ENTERPRISE NETWORK MANAGEMENT

Final Project 2019

SCENARIO

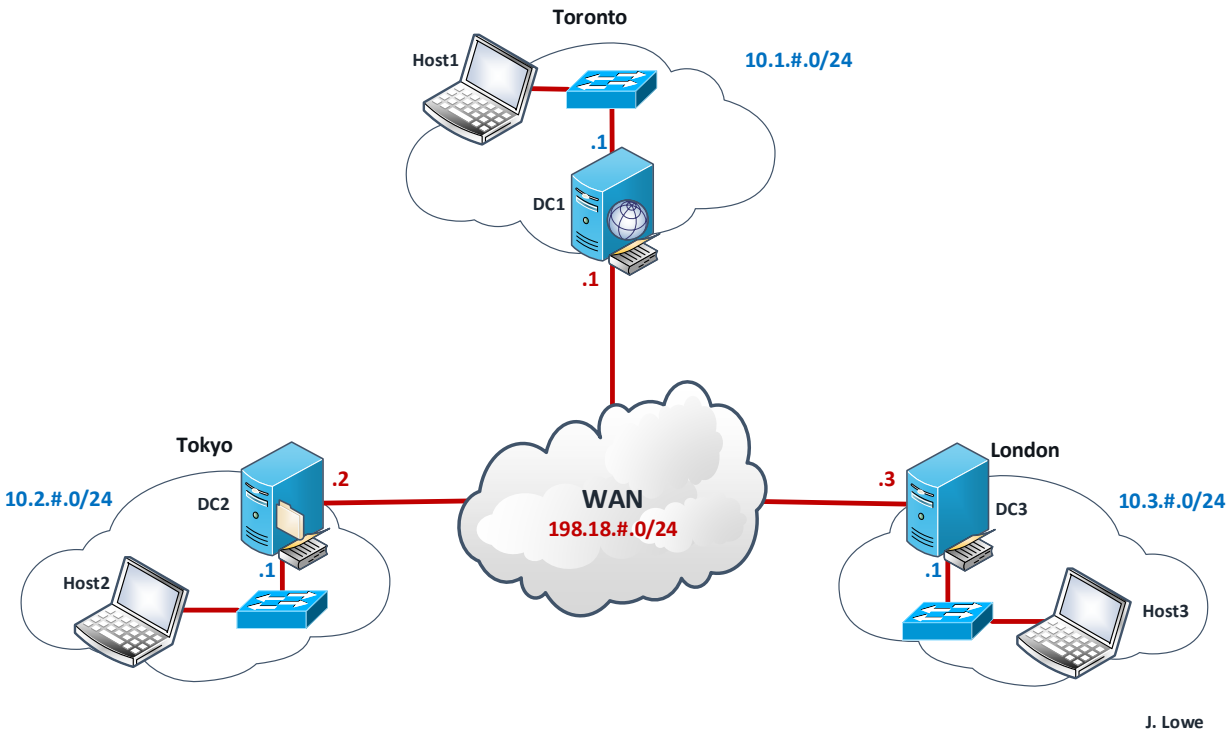
The International Travel Agency (ITA) is a multinational corporation that provides packaged travel services for small to medium enterprises (SMEs) around the world. Boasting thousands of customers and hundreds of employees, the ITA has an enterprise network spanning multiple geographical regions to deliver critical services required daily by their employees and customers.

The International Travel Agency has contracted your team to overhaul part of their current enterprise network. Using your expert knowledge, your team is responsible for deploying a unified Active Directory environment that can be used to control access to their network resources while providing various services, including.

- Configure Active Directory to provide centralization administration and access to resources
- Configure DHCP and DNS to provide addressing and name resolution services to end-user devices
- Configure file sharing services to provide a centralized repository for departmental files, providing enhanced security and backup capabilities
- Configure group policy to enable the ITA administrators the ability to standardize the network and security postures of devices in the network
- Configure various other features as required

TOPOLOGY

The ITA physical network topology is laid out as shown below:



TASKS

After meeting with the IT team at ITA, you have developed the following list of tasks that need to be completed in order to implement ITA's enterprise network.

IMPORTANT NOTES:

- **#** is your group number in all instances
- In all instances **x** = 1 for Toronto, **x** = 2 for Tokyo, **x** = 3 for London (for IPv6 addresses use 1111, 2222, 3333 in place of the **x**)
- Document all settings and passwords as you go. You will be required to submit these to Blackboard
- Complete tasks one at a time, on one server at a time, so you don't create conflicts
- Use the default values anytime you are not given specific values in the instructions below
- The default password on the hosts is **password**. You should change this to something more complex.
- You should take snapshots of your instances after each major configuration component

BASIC SERVER SETUP

Task 1. Create the three server instances using the details below:

- Instance Names: **DC1**, **DC2**, and **DC3**
- Source: **Windows Server 2016**
- Flavor: **Windows**
- Networks: **WAN** and either **Toronto** (DC1), **Tokyo** (DC2), or **London** (DC3)
  NOTE: Add only the **WAN** interface to each instance first, launch the console and rename the interface to "WAN", then return and add the LAN interface and name it **Toronto**, **Tokyo**, or **London** (this is VERY important for the initialization scripts to work properly)
- Security Groups: **None** (remove any that are added by default)

Task 2. Create the three host instances using the details below:

- Instance Names: **Host1**, **Host2**, and **Host3**
- Source: **Windows 10**
- Flavor: **Windows**
- Networks: Either **Toronto** (Host1), **Tokyo** (Host2), or **London** (Host3)
- Security Groups: **None** (remove any that are added by default)
- Name the interfaces of each host appropriately inside the VM (**Toronto**, **Tokyo**, or **London**)

Task 3. Configure the following static addresses:

- DC1, DC2, and DC3 WAN interfaces: **198.18.#.x/24** (uncheck IPv6 on the WAN interface). Use **127.0.0.1** as the DNS server on DC1 and **198.18.#.1** as the DNS server on DC2 and DC3
- DC1, DC2, and DC3 LAN interfaces: **10.x.#.1/24** and **2001:DB8:x:#::1/64** (**x** = 1111, 2222, 3333). Do not assign a DNS server to these LAN interfaces
- Do not assign default gateways to the WAN or LAN interfaces
- Once all other interfaces have been attached, attach the HRL interface to each VM. Rename the interface to **HRL** from within the VM. Each interface should receive a **172.17.x.x** address from the HRL. Make note of this address for each VM then do the following:
  - On each VM change the IPv4 settings of the HRL interface to **static** rather than DHCP
  - Statically set the IPv4 address of the HRL interface to match the DHCP address that was previously given to that VM. Set the subnet mask to **255.255.0.0** (/16)
  - Set the default gateway to **172.17.0.1**
  - Leave the DNS server fields empty

Task 4. Change the computer names according to the topology (**DC1**, **DC2**, **DC3**, **Host1**, **Host2**, and **Host3**) then restart the machines

NOTE: You should now be able connect to your devices remotely through the VPN (or the HRL Wi-Fi if you're in the lab). Using Remote Desktop and the static IP address you assigned to the HRL interface of each VM you can RDP into your VMs. This is much faster than the web console and will allow you to copy files from your computer to the VM. The default username is **user** for the hosts and **administrator** for the DCs.

IMPORTANT NOTE: At this point you must run the initialization scripts from Blackboard on each VM. Make sure they are run as administrator and that you run the correct script on the correct virtual machine (e.g. TorontoInitScript on DC1, TokyoInitScript on DC2, HostInitScript on each Host etc.). Ensure you have properly completed steps 1-4 before running the scripts. **You will likely need to run each of the DC scripts twice, rebooting the machines between executions. Follow any instructions that appear during script execution.**

ACTIVE DIRECTORY FOREST AND DOMAIN SETUP

Task 5. Install AD DS on all three DCs, one at a time starting with DC1, and promote them to domain controllers using the following information (use the defaults if not specified below)

- Create a new forest called **ita#.com** (**#** is your group number)
- Ensure that **DNS** and the **Global Catalog** roles are added to all three DCs
- DC3 (London) should be created as a **Read-Only Domain Controller (RODC)**
- When promoting DC2 and DC3 use the credentials for an administrator account in ita#.com
- You will need to manually create a delegation record in DNS for DC3's IPv4 and IPv6 addresses (and possibly DC2 if they don't exist)
    - Add an NS record and a blank A record (A record with no host name).
    - Ensure there is an existing A record with the dc3 hostname
    - Make sure there is an NS record for DC1 and DC2 as well (should happen automatically, but if they don't exist you must make them)

Task 6. Transfer the Infrastructure Master and Domain Naming Master roles from DC1 to DC2

DHCP

Task 7. Configure DHCP on all three servers, except where noted

- Install the DHCP role
- Authorize the DHCP server (Note: For the RODC, you may need to do this from a writeable DC)
- Configure and activate the following IPv4 DHCP scopes

    - Server: **DC1**
    - Name: **Toronto IPv4 Subnet**
    - Address Range: **10.1.#.1 to 10.1.#.254**
    - Subnet Mask: **255.255.255.0**
    - Lease Duration: **5 days**
    - Excluded Addresses: **.1 to .50**

    - Server: **DC2**
    - Name: **Tokyo IPv4 Subnet**
    - Address Range: **10.2.#.1 to 10.2.#.254**
    - Subnet Mask: **255.255.255.0**
    - Lease Duration: **5 days**
    - Excluded Addresses: **.1 to .50**

    - Server: **DC3**
    - Name: **London IPv4 Subnet**
    - Address Range: **10.3.#.1 to 10.3.#.254**
    - Subnet Mask: **255.255.255.0**
    - Lease Duration: **5 days**
    - Excluded Addresses: **.1 to .50**

- Configure and activate the following IPv6 DHCP scopes

    - Server: **DC1**
    - Name: **Toronto IPv6 Subnet**
    - Prefix: **2001:DB8:1111:#::/64**
    - Preferred Lifetime: **5 days**
    - Valid Lifetime: **7 days**
    - Excluded Addresses: **:1 to :50**

- Server: **DC2**
- Name: **Tokyo IPv6 Subnet**
- Prefix: **2001:DB8:2222:#::/64**
- Preferred Lifetime: **5 days**
- Valid Lifetime: **7 days**
- Excluded Addresses: **:1 to :50**

- Server: **DC3**
- Name: **London IPv6 Subnet**
- Prefix: **2001:DB8:3333:#::/64**
- Preferred Lifetime: **5 days**
- Valid Lifetime: **7 days**
- Excluded Addresses: **:1 to :50**

- Add IPv4 scope options:
  - 003 Router (default gateway) as **10.x.#.1**
  - 006 DNS Server as **198.18.#.x**
  - 015 DNS Domain Name as **ita#.com** (**#** is your group number)
- Add IPv6 scope options:
  - 00023 DNS Recursive Name Server IPv6 Address as **2001:DB8:x:#::1**
  - 00024 Domain Search List as **ita#.com** (**#** is your group number)
- Configure reservations on each server so that each host receives **.100** and **::100** from the DHCP server
  - Name the reservations after the hostname of the client (e.g. **Host1**)
  - You can get the DUID, IAID and MAC address of each host from the output of the **ipconfig /all** command
- Configure DC2 to be a failover DCHP server for the **Toronto IPv4 Subnet**
  - Name the relationship **Tokyo-Toronto-DHCP-Failover**
  - Set the mode to **Hot standby**
  - Reserve **10%** of the address space for the standby server
  - Enable message authentication with the shared secret **ITA$hared$ecret**
- Verify that hosts all receive appropriate IPv4 and IPv6 addresses and related settings

AD USERS, COMPUTER AND OUS

Task 8. Create the following OUs on DC1:

- Beneath the **ita#.com** domain, create the following OUs:
  - **Accounting**
  - **Marketing**
  - **Research**
  - **Sales**
  - **Support**
  - **Workstations**
- Within each OU (except Workstations) create the following OUs:
  - ***<OU Name>*Mangagers** (e.g. AccountingManagers, SalesManagers)
  - **Temp*<OU Name>*** (e.g. TempAccounting, TempSales)
- Prevent accidental deletion of all OUs that you create

Task 9. Manually create the following User Accounts on DC1:

First Name	Last Name	Job Role
Joan	Ark	Marketing Manager
Glen	Ross	Sales Manager
Jerry	Maguire	Marketing
Dorothy	Boyd	Marketing Temp
Jordan	Belfort	Sales Temp
Albert	Hawkins	Research Manager
Frederick	Banting	Researcher
Bob	Newhart	Accountant
Linus	Torvalds	Support Manager
John	Chambers	Tier 1 Support

- The user account name should be **First Name + Last Name** (e.g. Joan Ark)
- The logon names should be **First Initial + Last Name @ita#.com** (e.g. jark@ita50.com)
- The original password should be **Pa$$w0rd** (with a zero as the "O") and must be changed after first logon

Task 10. Place all user accounts in the departmental OU corresponding to the employee's department. For example:

- If an employee is not a manager or temp then they go in the root of the department OU
- The Marketing\MarketingManagers OU for the Marketing Manager
- The Sales OU for the Sales employee
- The Sales\TempSales OU for the Sales Temp employee
- The Support OU for the Tier 1 Support employee

Task 11. For the Temporary Sales employee:

- Limit the logon hours to allow logon only from **8am to 5pm Monday through Friday**
- The user account should expire on **December 31st of this year**
- In addition, disable the account for the temporary marketing employee

Task 12. Bulk import users into AD using the CSVDE tool and the CSV file given on Blackboard:

- The CSV will need to be modified to add the following fields with the correct format: **DN, objectClass, sAMAccountName, name, cn, givenName, sn, userPrincipalName, department**
- Use the account settings from above to fill in the required CSV fields
- The users should be imported into the correct OU based on their department in the CSV file
- After importing the accounts, enable them in AD Users and Computers (note that they will not have passwords set; this is fine)

Task 13. For all users in the Support OU (but not the SupportManagers OU), allow logon only to the **Support** computer (this machine doesn't exist yet but will be added later).

Task 14. Create the following global security groups in the ITA domain:

- Create a global security group named **Accounting** in Accounting OU
- Create a global security group named **Research** in the Research OU
- Create a global security group named **Sales** in the Sales OU
- Create a global security group named **Marketing** in the Marketing OU
- Create a global security group named **Support** in the Support OU
    - Add all user accounts in the corresponding OUs and sub-OUs as members of these newly-created groups

Task 15. Create the following domain local security groups in the ITA domain:

- Create a domain local security group called **Accounting Resources** in the Accounting OU
- Create a domain local security group called **Marketing Resources** in the Marketing OU
- Create a domain local security group called **Research Resources** in the Research OU
- Create a domain local security group called **Sales Resources** in the Sales OU
- Create a domain local security group called **Support Resources** in the Support OU
    - Add the **Accounting**, **Research**, **Sales**, **Marketing**, and **Support** global groups as members of their respective domain local groups (e.g. Support should be a member of Support Resources)

Task 16. Create a domain local security group called **Managers** in the Users container

- Add the following user accounts as members of the group:
    - **Joan Ark**
    - **Glen Ross**
    - **Albert Hawkins**
    - **Linus Torvalds**

Task 17. Create global security groups in the Users container for each of the administrative roles listed. Use the role name for the group name (no space):

- **PasswordAdmins** - able to reset user passwords and force password change at next logon for any user in the domain (apply at the domain level)
- **ComputerAdmins** - able to join computers to the domain for the entire domain (apply at the domain level)
- **GPOLinkAdmins** - able to manage GPO links for departmental OUs (apply at each of the specific OUs: Accounting, Marketing, Research, Sales, and Support)
- Use the **Delegation of Control Wizard** to delegate the necessary permissions at the correct level to each group. In the wizard, use the common tasks option for delegating control

HOST SETUP

Task 18. Join all three hosts to the **ita#.com** domain

Task 19. Move **Host1**, **Host2**, and **Host3** to the **Workstations** OU after they have been joined to the domain

Task 20. Pre-stage the following computer accounts in the Workstations OU

- **Sales1**, **Support**, **Accounting1** to **Accounting3**, **Research1** to **Research5**, and **Marketing2**

DNS

Task 21. Configure DNS on DC1, DC2, and DC3 to:

- Forward name resolution requests outside of the ITA domain to the ISP DNS servers at **203.0.113.100** and **203.0.113.101** (remove any existing forwarders)
- These addresses won't be resolvable (they don't exist)
- Use root hints for requests if the ISP DNS servers are unavailable

Task 22. Configure a reverse lookup zone:

- Create an IPv4 AD-integrated reverse lookup zone for subnets **198.18.#.0/24**
- Manually create A records and PTR records for the following hosts in ita#.com:
    - **ITAFiles01** - **198.18.#.2**
    - **ITAFiles02** - **198.18.#.3**
    - **ITAWeb** - **198.18.#.1**

Task 23. Configure a primary zone on the DC1 DNS server:

- Create the **ita#.private** zone on the DC1 DNS server (**#** is your group number)
- Configure the new zone to be stored in AD
- Replicate data with all DNS servers in the domain
- Allow only secure dynamic updates

Task 24. In the **ita#.private** zone, enable clients to connect to the web server (**ITAWeb**) using the following records:

- A blank **A** record pointing to **198.18.#.100** (this allows users to connect to the ITA web server using just the URL **ita#.private**)
- A **CNAME** record called **intranet**
- A **CNAME** record called **www**
- Point each CNAME to the **ITAWeb** host record in the **ita#.com** zone

FILE SHARING

Task 25. Create folders on DC2 (Tokyo) with the following NTFS permissions:

Folder	AD Group	NTFS Permission
C:\Departments\Accounting	Accounting Resources domain local	Allow Full Control
C:\Departments\Research	Research Resources domain local	Allow Full Control
C:\Departments\Sales	Sales Resources domain local	Allow Full Control
C:\Departments\Support	Support Resources domain local	Allow Full Control
C:\Departments\Marketing	Marketing Resources domain local	Allow Full Control

Task 26. Create a **C:\Personnel** folder on DC2 (Tokyo) with private employee information and set the following permissions:

- Share the folder as a hidden share called **HR$**
- Grant the **Managers** group the **Allow Full Control** sharing and NTFS permissions
- Remove all inherited NTFS permissions and share permissions from the folder after the Managers share and NTFS permissions have been configured

Task 27. Share the **C:\Departments** folder using the share name **Departments**.

- Use **Advanced Sharing**
- Set the share permissions to allow **Everyone** to have **Full Control** permissions

Task 28. Create the **C:\Archives** folder for storing old data. Configure the share and NTFS permissions for the folder as follows:

- Share C:\Archives using the share name **Vault**
- Configure share permissions to grant **Allow Full Control** to **Everyone**
- Give the **Research Resources** domain local group the **Full Control** NTFS permissions
- Give the **Support Resources** domain local group **Read & Execute** NTFS permissions
- Grant the **Administrators** group **Full Control** NTFS permissions
- Remove all inherited permissions for the folder

GROUP POLICY

Task 29. Create a GPO using a Starter GPO

- Enable the Administrative Templates central store by creating the Starter GPOs folder
- Create a starter GPO named **DNS Settings**
- Edit the starter GPO and configure the following settings (browse to Computer Configuration\Administrative Templates\Network\DNS Client)
  - **Primary DNS Suffix** = **ita#.com** (**#** is your group number)
  - **DNS Servers** = **198.18.#.1 198.18.#.2 198.18.#.3**
  - Enable **Dynamic Updates of DNS records**
  - Enable **registering of PTR records** and set it to **Register**
  - Turn off **multicast name registration**
- Create a new GPO named **TestGPO** using the new starter GPO you created. Do not link the GPO to any OUs
- Verify that the starter GPO settings were applied to the new GPO

Task 30. Edit the **default domain policy** and configure the account policy settings to meet the following requirements

- Passwords must be at least **9 characters long**
- Passwords must meet **complexity requirements** (uppercase letter, lowercase letter, number, and symbol characters)
- Users must change their passwords every **90 days**
- Users cannot change a new password for at least **14 days**
- Any new password must be different than the **previous 10 passwords**
- If **five** incorrect passwords are entered within a **10 minute** interval, lock the account
- Keep accounts locked for **60 minutes**, then unlock the account automatically

Task 31. Edit the **default domain policy** and configure an Audit Policy as follows:

- When a **logon** or **account logon** attempt is made (successful or not), record an event in the security log on each workstation. Remove all other auditing (Define the policies and uncheck success and failure)
- In Security Options, enable the **Audit: Shut down system immediately if unable to log security audits** policy
- In Event Log settings, enable the **Retention method for security log** policy and configure it to **Do not overwrite events (clear log manually)**

Task 32. Create a GPO called **Workstation Security** and configure the following options

- Prevent logon with the guest local user account by disabling the **Accounts: Guest account status** policy
- Change the local administrator username to **ENM2019** by enabling the **Accounts: Rename administrator account** policy
- Prevent hackers (shoulder surfers) from seeing valid usernames by enabling the **Interactive logon: Do not display last user name policy**
- Set a message for users logging in by setting the **Interactive logon: Message text for users attempting to log on** policy to "**You are connecting to the ITA internal network. Only authorized users may access resources on this network**"
- Set the title that will appear on this message by setting the **Interactive logon: Message title for users attempting to log on** policy to "**Warning: Authorized users only!**"
- Prevent unauthorized users from shutting down workstations by disabling the **Shutdown: Allow system to be shut down without having to log on** policy
- Link the GPO to the **Workstations** OU

Task 33. Grant administrator rights to all of the workstations in the domain (applied to the **Workstations** OU)

- Create a global security group called **Desktop Admins** in the Users container in AD DS
- Configure a restricted groups policy in the **Workstation Security** GPO object that adds the **Desktop Admins** group as members of the local **Administrators** group on all of the workstations

ADDITIONAL FEATURES

Task 34. Configure one of the following additional Windows Server features. You should take a snapshot of your instances before you implement the additional feature:

- WSUS (use Group Policy to make all hosts get their updates from the WSUS server)
- DFS (create additional shares on the other DCs and make them available centrally via DFS)
- WDS (Windows Deployment Services for image management; create an image with unattended installation and Sysprep)
- IIS (and set up a web site on DC1 available at **intranet.ita#.private**, **www.ita#.private**, and **ITAWeb.ita#.com** from any host)

VERIFICATION

Although not comprehensive, you can use the following steps to verify basic functionality of your enterprise network.

VERIFYING ACTIVE DIRECTORY

- Verify that all users and groups appear on all three domain controllers
- Verify that the groups contain the correct users, and are the correct type (global security, domain local security)
- Verify that the users were successfully imported using CSVDE and that they are not disabled
- Verify that the Workstations OU contains the three hosts, as well as the pre-staged computers
- Verify that you cannot created, delete, or modify users or groups on DC3 (the RODC) if the WAN interface is down

VERIFYING DHCP AND DNS

- Verify that all three hosts receive the correct IPv4 and IPv6 addresses (.100 and :100) and related settings
- Verify that the first 50 addresses are excluded from each range (both IPv4 and IPv6)
- Verify that the Toronto IPv4 Subnet is being replicated to DC2 as part of failover
- Use the **nslookup** tool to verify that hosts in all three LAN networks can resolve the names:
    - **ITAFiles01.ita#.com**
    - **ITAFiles02.ita#.com**
    - **ITAWeb.ita#.com**
    - **ita#.private**
    - **intranet.ita#.private**
    - **www.ita#.private**

VERIFYING FILE SHARING

- Verify that all hosts can connect to **\\DC2.ita#.com** and see/open the following shares:
    - Departments
    - Vault
- Verify that attempts to open the **c:\personnel** folder directly on DC2 give you an error that you do not have permission to access the folder (do not click the button that grants you permissions)

VERIFYING GROUP POLICY

- Try setting a password on one of the user accounts that doesn't meet the length or complexity requirements and verify that you receive an error
- Log in to one of the hosts and verify the following:
    - The logon screen should not display any previous usernames
    - You should receive a warning message about authorized users when you attempt to logon
    - Verify that the local administrator account has been automatically renamed to **ENM2019**
    - Verify that the **Desktop Admins** group has been made part of the local **Administrators** group on the hosts

DELIVERABILES

DEMONSTRATION

After you have completed the project, take snapshots of all six instances. Name them **ENMProject-Group#-<*hostname*>-Final** (hostname is DC1, DC2, DC3, Host1, Host2, or Host3). These instances will be used to mark the completion of the final project. All tasks will be verified by launching these snapshots of the instances.

You must submit your passwords and any other settings that will be needed to access your hosts and servers in order to grade them.

You also need to outline on Blackboard the details of the additional feature you implemented in Task 34. Be sure to include enough details that the TA can assess whether the feature was implemented correctly (e.g. which feature, which machines, how is it supposed to work?).

PRESENTATION

You will be required to give a 10-minute presentation according to the schedule that will be posted to Blackboard. Your presentation must include:

- A description of the additional feature that you deployed. You should answer the questions: what? why? where? and how?
- Describe how you would implement disaster recovery in your infrastructure. Include examples of how you would prepare for, and recover from, a failure of:
    - Active directory or the failure of one or more domain controllers
    - Any of the DNS or DHCP servers
    - The file share on DC2

You must include a PowerPoint presentation, and this presentation must be submitted to Blackboard by the due date indicated.