizard
   (a) Selected Store updates locally and specified the path to the second hard drive W:
   (b) Selected to synchronize from another WSUS server and specified wsus.cit.lcl as the upstream server
   (c) Chose to synchronize manually and clicked Next
   (d) Selected products to synchronize: Windows 10, Windows Server 2019
   (e) Selected classifications to synchronize: Critical Updates, Security Updates, Definition Updates
   (f) Set synchronization schedule and clicked Next
   (g) Started the initial synchronization and completed the wizard

Approved Updates for Deployment

1. In WSUS console, expanded the server node and went to Updates

2. Selected the updates for Windows 10 and Windows Server 2019
3. Right-clicked the updates and selected Approve
4. Approved the updates for all computer groups

Configure Clients to Use WSUS via Group Policy Created a New GPO for WSUS

1. Opened Group Policy Management from Server Manager | Tools
2. Right-clicked the domain and selected Create a GPO in this domain, and Link it here
3. Named the GPO *WSUS Update Policy* and clicked OK

Configured WSUS Settings in GPO

1. Right-clicked the newly created GPO and selected Edit
2. Navigated to Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Update
3. Enabled the policy *Specify intranet Microsoft update service location*
   (a) Set the intranet update service URL to `http://wsuserver.group10.c242.cit.lcl:8530`
   (b) Set the intranet statistics server URL to `http://wsuserver.group10.c242.cit.lcl:8530`
4. Enabled the policy *Configure Automatic Updates*
   (a) Set the option to Auto download and schedule the install
   (b) Set the scheduled install day and time
5. Closed the Group Policy Management Editor

Verified Group Policy Application

1. On a client machine, ran ‘gpupdate /force‘ from an elevated command prompt
2. Checked Windows Update settings to ensure they pointed to the WSUS server

3.2.2 Use PowerShell Remote to list/stop/start services on a remote machine

Enable PowerShell Remoting on Remote Machine

1. Opened PowerShell as Administrator
2. Enabled PowerShell Remoting: *Enable-PSRemoting -Force*

Test PowerShell Remoting Connection from Domain Controller

1. Opened PowerShell as Administrator on the domain controller
2. Tested the connection to the remote machine: *Test-WsMan -ComputerName RemoteMachineName*

List Services on Remote Machine

1. Listed services on the remote machine: *Invoke-Command -ComputerName RemoteMachineName -ScriptBlock { Get-Service }*

Stop a Service on Remote Machine

1. Stopped a service on the remote machine: *Invoke-Command -ComputerName RemoteMachineName -ScriptBlock { Stop-Service -Name "ServiceName" -Force }*

Start a Service on Remote Machine

1. Started a service on the remote machine: *Invoke-Command -ComputerName RemoteMachineName -ScriptBlock { Start-Service -Name "ServiceName" }*

3.2.3 VMware Thinapp

Using a clean install of Windows 10, take a snapshot and install Thinapp. Run the Thinapp setup- capture and install Visio. Concluded setup-capture and save the package to a network location. Revert to the snapshot and run the package on the computer START Lab Procedure Documentation: **Install VMware ThinApp on Windows 10**

1. Opened **win10site2** machine
2. Downloaded VMware ThinApp from the rtfm.cit.lcl fileshare
3. Installed VMware ThinApp:
   (a) Double-clicked the installer
   (b) Accepted the defaults to complete the installation

Prepare for ThinApp Capture

1. Took a snapshot of **win10site2** machine:
   (a) Opened **VMware vSphere Client**
   (b) Right-clicked **win10site2**
   (c) Selected *Snapshot | Take Snapshot*
   (d) Named the snapshot *Pre-ThinApp Capture* and clicked *OK*

Run ThinApp Setup Capture

1. Opened **VMware ThinApp** on **win10site2**
2. Selected *Capture* in ThinApp Setup

3. Chose *Prescan* to create a baseline of the system
4. Installed Microsoft Visio 7:
   (a) Ran the Microsoft Visio 7 installer
   (b) Followed the prompts to complete the installation
5. After installation, returned to ThinApp Setup
6. Selected *Postscan* to capture changes made by the Visio installation
7. Entered application details:
   (a) **Application Name**: Microsoft Visio 7
   (b) **Project Location**: *C:7*
8. Clicked *Next* and then *Build Now* to create the ThinApp package

Save ThinApp Package to Network Location

1. Navigated to the project location *C:7*
2. Copied the ThinApp package to a network location

```
\network\SCDC01\Bullzip\Microsoft Visio 7
```

Revert to Pre-ThinApp Capture Snapshot

1. Opened **VMware vSphere Client**
2. Right-clicked **win10site2**
3. Selected *Snapshot* | *Revert to Snapshot*
4. Chose *Pre-ThinApp Capture* snapshot and clicked *OK*

Deploy ThinApp Package on Windows 10

1. Navigated to the network location

```
\network\SCDC01\Bullzip\Microsoft Visio 7
```

2. Ran the ThinApp package for Microsoft Visio 7 on **win10site2**
3. Verified that Microsoft Visio 7 was functioning correctly

4 RESULTS

In the lab, several crucial configurations and services were successfully implemented for the virtualized environment, spanning across two enterprise locations. The detailed results include a physical and logical network diagram, IP schema, computer names, and user login information.

4.1 Physical Network Diagram

4.2 Logical Network Diagram

4.3 Machine Networking/Login Information Table

table	**ESXi1.2 Server**	**ESXi2.1 Server**	**vCenter**
Pnic1 (CNIT242G10A)	44.100.10.191	44.100.10.192	44.100.10.170
Pnic2 (CNIT242iSCSI)	192.168.52.10	192.168.54.10	N/A
Pnic3 (CNIT242G10B)	44.100.60.10	44.100.60.10	N/A
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	44.100.10.1	44.100.10.1	44.100.10.1
DNS	44.100.10.10	44.100.10.10	44.100.10.10
Secondary DNS	44.100.60.10	44.100.60.10	44.100.60.10
SAN server IP	192.168.52.254	192.168.54.254	N/A
Login	root	root	administrator
Password	Cnit242!	Cnit242!	Cnit242!

table cont.	**Windows 2022 Srv.(SCDC01)**	**site2win10**	**Windows 11 VM**
Pnic1 (CNIT242G10A)	44.100.10.10	N/A	44.100.10.111
Pnic2 (CNIT242iSCSI)	N/A	N/A	N/A
Pnic3 (CNIT242G10B)	N/A	44.100.60.120	N/A
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	44.100.10.1	44.100.60.1	44.100.10.1
DNS	44.100.10.10	44.100.60.10	44.100.10.10
Secondary DNS	44.100.60.10	44.100.10.10	44.100.60.10
SAN server IP	N/A	N/A	N/A
Login	Administrator	Administrator	Administrator
Password	Cnit242!	Cnit242!	Cnit242!

table cont.	**Windows 2019 Srv.(SCDC02)**	**WSUSserver**	**IISserver**
Pnic1 (CNIT242G10A)	N/A	44.100.10.202	44.100.10.200
Pnic2 (CNIT242iSCSI)	N/A	N/A	N/A
Pnic3 (CNIT242G10B)	44.100.60.10	N/A	N/A
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	44.100.60.1	44.100.10.1	44.100.10.1
DNS	44.100.60.10	44.100.10.10	44.100.10.10
Secondary DNS	44.100.10.10	44.100.60.10	44.100.60.10
SAN server IP	N/A	N/A	N/A
Login	Administrator	Administrator	Administrator
Password	Cnit242!	Cnit242!	Cnit242!

4.4 User Login Information

- **Administrator** (Domain: group10.c242.cit.lcl)
  - Username: Administrator
  - Password: Cnit242!

4.5 Summary of Accomplishments

In Phase I of the project, several key objectives were successfully achieved. First, a new VM port group was added by configuring additional NICs on ESXi servers and setting up network settings specifically for site2. This effort resulted in the creation of a new port group and virtual switches dedicated to the second enterprise location. Second, a second domain controller was deployed through the implementation of a new instance of Windows Server VM. This deployment included defining the new subnet and site within Active Directory, along with the relocation of FSMO roles to ensure redundancy and resilience in domain operations.

Additionally, a Windows 10 VM was successfully installed and configured at the new location, seamlessly integrating it into the domain while verifying network connectivity. Microsoft Backup, utilizing Vembu, was set up for domain controllers, featuring scheduled weekly backups directed to a shared drive on a Windows 10 client. Moreover, an IIS web server was implemented following the cloning of a Windows Server VM template. This implementation included configuring public, private, and VLAN-specific web pages, each with appropriate access restrictions to manage information flow effectively within the enterprise network.

Furthermore, DFS was implemented across two domain controllers to facilitate home directory and desktop data replication. This initiative involved the creation of DFS namespaces and the configuration of replication mechanisms to ensure data consistency and accessibility across the enterprise.

Moving into Phase II, additional milestones were achieved. WSUS was implemented for efficient update management by cloning the Windows Server VM template and configuring clients to pull updates via Group Policy Objects (GPOs). PowerShell Remote Management was utilized to remotely manage services on designated machines, successfully executing tasks such as service listing, stopping, and starting with precision and efficiency.

Lastly, VMware Thinapp was employed to package and deploy Microsoft Visio 7 to physical machines across the network. This deployment strategy ensured seamless integration and usability of Visio 7, enhancing productivity and accessibility for users throughout the enterprise.

These accomplishments across both phases demonstrate effective planning, implementation, and management of critical IT infrastructure components to support organizational objectives and enhance operational efficiency.

5 CONCLUSIONS

In reflection upon the Yorkshire School System's IT infrastructure enhancement project, it is evident that all outlined objectives have been successfully achieved. This initiative was critical in fortifying disaster recovery capabilities, facilitating seamless integration across multiple locations, and optimizing IT resource management. The project encompassed several key components: the enhancement of network infrastructure with new segments and VLAN configurations, strengthening domain services through the deployment of a second domain controller and Active Directory optimizations, and improving client services with Windows 10 installations at new locations. Additionally, the implementation of Vembu Backup for scheduled domain controller backups, configuration of an IIS web server for diverse web page hosting, and deployment of DFS for data redundancy across domain controllers have significantly bolstered system resilience and accessibility. Centralized update management via WSUS and GPO configurations further streamlined software patching and fortified system security. In conclusion, by successfully meeting these objectives, the project has effectively fulfilled the requirements and expectations set forth in the business case, ensuring that the Yorkshire School System now operates with a robust, secure, and scalable IT infrastructure ready to support its expanding services and ensure continuity in operations.

6 RECOMMENDATIONS

1. **Keep Detailed Network Configuration Documentation:** Start by meticulously documenting the configuration details for new VM port groups and network settings on ESXi servers. Ensure clarity in naming conventions for port groups and adherence to the new site. Verify that all VMs in the new location are correctly addressed using the "Secondary IP Addresses" range to avoid network connectivity issues during setup and testing.

2. **Do Not Rush Deployment of IIS Web Server and Configuration:** Before deploying and configuring the IIS web server, ensure thorough planning and documentation of the setup process. Pay close attention to configuring public, private, and VLAN-specific web pages according to specified access levels. Verify that permissions are correctly set up to ensure seamless access for intended user groups while maintaining security protocols. Test each web page configuration on different clients to ensure that it is working over the network.

3. **Be Careful When Configuring DFS:** When implementing DFS across domain controllers and deploying WSUS, prioritize careful configuration and testing. Ensure DFS domain namespace implementation includes updating references to shares in profiles, folder redirection, and group policies to use the DFS namespace instead of specific server shares. Test DFS replication thoroughly to confirm data synchronization between domain controllers.

7 BIBLIOGRAPHY

About BDRSuite – HelpGuide. (2024).
https://www.bdrsuite.com/guide/vembu-bdr-suite/7-0/en/about-bdrsuite.html

Akpeokhai, O. (2024). Lab TA. Personal communication.
https://discord.com

Install ThinApp. (2024).
https://docs.vmware.com/en/VMware-ThinApp/5.2.4/com.vmware.thinapp.user/GUID-27B7EB2D-0F98-4BFB-9B11-DAB03B3A0ED1.html

Microsoft. (2022, August 16). Active Directory Domain Services Overview. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft. (2024). Windows 11 overview for administrators - What's new in Windows. Learn.microsoft.com.
https://learn.microsoft.com/en-us/windows/whats-new/windows-11-overview

Rawles, P. (2024). Lab Instructor. Instruction Video.
https://purdue.brightspace.com

Wong, O. (2024). Lab TA. Personal communication.
https://discord.com

8 APPENDIX A: PROBLEM SOLVING

8.1 Problem 1: DFS Namespace Configuration

Problem Description
During the implementation of DFS across domain controllers, accessing shares via the DFS namespace encountered intermittent connectivity issues, affecting user access to home directories and desktops. **Possible Solutions**

- Verify DNS Configuration: Check DNS settings to ensure proper resolution of DFS namespace addresses.
- Firewall Inspection: Review firewall rules on both domain controllers to allow DFS traffic between sites.
- DFS Replication Monitoring: Monitor DFS replication logs for any errors or delays in synchronization.

Solutions Attempted

- Verified DNS settings for DFS namespace resolution.
- Checked firewall rules but found no blocking issues initially.

Final Solution
Adjusted DNS server settings on client machines to prioritize local site domain controllers for DFS namespace resolution. This change ensured that clients accessed DFS shares from the nearest domain controller, resolving intermittent connectivity issues and improving access reliability across sites.

8.2 Problem 2: WSUS Client Update Failures

Problem Description
WSUS clients failed to receive updates from the WSUS server, despite correctly configured Group Policy Objects (GPOs) for update management. **Possible Solutions**

- GPO Refresh: Force a Group Policy update on client machines to ensure GPO settings are applied.
- WSUS Service Restart: Restart the WSUS service on the server to refresh update metadata.
- Client-side Troubleshooting: Manually initiate update checks on client machines to diagnose update download failures.

Solutions Attempted

- Forced GPO update on problem client machines using ‘gpupdate /force‘.
- Restarted WSUS service to refresh update metadata.

Final Solution
Identified that client machines had outdated Group Policy settings preventing them from reaching the WSUS server. Forced a Group Policy update using ‘gpupdate /force‘ on affected machines resolved the issue. Clients successfully started receiving updates from the WSUS server as intended.

8.3 Problem 3: Backup Target Access Issues

Problem Description
Scheduled backups using Vembu Backup failed due to access issues when targeting a Windows 10 client share as a backup destination. **Possible Solutions**

- Share Permissions Check: Review and adjust share permissions on the Windows 10 client share for backup access.
- Credentials Verification: Ensure correct credentials are used to authenticate backup jobs to the Windows 10 share.
- Vembu Backup Configuration Review: Double-check Vembu Backup settings to verify correct configuration of backup jobs and targets.

Solutions Attempted

- Verified share permissions and adjusted to allow backup access.
- Double-checked credentials used for backup jobs.

Final Solution
Discovered that the Windows 10 client’s firewall settings were blocking incoming backup connections. Updated firewall rules to allow inbound connections on the designated backup port resolved access issues. Subsequent backup jobs completed successfully, ensuring reliable data protection for domain controllers.