**MODULE 8: PORTFOLIO PROJECT**

Deploy and Administer Windows Server 2012

Ismail Elmaliki

ITS 405 – Intermediate Networking

Colorado State University – Global Campus

Professor Raquel Hicks

June 9, 2018

Introduction

As an IT consultant leading the charge for Worldwide Advertising Incorporated, I’ll be able to implement lasting tech solutions that are tailored to company needs (both short-term and long-term). As summarized by your CIO, she was able to provide me with the following information:

* *Employee Structure* – the total number of employees as well as number that are in each department such as Executives, Accounts, Sales, HR, and other departments mentioned.
* *Two Sites* – One main location in Los Angeles and one in New York.
* *Networking* – with networking already setup in both locations, they need a secure VPN tunnel for secure inter-site traffic.
* *File Access and Sharing –* departments within the company need to be able to share information while remaining private from other departments as needed.

Based on those points listed out by your CIO, here are some technical points that I’ll be focusing on then will be covering in-depth on why they’ll be the most appropriate solution for your organizational needs:

* Deployment and Server Editions
* Domain Name Service (DNS)
* Active Directory and OU
* Group Policies
* Virtual Private Network
* File Sharing and Permissions

**Deployment and Server Editions**

Before virtual and cloud computing, IT administrators always had to order physical servers at least weeks in advance, then physically setup and install all necessary software. Fast forwarding to today, there are many approaches IT can take today – have in-house servers that run virtualization (which will lead to less demand of ordering additional hardware), rely on cloud computing services entirely like Amazon’s AWS and Microsoft’s Azure, or have a hybrid environment of both in-house servers and utilizing cloud computing. Referring to a blog from Milner’s website titled The Advantages and Disadvantages of Virtualization (2015), the advantages of virtualization include: reduced spending, easier backup and disaster recovery, better business continuity, and more efficient IT operations; some disadvantages include upfront costs for virtualization software, software licensing considerations, and a possible learning curve. The disadvantages however can easily be overcome with careful preparation and utilizing excellent project management skills; on the other hand, if a company fails to take appropriate steps before adopting newer technology, then virtualization can be a drawback.

With that being said, Azure – Microsoft’s Cloud Based Solution – would be the best way to go and will work well in conjunction with Microsoft Server 2012. By choosing a cloud-based solution, this will account for business future necessities and include the following features that physical servers don’t offer:

* *Scalability* - the ability to increase in size easily; for example, if an additional server is required based on demand, this can be done within just a few minutes with cloud computing. Whereas without cloud computing, IT would need to figure out the exact specs they would need, then order the server which doesn’t arrive until a week or so. From there, IT would have to configure that server which can take hours.
* *Elasticity* - this is referred to as the ability to scale up or scale down resources. For example, let’s say we currently have 5 web servers running - what if after a year turns out only 2 is required? Without cloud computing, there would just be 3 additional servers collecting dust and would be considered a wasted asset. However, with cloud computing servers can easily be scaled up or scaled down - again, all within a few minutes.
* *Fault tolerance* - with cloud computing, this is a given and doesn’t require much worries for IT.
* *Highly Available* - it’s extremely rare for cloud computing services to fail; they’re highly available in service and continue operating.
* *Included Security Standards* – Microsoft Azure by default has DDoS protection and will allow IT employees moving forward to fine-tune what’s allowed to come in and out using port security rules.

Bringing it all together, cloud-computing’s flexibility with scaling and elasticity allows any business to scale up or down its resources easily while saving time and money for IT staff so they can focus on growing the company by implementing up-to-date tech solutions that empower staff members at WAI.

**DNS**

In an article published by Microsoft titled DNS Namespace Planning (2018), it provides wonderful insight on things to consider when designing a DNS namespace for enterprise environments. First, it's important to identify the DNS namespace that'll be used for the company and register it for use on the internet by utilizing sites like networksolutions.com to ensure the registered name that's created is unique. Second, distinguishing between internal and external namespaces - for example, **wa-inc.com** can be the external address for Worldwide Advertising Incorporated while the internal can be a subdomain like **corp.wa-inc.com**. For internal addresses within different regions, using different subdomain names like **la.corp.wa-inc.com** for Los Angeles and **ny.corp.wa-inc.com** for New York. Lastly, I’ll make sure that root servers aren't created unintentionally. If the "." zone exists, that means a root server has been created and it's ideal to remove that for proper name resolution to work.

As a certified cloud architect and having experience in setting up DNS for previous companies, I’m aware that preventing mistakes along this process will prevent issues moving forward for IT staff as the company expands. In an article titled 9 Windows DNS mistakes to avoid (2016) by Casper Manes, some things that can arise from DNS mistakes include DNS servers being too far away from clients, having that DNS server point to itself at first and not changing that as more DNS servers are added, and allowing zone transfers externally but not allowing them internally. With that said, having an understanding of common mistakes made in corporate will ensure they’re prevented altogether when setting up WAI’s DNS.

**Active Directory**

Now that DNS is covered, that knowledge can be applied with setting up Active Directory tailored to WAI’s requirements. To start things off, let’s go back to those DNS examples while adding structure to them.

As we see, the domain with the highest hierarchy is **wa-inc.com**, which is publicly accessible. Underneath **wa-inc.com** are its child domains - **wa-inc.com/about** and **corp.wa-inc.com**. The about page is publicly available to the world so customers can understand what Worldwide Advertising is about and what services can it offer to potential clients. On the other side is **corp.wa-inc.com**, which is only accessible to employees and focuses on the company internal structure. From there, the corporate domain also has child domains and is branched out by location – both Los Angeles and New York respectively.

From here, we can now go deeper into the Active Directory structure by setting up organizational units (OUs) as required. Based on the current employee structure, we know the following numbers of each department are as follows:

* *Executives –* 10
* *Accounts and Sales –* 150
* *Creative, Media, and Production –* 100
* *Human Resources and Finances –* 30
* *IT -* 10

We also know that most staff members will be located in Los Angeles, but at least one of each staff member will be located in New York. Now that we have the facts gathered, here’s how the employee organizational units will be structured as shown below:

* corp.wa-inc.com
  + la.corp.wa-inc.com
    - Accounting
    - Creative
    - Executive
    - Finances
    - HR
    - IT
    - Media
    - Production
    - Sales
  + ny.corp.wa-inc.com
    - Accounting
    - Creative
    - Executive
    - Finances
    - HR
    - IT
    - Media
    - Production
    - Sales

By having a solid OU Structure in Active Directory, it’ll help with allocating proper network resources and provide a solid foundation for the IT team to rely on.

**Group Policies**

According to Brad Rudisail’s article titled 5 Things You Didn’t Know about Group Policy and Active Directory (2016) via techopedia, we can think of Group Policy as a way of delivering configuration settings such as: security settings (password and lockout policies), correct display settings for the designated machines, methods in which Windows Updates are delivered, and power management settings for portable devices. The purpose of Group Policy is to provide an IT administrator with leverage to manage both users and devices within the network and ensure app settings remain in compliance – like preventing users from accessing command prompt and the registry editor (powerful tools that only admins should have access to).

As far as Group Policy best practices, Robert Allen wrote a great article on that titled Group Policy Best Practices (2016) via Active Directory Pro. In his article he highlights the following: 1) Don’t modify the Default Domain Policy since it applies to all users and computers and additional settings should be placed into a separate GPO; 2) Don’t modify the Default Domain Controller Policy – again, any other settings to the Domain Controllers should be set in a separate GPO; 3) Good OU Structure Will Make Group Policy Deployment much easier – make sure to have a solid OU structure that makes sense so proper group policies can be applied to both OUs and corresponding sub-OUs; 4) Use small GPOs to simplify administration – there isn’t a one size fits all GPO and attempting to do this will lead to misfortune down the road as an IT administrator. It’s always better to break out GPO policies with corresponding settings (for example, having separate GPO policies for Browser Settings, Security Settings, Power Settings, etc.). Bringing it all together, because of creating solid Active Directory OU structures from the last section we can deploy proper group policies in an organized fashion.

**Virtual Private Network**

We often hear the word VPN being thrown around casually, so it’s important to take a step back and explain it before jumping into VPN configuration. As summarized by an article from PC Magazine titled What Is a VPN, and Why You Need One (2018), a virtual private network creates a virtual encrypted tunnel between you and a remote server operating by a VPN service. As a result, all data is routed through a VPN tunnel to secure the data from malicious users while masking your identity. So how does it apply to corporate network environments and why is it important? If employees are to work remotely by using open networks, the last thing we’d want is for malicious users taking advantage of those open networks and stealing valuable information that’s relevant to the company! We’d want employees to securely connect to our network in the office using a VPN while making sure both the New York and Los Angeles offices are interconnected through a VPN as well.

With that said, a VPN can be configured using Windows Server 2012. According to an article titled Configure VPN in Windows Server 2012 (2016) via TechGenix by Richard Hicks, configuring a VPN starts with installing the VPN role via PowerShell, configuring remote access via the Routing and Remote Access console, configuring DHCP relay agent via that same console, then granting remote access to groups in our Active Directory structure. This will ensure that only authorized users can connect to the VPN and it’s that simple! Of course, it’s also a must to make sure that client devices can actually connect to the VPN server and enter appropriate domain credentials.

**File Sharing and Permissions**

Colleagues will often need to collaborate effectively with one another via file sharing to access necessary information from one place rather than storing duplicates on their computer. Again, Windows Server 2012 has the solution to this as highlighted via Scott Lowe’s article titled How to share a folder in Windows Server 2012 from TechRepublic: it’s as simple as going to Server Manager – File and Storage Services – Shares – then from the Tasks menu, clicking the New Share option. From there, there’ll be multiple settings available to fine-tune shared folders with regard to which department can have access, setting specifics like read/read-write/deny access, setting storage limits, the ability to cache data, and going deeper into file permissions.

It’s also important to understand some differences between NTFS disk quotas and FSRM quotas as highlighted from the blog post 2003 FSRM and NTFS Quotas compared (2009) via Wayne’s World of IT:

* FSRM provides per-folder quotas whereas NTFA provides per-user/volume quotas
* FSRM quotas count only the size on disk of files, whereas NTFS quotas count logical uncompressed files
* FSRM provides improved reporting and alerting for quotas, whereas NTFS quotas only provide rudimentary reporting and event-log entry alerting
* FSRM has no supported automation interface to manage quotas, whereas NTFS quotas can be managed by WMI
* FSRM provides very strong support for command-line administration with dirquota.exe, with NTFS quotas having limited support available through fsutil
* FSRM quotas provide improved notification – including in-built email, event logging, running a command or triggering a report

As far as when to use one over another, FSRM from a system administrator’s standpoint is the way to go when setting general restrictions to all accounts on a domain – for example, setting a limit of 1GB being stored to the Desktop. Referencing an article from RootUsers titled Configure Quotas with File Server Resource Manager (2017), if that 1GB limit is reached, then: a) an email message can be sent to administrators and the affected users, b) an event can be sent to the event log, and c) a command/script can be executed to automatically compress, move, or delete old or larger files automatically (if the threshold is reached for example). From a high-level standpoint, FSRM has the advantage over NTFS disk quotas. On the other hand, if there’s a shared network on the drive that needs to be fine-tuned with specific quotas that are specific to users, then NTFS disk quotas has the advantage of setting those specific limits to specific users. But from a System Administrator standpoint there isn’t much monitoring when it comes to it. Hence both of these features can be used by IT staff to set quotas to users within domains as needed.

**Conclusion**

Bringing everything together here, we were able to clearly define solutions for server deployment and preferred OS, properly structuring DNS and Active Directory OUs, deploying group policies and how a good DNS and Active Directory OUs play an important role, setting up a VPN so users can connect to the corporate network resources securely while authenticating with their credentials, and file sharing/permissions so employees are empowered to collaborate with one another while setting the right permissions based on department access.

References

DNS Namespace Planning. (2018, April 18). Retrieved June 10, 2018, from Microsoft website:

https://support.microsoft.com/en-us/help/254680/dns-namespace-planning

Eddy, M. (2018, February 21). What Is a VPN, and Why You Need One. Retrieved June 10,

2018, from PC Magazine website: https://www.pcmag.com/article/352757/you-need-a-vpn-and-heres-why

Hicks, R. (n.d.). Configure VPN in Windows Server 2012 R2. Retrieved June 10, 2018, from

TechGenix website: http://techgenix.com/configure-vpn-windows-server-2012-r2/

Jarrod. (2017, March 13). Configure Quotas with File Server Resource Manager (FSRM).

Retrieved June 10, 2018, from RootUsers website: https://www.rootusers.com/

configure-quotas-with-file-server-resource-manager-fsrm/

Logan, K. (2015, July 14). The Advantages and Disadvantages of Virtualization.

Retrieved June 10, 2018, from Milner website: http://milner.com/company/blog/technology/2015/07/14/the-advantages-and-disadvantages-of-virtualization

Lowe, S. (2012, October 11). How to share a folder in Windows Server 2012. Retrieved June 10,

2018, from TechRepublic website: https://www.techrepublic.com/blog/data-center/how-to-share-a-folder-in-windows-server-2012/

Manes, C. (2016, October 10). 9 Windows DNS Mistakes to Avoid. Retrieved June 10, 2018,

from TechGenix website: http://techgenix.com/windows-dns-mistakes/

Martin, W. (2009, February 9). 2003 FSRM and NTFS Quotas compared. Retrieved June 10,

2018, from Wayne's World of IT website: http://waynes-world-it.blogspot.com/2009/02/2003-fsrm-and-ntfs-quotas-compared.html