**MODULE 8: PORTFOLIO PROJECT**

IT Proposal for Kris Corporation

Ismail Elmaliki

ITS 430 – Network Enterprise Solutions

Colorado State University – Global Campus

Stuart Gold

August 5, 2018

Introduction

As an IT consultant with tremendous experience, one of my major responsibilities is identifying areas of concern with company IT infrastructure then applying long-term technological solutions – that way employees at the workplace are able to be at their productive best with minimal technological disruptions. By applying long-term and well-thought-out technological solutions, Kris Corporation and its employees can focus on what they do best – manufacturing parts for the automotive industry while staying ahead of the competition because of their technology. Through multiple meetings with company executives, the following are major IT concerns within the company:

* *Running multiple domains while using a single identity.*
* *With locations in five major cities nationwide – having consistent IT solutions with some form of centralization rather than having five completely separate servers.*
* *Running out of physical space for servers.*
* *With all sites independently connected to the Internet, file sharing across locations has become a challenge.*

Now that the major challenges have been listed out, below are features of Windows Server 2012 to address those concerns. Further details will be outlined on each of these topics as well as how they’ll resolve those major IT concerns:

* *Active Directory and Windows Server 2012*
* *DNS*
* *DHCP*
* *Hyper-V*
* *File Sharing*

**Active Directory in Windows Server 2012**

At the moment, Kris Corporation is running Windows Server 2008 – although it currently gets the job done, it’s critical to consider upgrading to Windows Server 2012. By upgrading to a more current OS, the company will be able to utilize new features that can address many of the current IT challenges existing today. One major reason why upgrading to Windows Server 2012 should be strongly considered is because of new features added to Active Directory. According to Shields (2012), Active Directory in Server 2012 includes many features that are worth upgrading to. Some of those features include:

* **GUI for Recycle Bin** - Recycling bin for Active Directory now has a GUI whereas in 2008 it was only accessible via PowerShell.
* **UI for Fine-Grained Password Policies** - This also includes in GUI in Active Directory 2012 and makes fine tuning password policies easier to apply and deploy.
* **Windows PowerShell History Viewer** - Being able to see Windows PowerShell commands corresponding to actions performed in the Active Directory UI; this makes it easy to reference those commands and allows IT administrators to automate repetitive as a result!
* **Windows PowerShell Cmdlets for Active Directory Replication and Topology** - having more commands for PowerShell for active directory replication and topology means more automation for repetitive tasks and that System Administrators can work efficiently.
* **Virtual Snapshot and Cloning Support** - Now Active Directory and hypervisor snapshots can mix (if your hypervisor supports VM Generation ID).

There are even more features included with Active Directory in Windows Server 2012 and many of those features can be utilized by IT staff members in their day-to-day for easier administrations tasks. Before making the transition to Windows Server 2012, it’s important that current IT staff regularly backup and have a full-system snapshot of the current Windows Server 2008 platform. From there, choosing the right Windows Server 2012 edition as highlighted by Desai (2013); because Kris Corporation is a large organization in this case, upgrading to Windows Server 2012 Datacenter Edition meets the current need of the organization today and as the company grows moving forward. As far as when to perform the upgrade to Server 2012, it’s important to have best practices in place; as Rosato (2018) highlights at a high level: using a change control process, reading all related documentation, applying updates on a need only basis, testing on a non-production server, and having a working backup for possible downtime. With backups, there are two approaches (and both can be used for extra assurance!): local and cloud. Plett (2016) highlights common local backup tasks that are possible with Windows Server and choosing the right backup type. Also setting up a backup schedule and making sure that storage drives are at least 2.5 times the storage capacity of data that requires a backup. Another way of keeping data safe is through a cloud-based backup service from Microsoft, which support virtual machine as well as physical Windows Servers. Referencing Backup Pricing (2018), Microsoft highlights the monthly cost of using their Azure backup service based on storage amount. Both are wonderful backup solutions and should be considered!

Another feature of Active Directory that will benefit Kris Corporation is Active Directory Federation Services (AD FS). As Mathers (2017) explains, AD FS is an identity access solution to provide employees with seamless SSO (Single-Sign On) access to protected Internet apps or services. Specifically, with Windows Server 2012 R2 as highlighted by Mathers (2017), AD FS can help with managing risk using multi-factor access control, controlling policies to require multi-factor authentication for all apps or specific apps, and providing authentication and authorization capabilities for accessing external sites that are protected by the Web App Proxy. There are endless benefits to AD FS, with ease of administration and controlling login centrally from Active Directory rather than managing 12 different apps that’ll require separate username and passwords.

**DNS**

Now that Active Directory new features, upgrading to Windows Server 2012, and backing up have all been covered, it’s important to analyze the current domain model of Kris Corporation then review an accurate solution that’s best for the company and its IT infrastructure moving forward. Because the company has multiple geographic locations and needs interconnectivity with other sites, a regional domain model is the right option. Mathers (2017) points out that deploying regional domains reduces replication traffic over WAN links versus the single model approach which replicates to all domain controllers within the current corp.kris.local domain. Here’s an example below to highlight an ideal domain structure based geographical location:

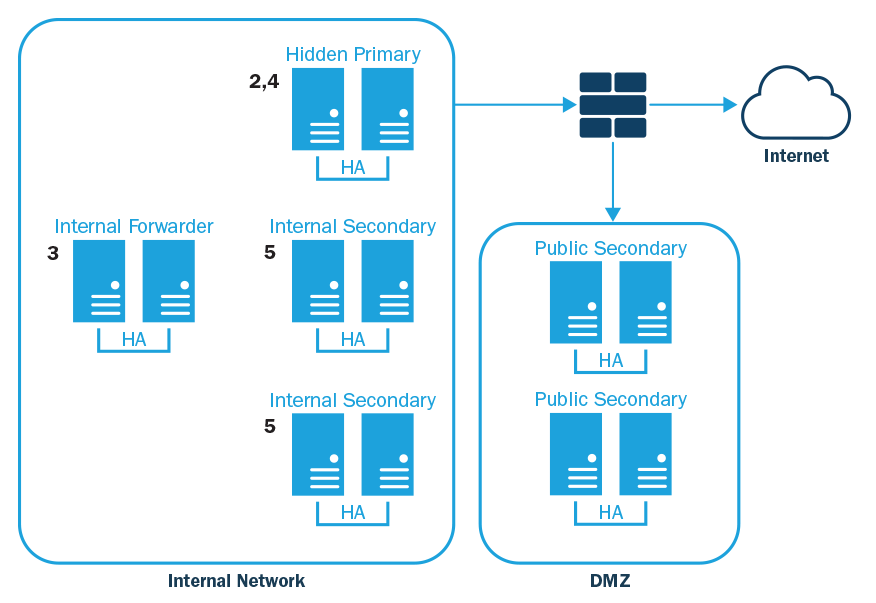
* Kris.local
  + Corp.kris.local
    - Atlanta.corp.kris.local
    - Baltimore.corp.kris.local
    - Chicago.corp.kris.local
    - Seattle.corp.kris.local
    - Sandiego.corp.kris.local

This type of hierarchy will lead to ease of administration, IT staff knowing which user is associated to which domain, and easily deploying group policies to either the entire domain or specific locations!

With regard to DNS Configuration with Active Directory, it’s important to list best practices. Referencing Best Practices for DNS Configuration in an Active Directory Domain (2018), there should be a certain number of DNS controllers based on location and the number of employees working at that particular location. For example, within a small environment at least one domain controller should be a DNS server, whereas in a larger environment “at least two domain controllers at each physical site should be DNS servers”. Applying those concepts to Kris Corporation, it would be ideal to have at least two domain controllers at the Seattle location. With other locations, the amount of DNS servers greatly depends on employee count and expected employee growth over the next upcoming years. Also, in a multi-site environment like Kris Corporation, domain members should be configured to use DNS servers at their local site before looking to DNS servers at different sites – that way the amount of DNS traffic crossing slow WAN links is minimized! It’s also a best practice to use AD-Integrated DNS zones to simplify DNS replication and improve security – expanding more on that, because AD-Integrated DNS Zones are stored in directory partitions within Active Directory, those directory partitions replicate along the rest of AD with no extra configuration required for DNS replication. With keeping these best practices in mind and others, it’s now time to review best practices for securing DNS.

Langston (2017) highlights a few best practices when designing a secure, reliable DNS infrastructure:

* *Only make available what must be available* – avoid mixing public and private DNS functionality. For example, if there are domain names that must be resolved publicly, then only exclusive public DNS server(s) should be dedicated to that functionality; the rest of the DNS servers should be restricted to the public and available for internal access only.
* *Ensure availability* – a DNS server should be a part of a high-availability pair or cluster. That way a DNS server fails, there’s a backup available to take over the load.
* *Ensure that primary DNS servers are hidden* – DNS servers that host a master copy should be hidden! With a primary DNS server hidden, its responsibility is to serve that data to secondary nameservers and are not accessible to any end-user. This goes for external (public) primary DNS servers too – they should be behind a firewall with firewall rules in place to ensure only secondary DNS servers are the ones performing queries and transferring from primaries.
* *Think locally* – it’s important that users within the organization (and externally) are using nameservers that are local to them; this will avoid delays and unresponsiveness from distant WAN links.



*Diagram of an ideal and secure DNS setup.*

**DHCP**

Dynamic Host Configuration Protocol in Windows Server 2012 provides IP addresses to network client computers and server machines. As McIllece (2018) explains, DHCP maintains TCP/IP configuration information of clients in a centralized and automated fashion. The benefits of DHCP is the fact that it minimizes manual IP address configuration and reduces network administration since TCP/IP configurations are defined from a central location.

Because DHCP is an important part of any corporate IT infrastructure, having fault-tolerant features are a must. Thankfully as Clercq (2014) points out, the Windows DHCP server in 2012 supports three fault-tolerance options: installing DHCP on a Windows failover cluster, setting up a split-scope DHCP, or setting up DHCP failover – a feature that’s introduced in Windows Server 2012.

* *Installing DHCP on a Windows failover cluster* – installing DHCP on a two-node Windows failover cluster allows a second DHCP server to take the DHCP load if the primary DHCP server fails. The only issue with this method is that it uses shared storage and requires more of an upfront investment for storage redundancy.
* *Setting up a split-scope DHCP* – this method uses two independent DHCP servers that share responsibility for the same DHCP scope. One part of the IP address pool is assigned to the primary DHCP server while the other is assigned to the backup server. Although this method has fault-tolerance in place, it’s flawed if one of those servers fail – that means half of the IP address pool in the DHCP scope can’t be reached.
* *Setting up DHCP failover* – with this option, one or more complete DHCP scopes can be replicated to another DHCP server. To set this up in Windows Server 2012, right-clicking the DHCP scope from the DHCP management interface will bring up the **Configure Failover** option. With setting it up, one of two DHCP failover modes would require selection: either hot standby or load sharing. Hot standby mode is a failover relationship, where a primary DHCP server is responsible for leasing IP configuration data and the second DHCP standby server assumes the role of the primary server if it becomes unavailable. With load sharing mode, the two DHCP servers simultaneously lease IP configuration data to clients within the subnet. Without a doubt, DHCP failover would be the best option for Kris Corporation because of its true fault-tolerance and high availability.

Although DHCP has made life easier for network administrators and IT professionals, solutions for further centralized management in conjunction with DHCP in large organizations should be considered. As Joyner (2013) mentions, utilizing IP Address Management (IPAM) in Windows Server will help keep track of IP address information and to use those addresses even more efficiently. It manages the functionality of DHCP and DNS servers, as well as Network Policy Servers and Active Directory Domain Controllers. With this feature included in Windows Server 2012, this is a must tool for Kris Corporation to continually manage IP addresses within the organization – an excellent long-term solution that will save headaches in the future as the company continually expands nationally.

**Hyper-V**

Many organizations today are utilizing virtualization and making it a vital part of their IT infrastructure because of its ability to scale quickly and efficiency. As Warren (2008) defines it, a virtual machine is “a fully functioning virtual computer, where you can install a guest operating system of your choice, with network configuration, and a full suite of PC software”. A single server for example (depending on hardware) can have multiple virtual machines installed, which would essentially virtualize IT infrastructure and lead to less dependency of excessive hardware. Going further, Collins (2016) mentions that in the context of organizations virtualizing their IT infrastructure, they need a **hypervisor** – a thin layer of software that manages those virtual machines and allocates required resources. In Windows Server, Hyper-V is a hypervisor that allows IT administrators to create virtualized environments and manage them. Collins (2018) also points out pros and cons of Hyper-V, which include the following:

Pros

* Cheaper than other hypervisors like VMWare.
* Allows users to run a lot of VMs at one time with dynamic memory management.
* Maintenance doesn’t result in downtime.
* Backing up VMs are easy and to the point.

Cons

* Not the greatest support for Linux operating systems.
* All VMs have to go offline for a reboot when security updates are applied to its OS.

Despite some of those cons of Hyper-V, it’s clear that it fits the organizational needs of Kris Corporation. Another feature that will greatly benefit the company is Hyper-V’s replica feature – as Collins sums it up, it makes replication of servers across a WAN easy for an organization of any size! When combined with business continuity planning, Hyper-V’s redundancy can mitigate risk. With that said, it’s clear that Hyper-V and its ability to virtualize servers efficiently and easily is the solution to solving physical space issues in the Atlanta location as well as other locations.

**File Sharing**

It’s clear that at Kris Corporation, there are many locations nationwide with an existing IT setup that makes it difficult to share files across the organization. However, Windows Server 2012 makes file sharing easy within the organization. As Lowe (2012) highlights, after installing the File and Storage Services role, open Server Manager and navigate to:

**File and Storage Services -> Shares -> Tasks -> New Share**

After that, choosing a protocol that’ll be used for the new share. Within Kris Corporation, choosing the SMB Share – Advanced protocol would be the best choice because IT administrators can: set folder owners for access-denied assistance, configure access policies, and enable quotas. After selecting a drive location and share name, settings like **Enable access-based enumeration** can be checked off – that way files and folders are only displayed to users with granted permissions. **Encrypting data access** is another option that appears, which secures data within the share from unauthorized access. After selecting features from the Other Settings dialogue, it’s now time to set those **Permissions!** This is where an administrator can ensure only certain users from particular departments have access to data – for example, for an Accounting shared folder only users from the Accounting OU should have permission to read/write files and subfolders of that folder. In addition, specific permissions like giving IT administrators full control to those folders, subfolders and files can also be set. Once permissions are setup, **Quotas** can be enforced onto users – for example, having a 100 MB limit for each user accessing a specific shared folder. If the default quotas aren’t suited for a specific shared folder an IT administrator creates, then he/she can create a custom quota template from File Server Resource Manager. After it’s created, then it’ll be listed as a quota template choice for that new share.

**Conclusion**

Bringing it all together, the solution to many of Kris Corporation’s existing IT infrastructure challenges is utilizing Windows Server 2012 and its tools for long-term solutions. Active Directory is an incredible tool with even more functionality in Windows Server 2012 to address needs such as domain models and utilizing Active Directory Federation Services for SSO. From there, modeling DNS for Kris Corporation while addressing security to protect both external and internal DNS servers. Also utilizing virtualization with Hyper-V to virtualize existing IT infrastructure and save physical space; lastly sharing folders by creating a new share from File and Storage Services. By continually training IT staff on staying up to date with Windows Server and its many tools, Kris Corporation will continue to stay ahead of the competition with manufacturing auto parts while having an IT infrastructure that’s continually working.

References

Backup pricing. (n.d.). Retrieved August 6, 2018, from Microsoft website:

https://azure.microsoft.com/en-us/pricing/details/backup/

Best Practices for DNS Configuration in an Active Directory Domain. (2017, November 23).

Retrieved August 6, 2018, from Dell website: https://www.dell.com/support/article/us/en/04/sln155801/best-practices-for-dns-configuration-in-an-active-directory-domain?lang=en

Collins, T. (2016, May 5). Microsoft Hyper-V Performance and Cloud Hosting: Pros and Cons.

Retrieved August 6, 2018, from Atlantech website: https://www.atlantech.net/blog/microsoft-hyper-v-performance-and-cloud-hosting-pros-and-cons

Desai, P. (2013, April 26). How To Upgrade Windows Server 2008 R2 To Windows Server 2012.

Retrieved August 6, 2018, from PrajwalDesai website: https://prajwaldesai.com/how-to-upgrade-windows-server-2008-r2-to-windows-server-2012/

De Clercq, J. (2014, October 14). Fault-Tolerance Options for Windows DHCP Servers. Retrieved

August 6, 2018, from IT Pro Today website: https://www.itprotoday.com/windows-8/fault-tolerance-options-windows-dhcp-servers

Joyner, J. (2013, June 23). How to use IP Address Management in Windows Server 2012.

Retrieved August 6, 2018, from TechRepublic website: https://www.techrepublic.com/blog/data-center/how-to-use-ip-address-management-in-windows-server-2012/

Langston, M. (2017, February 6). Six Best Practices for Securing a Robust Domain Name System

(DNS) Infrastructure. Retrieved August 6, 2018, from Carnegie Mellon University website: https://insights.sei.cmu.edu/sei\_blog/2017/02/six-best-practices-for-securing-a-robust-domain-name-system-dns-infrastructure.html

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

6, 2018, from TechRepublic website: https://www.techrepublic.com/blog/data-center/how-to-share-a-folder-in-windows-server-2012/

Mathers, B. (2017, May 30). Identify Your AD FS Deployment Goals. Retrieved August 6, 2018,

from Microsoft website: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/identify-your-ad-fs-deployment-goals

Mathers, B. (2017, May 30). Reviewing the Domain Models. Retrieved August 6, 2018, from

Microsoft website: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/ reviewing-the-domain-models

Mathers, B. (2017, May 30). Understanding Key AD FS Concepts. Retrieved August 6, 2018, from

Microsoft website: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/understanding-key-ad-fs-concepts

McIllece, J. (2018, March 23). Dynamic Host Configuration Protocol (DHCP). Retrieved August

6, 2018, from Microsoft website: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Rosato, R. (n.d.). Best Practices for Applying Service Packs, Hotfixes and Security Patches.

Retrieved August 6, 2018, from Microsoft website: https://msdn.microsoft.com/en-us/library/cc750077.aspx

Shields, G. (2012, July 3). Quick Guide: What's New in Windows Server 2012 Active Directory.

Retrieved August 06, 2018, from Redmond Magazine website: https://redmondmag.com/articles/2012/07/01/whats-new-in-windows-server-2012-active-directory.aspx

Warren, S. (2008, December 4). What is your best definition of a virtual machine? Retrieved

August 6, 2018, from TechRepublic website: https://www.techrepublic.com/blog/virtualization-coach/what-is-your-best-definition-of-a-virtual-machine/