**Group 3**

**10/05/2017**

**IT 310 – 41**

**Assignment 2**

**Group3\_Assign2.docx**

**Case Project 3-1:**

Server Manager is an incredibly convenient and powerful tool that consolidates administrative functions that makes a server easier to manage. This is key for beginner and intermediate administrators, as incorrect configurations can be avoided when using the intuitive step-by-step wizard processes. Capabilities of Server Manager are as follows:

* + Configure a server from the beginning.
  + View computer configuration information.
  + Change server roles and system properties.
  + Configure networking.
  + Configure remote desktop.
  + Configure security, including the firewall.
  + Configure a multitude of server roles, from a basic file server to advanced network services.
  + Add or remove features.
  + Run diagnostics.
  + Manage storage and backups.
  + Manage multiple servers from one place.

New features for Server Manager in Windows Server 2016:

* + The local server option – Makes all local server properties available to manage.
  + Multiple servers are easier to manage form one place.
  + Grouping of servers – Allows all servers in a specific group to receive commands simultaneously.
  + A more robust Dashboard – More quick-start guidance for setting up one or more servers and establishing groupings used to manage specific kinds of severs.
  + New Server Manager GUI – Added features, such as greater ability in adding and managing remote servers.

How to start Server Manager:

Click on the “Start” icon and click Server Manager tile. Another option is to click Server Manager under the “S” application listings.

How to install roles and features to a server:

* + Step 1. Ensure Server Manager is open.
  + Step 2. Ensure Dashboard is selected in the left pane.
  + Step 3. In the right pane, click **Add roles and features** under the Welcome to Server Manager.
  + Step 4. If you see the Before you begin window in the Add Roles and Features Wizard, Click **Next**.
  + Step 5. Make sure that Role-based or feature-based installation is selected in the Select installation type window. Type Next.
  + Step 6. Ensure your computer is selected in the Server Pool box in the Select destination server window and click Next.
  + Step 7. In the Select server roles window, check the box for whatever role is to be installed. If a dialog box is available, click **Add Features**.
  + Step 8. Click Next in the Select server roles window.
  + Step 9. Click Next in the Select features window.
  + Step 10. In the Select role services window, make sure the role required is selected, and click Next.
  + Step 11. Click install in the Confirm installation selections widow.
  + Step 12. Wait a few moments as the role is installed.
  + Step 13. When the installation progress window shows that the installation succeeded, click Close.

**Case Project 3-5:**

Light Crafters will need to run the Best Practices Analyzer, or BPA, to ensure their currently installed roles are up to Microsoft recommended guidelines. This will generally ensure sound implantation when the company begins live operations. The BPA is initiated through Server Manager and the steps to start the program are as follows:

* + - Step 1. Open Server Manager.
    - Step 2. Click on a Local Server in the left pane (The sever that requires compliance).
    - Step 3. In the right pane, scroll to Best Practices Analyzer.
    - Step 4. Click the down arrow for TASKS.
    - Step 5. Click start BPA Scan and wait for the scan to complete.
    - Step 6. Read the results shown for the scan. Servers with multiple roles will can each role listed. Click on the role to see the results of each role.

After the scan, if problems are found, the reports will be categorized by three levels of severity:

* Information – Indicated the role is in compliance, but a change is recommended.
* Warning – The role complies under current operating conditions, but this may change if the operating conditions change.
* Error – The role does not meet best practices and problems should be expected.

**Case Project 4-4:**

In order to fix the issue of outdated data and extra paperwork in the Outlet Stores, I would recommend that each store be setup into sites. Each store site can be organized into geographical locations, and be fined tuned for individual needs by organizational units (OU’s). The use of sites through Active Directory uses the TCP/IP (container) concept of communication, effectively fixing the issue of network connectivity. To ensure up-to-date data transfers and server updates between the stores and home complex, the use of a bridgehead domain controller is required. A bridgehead server will replicate data form the home complex writable DC to the sites RODC’s (explained below).

In terms of ensuring security at each outlet site, RODC servers provide a stable means without the need of administration personnel. DODC’s provide protection from unauthorized network intrusions (due to the RO nature of the server), limited cache of data (protects company wide data, limited to only the hardware stolen). Expanding on the possibility of theft, RODC’s can utilize Bitlocker Drive Encryption. In the event that the server is stolen, data is encrypted and protected data deleted, preventing thieve from getting valuable data. Finally, the RODC acts as a key distribution center, allowing only authorized users to access the system. This is done by requesting a user credential check with the DC and saving it to the cache.

In short, the use of sites within Active Directory and the installation of a bridgehead server can solve the issues the Outlet Stores are experiencing; Using Active Directory for management efficiency and site implantation/organization and using a bridgehead to replicate server information from the home complex DC (Datacenter) to the RODC’s in each site, cutting down on old data and redundant paperwork.

Recommend upgrades:

10 RODC servers (One per site)

2 Writeable Domain controllers. 1 in the home complex and 1 in a separate location for data redundancy and prevention of “single point failure” scenarios. (Note: if the secondary backup DC is located in a store site, harden with typical physical security options)

2 bridgehead severs (1 for each datacenter) to replicate data between the two datacenters and the site RODC’s.