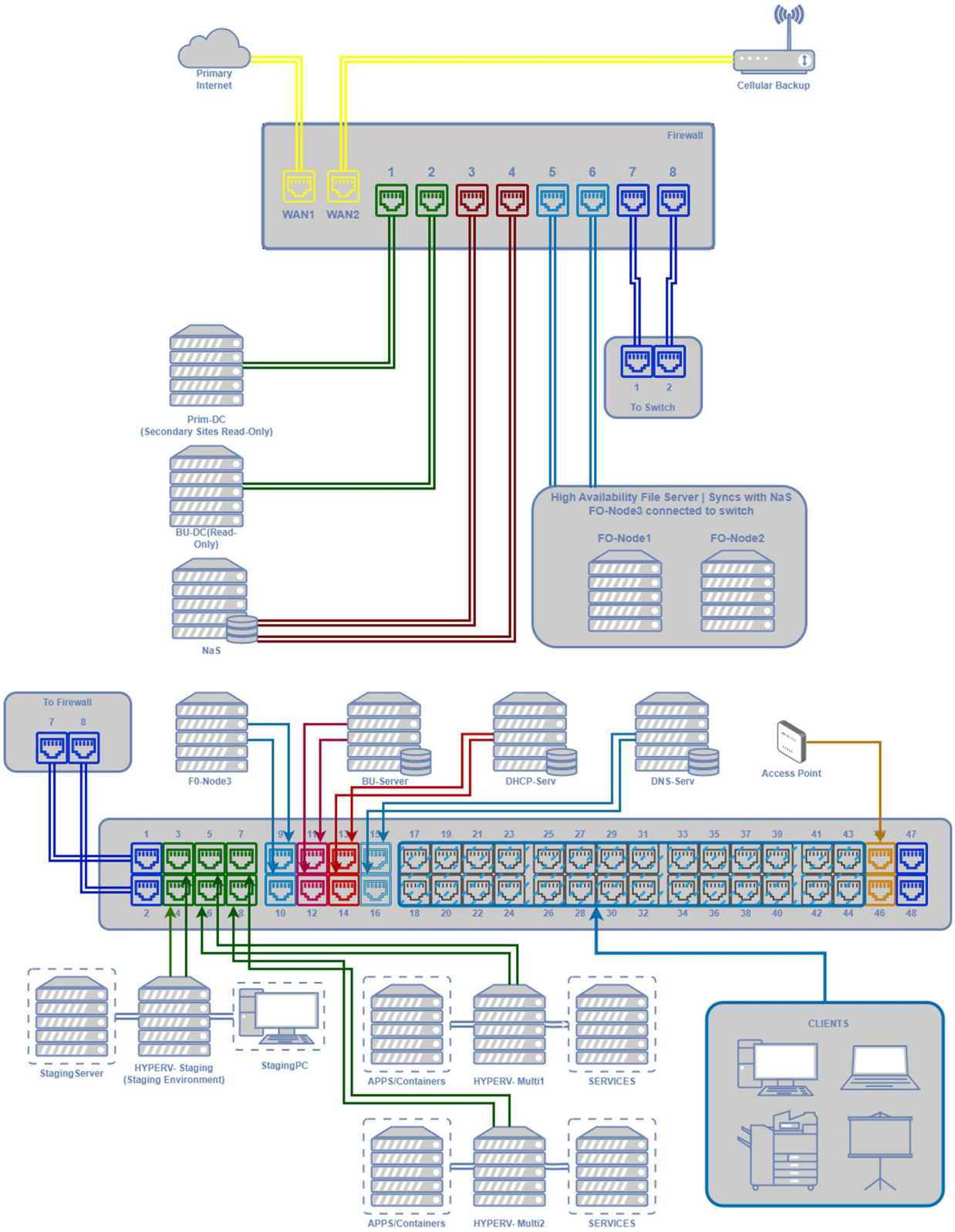
FakeTron Software Inc. | Installation & Recovery Guide

The purpose of this guide is to provide information on the installation, deployment, and recovery strategies for FakeTron Software Inc's network and computer infrastructure. This guide is intended to aid technicians in successfully installing, upgrading, and updating current and future sites. In addition, this guide contains recovery strategies to aid technicians in the event of equipment failures, natural disasters, and cyber threats. The ecosystem is designed with multiple redundancies in mind, such as a primary and backup Active Directory, NaS with a fail-over cluster consisting of 3 nodes, and layer 1 redundancy to multiple servers. The site will also be configured to have a primary and cellular backup internet connection. A VPN can be configured on the firewall at primary site and firewall at future site to connect and share resources. The ecosystem also has 2 Hyper-V servers capable of hosting virtual machines and containers to run apps. Services such as WSUS, log server, and update server can also be run on virtual machines. Ecosystem also includes a Hyper-V server for staging environment that allows for IT administrators to test updates and different implementations before rolling them out into the production environment. This guide also includes procedures and recommendations when it comes to server and infrastructure maintenance. As well as monitoring features provided by Windows Servers and third-party recommendations for network monitoring and ticket system that can aid technicians in keeping the ecosystem healthy and operating normally. This guide does not include roles and responsibilities of, group policy configurations, or network and server hardening techniques, but it is recommended for the organization to consult with their IT department or relevant leadership for best practices and implementations that pertain to the security and proper access levels of its employees and vendors for the safety of the ecosystem.

Topology


Primary Internet
Cellular Backup
Firewall
WAN1
WAN2
1 2 3 4 5 6 7 8
Prim-DC (Secondary Sites Read-Only)
BU-DC(Read-Only)
NaS
1 2
To Switch
High Availability File Server | Syncs with NaS
FO-Node3 connected to switch
FO-Node1
FO-Node2
To Firewall
7 8
F0-Node3
BU-Server
DHCP-Serv
DNS-Serv
Access Point
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 47
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
StagingServer
HYPERV- Staging (Staging Environment)
StagingPC
APPS/Containers
HYPERV- Multi1
SERVICES
APPS/Containers
HYPERV- Multi2
SERVICES
CLIENTS

IP Map

The purpose of this section is to aid technicians in installing, updating, upgrading, troubleshooting, and configuring most aspects of the server and network ecosystem. The benefit of having a unified template for devices and physical configuration assignments allows for technicians to better understand how the ecosystem operates and can significantly improve recovery times in the event of an incident. For the purpose of this assignment, device groups have not been separated into vlans, in a real production environment, the network design would be slightly different and multiple vlans and subnets would be assigned to ports and devices for improved performance and access control. Also not included is VPN information which will be needed when the company expands to a new location for the purpose of sharing network resources. Also, by default, the primary and backup domain controllers have DNS setup and the DHCP could be configured to assign primary and secondary DNS IP addresses that point to the domain controllers IP's instead of DNS server. Using a dedicated DNS server seems to be a bit tricky and further research would be needed to figure out how it would work properly with the primary and secondary domain controllers since Active Directory relies on DNS to function properly. (Hindman, 2019) (Microsoft, 2023)

IP information

Local Network: 192.168.50.0 /24 **New Location:** 192.168.60.0 /24

Default Gateway: 192.168.50.254 **New Location:** 192.168.60.254

Reserved IP Ranges: 192.168.50.1-20/192.168.50.251-254 **New Location:** x.x.60.1-12/x.x.60.251-254

Primary DNS: 192.168.50.252 -or- 192.168.50.1 **New Location:** 192.168.60.252 -or- 192.168.60.1

Secondary DNS: 192.168.50.253 -or- 192.168.50.2 **New Location:** x.x.60.253 -or- x.x.60.2

Cluster: 192.168.50.4 **New Location:** 192.168.60.4

File Share Witness: \\faketron-cl\fsw

Device/Server	IP Address	Port(s)
Primary Internet	Dynamic WAN DHCP	FW – WAN1
Cellular Backup	Static IP: 166.254.46.13	FW- WAN2
Prim-DC	192.168.50.1	FW-Port 1
BU-DC(Read-Only)	192.168.50.2	FW-Port 2
faketron-fs	192.168.50.3	FW-Port 3-4
F0-Node1	192.168.50.5	FW-Port 5
F0-Node2	192.168.50.6	FW-Port 6
F0-Node3	192.168.50.7	SW-Port 9-10
HYPERV-Staging	192.168.50.8	SW-Port 3-4
HYPERV-Multi1	192.168.50.9	SW-Port 5-6
HYPERV-Multi2	192.168.50.10	SW-Port 7-8
BU-Serv	192.168.50.11	SW-Port 11-12
DHCP-Serv	192.168.50.12	SW-Port 13-14
DNS-Serv	192.168.50.252/192.168.50.253	SW-Port 15-16
Access Point	192.168.50.13	SW-Port 45-(46)
Clients	DHCP – 192.168.50.21-250	SW-Port 17-44

SW-Port 47-48: Optional trunk ports to expand to an additional switch

Deployment and Server Information

For the primary site, a total of 12 servers will be needed. The primary and backup Active Directory DC's will be on their own bare-metal servers for optimal performance and redundancy. The domain controllers are a vital part of the server ecosystem, and it is important to ensure that access to Active Directory always remains accessible. Since both of these servers will only have AD DS and DNS roles installed on them, WS2016 – Essentials will be sufficient for these machines.

The NaS server will also be on its own dedicated hardware, with multiple hard-drives with a RAID-5 configuration for added redundancy. The NaS server will sync with the high availability cluster servers F0-Node1-3. F0-Node3 is connected to the network switch so in the event the firewall goes offline, employees will still have access to file shares to minimize the impact of downtime. WS2016 – Datacenter Edition will be needed in order to use Storage Spaces Direct and Storage Replica features.

The HYPERV-Staging server allows IT administrators and developers to test new implementations, whether it be an update, upgrade, a new app or service that is hosted through a virtual machine or containerized. A staging environment is beneficial as it provides a sandbox where mock servers and apps can be tested with updates and configuration changes without affecting operations on the production side.

HYPERV-Multi1 and HYPERV-Multi2 allow for multiple apps and services to be run sharing the same hardware. Services such as IIS can be run on a nano-server on a Hyper-V server to host web applications needed by the firm if the app needs to be run in-house. Containerized apps can also be run on either HYPER-V server, it is also possible to migrate from the staging environment with ease when an app or service is ready to be rolled out into production. WS2016

will be needed for all Hyper-V servers since it provides unlimited support for containers, Hyper-V containers, and Nano Server support.

BU-Serv is the dedicated backup server capable of backing up data and server images in the event of an incident where a server within the ecosystem fails and needs to be replaced. Backups can be scheduled or manually performed. Incremental backups can be performed to reduce network traffic and bandwidth issues. The domain controllers typically aren't backed up since there are two of them and if one of them were to fail, the working DC can be promoted to primary, and active directory can resync after any hardware replacement with ease. Backup Server will need WS2016 – Datacenter Edition to fully take advantage of storage features Windows Server has to offer.

DHCP-Serv is used to automatically assign IP addresses for clients or devices connected to the network. The access point for Wi-Fi connectivity will also use this server to assign IP addresses to clients. Though the firewall does have the capability to run a DHCP server, having a dedicated DHCP server frees up resources on the firewall for better performance.

DNS-Serv allows for IP addresses to be pointed to a nameserver. This can be useful when web apps are installed on one of the Hyper-V servers, allowing for clients to enter a web address instead of an IP address. It would be recommended for both DHCP-Serv and DNS-Serv to have WS2016 – Standard Edition.

The Access Point allows for clients to connect to network via Wi-Fi. There are two ports assigned for this in the event more coverage is needed at a site, a second access point can be strategically placed. The access points can use the DCHP-Serv server to obtain IP information for clients to connect.

Client access ports allow for up to 28 PC's, printers, or other devices that are needed to

connect to the local network or internet. It is important to note that ports 47-48 are designated as trunk ports if the need to expand connection to a second switch is needed.

Active Directory

The purpose of Active Directory is to centralize user management and access. A server can be promoted to a domain controller, allowing for PC's and other servers to join the domain and utilize the access controls. By default, a DNS server also resides on the domain controller as AD heavily relies on DNS to function properly. There is also Group Policy that allows permissions and access controls to be assigned to different users and groups. Ensuring access to Active Directory is important because if AD goes down, users will not be able to access their accounts and it will prevent servers from communicating with each other. This is why there are typically a primary and backup domain controller in the event one of them goes down. The backup domain controller is typically read-only and syncs with the primary domain controller. In the event one of them goes down, PC's and servers primary secondary DNS assignments will point to the backup or primary DC, maintaining access to these important resources.

When the second office goes into production, there are two options. The secondary site could have 2 read-only DC's, and sync with the primary DC at primary office via VPN. A VPN between sites would also allow for other services and resources to be shared and could even benefit if some employees work remotely from home. In addition, when site upgrades Active Directory from Windows Server 2012 to Windows Server 2016, the firm can deploy WS2016 and install AD DS, promote it to a domain controller, then copy AD from WS2012, then make it the primary DC, then upgrade the WS2012 server to 2016 and make it the backup DC. This will eliminate downtime during the upgrade process. It is important to note that a secondary DNS address that points to the new WS2016 AD will need to be configured on all devices for this to

work properly. This can be a fairly easy process by using DHCP server to update IP information for clients, however, any servers statically configured will need to manually be updated.

Proper use of AD organizational units will aid in properly representing the business' structure. This includes applying proper assignments, access levels, and permissions to users, groups, computers, and other organizational units. For example, IT administrators will need to their own set of access levels and permissions from group policy, which employees from other departments shouldn't have. Also, there may be a billing or finances department that should have access to certain apps or systems that developers wouldn't necessarily need access to. When organizing OU's, it is important to keep in mind who should have access to what, so when adding group policy objects, if OU's are properly setup, it will be easier to effectively assign access levels and permissions to user and groups only to areas they need. According to Desmond et al. (2008), when it comes to the AD Organizational Unit hierarchy, other items have bearing on that design. There are two key design issues that affect the structure of OU's, which are permissions delegation and GPO placement. With that said, it is important to structure OU's in a manner that facilitates their respective administration. For example, IT administrators being in one OU, developers being in another. (Desmond et al., 2008)

There are a few requirements when deploying Active Directory. The first, the server needs to be named before installing AD. Second, the server must have a static IP address to function properly. Third, the server should be dedicated solely for running AD. It is also important that the hardware specs are sufficient to handle the workload that Active Directory will run under. (Mutuma, 2023)

Containers

The benefits of using containers for the firm will add efficiency to the apps they use for day-to-day operations. They are also portable and can move among many different types of systems without having to alter code. Developers will also benefit from using containers when collaborating with each other and the firm's clients. The firm will be able to easily deploy apps into their ecosystem without the need to plan for dependencies and altering the host OS's to accommodate. (Ghillis, 2023)

High Availability

High Availability plays a major role in the sustainability of the firm in multiple ways. HA allows for system components to have redundant access in the event of a failure, whether it be connectivity issues or hardware failure. The ecosystem has a NaS file resource server that syncs with a fail-over cluster that consists of 3 nodes. Network load balancing can play multiple roles. NLB has built-in features. First, NLB can detect if a cluster host fails or goes offline, and then recover. Second, NLB can balance the network load when hosts are added or removed. Third, NLB can recover and redistribute the workload within 10 seconds. (Microsoft, 2021)

The ecosystem also has a primary domain controller and a backup read-only domain controller, when DNS is properly configured and assigned to all devices, if one DC goes down, servers and PC's will still be able to access the other one, allowing IT administrators to troubleshoot and fix the affected DC. In some cases, the read-only DC may have to be converted to a primary DC, and the downed DC can be rebuilt and copied from the newly converted DC.

In addition, multiple servers have redundant layer 1 connectivity, meaning that there are 2 physical ethernet connections from the servers to the network equipment. This could also be used for network load balancing if a server is experiencing a high rate of data transfers.

(Troutman, 2021)

Hyper-V

The ecosystem consists of three Hyper-V servers, one intended to be used as a staging environment, and the other 2 for production capable of running type 1 hypervisors and containers. It is also possible to add the 2 production servers to the cluster, allowing live migrations and fail-over to take place in the event one of them go offline. The plan currently does not reflect this since this is a small firm but can be easily implemented if the firm decides to add further HA for their virtualized environments. This can be done by adding the Hyper-V servers to the HA cluster. Further expansion could include adding more Hyper-V servers to the ecosystem if needed. This adds to the many benefits of Hyper-V and using Hyper-V Servers to host type 1 hypervisors. First, multiple systems can make more efficient use of hardware resources. If each application or service were on their own bare-metal hardware, then there is a chance that much of the server's resources would remain unused. Other benefits include centralized computing with multiple advantages that include consistent level of service, improved security, reduced operational costs, standardized management approach, and clearer understanding of maintenance, power, and cooling costs. Another main benefit is using virtualization reduces time needed to migrate new software from the staging to the production environment, as well as deploying new apps or services to be integrated into the ecosystem. (Finn, 2010)

Disaster Recovery

One of the most important aspects when it comes to disaster recovery is having secure backups in the event of hardware failure. The ecosystem has a dedicated server for obtaining

backups of all systems and data. It is also possible to perform off-site backups, especially when the new office gets deployed. Redundancies such as extending nodes to the new office can aid in adding further redundancy in the event a natural disaster were to occur to one of the sites. There are also cybersecurity risks that would need to be considered when deploying backup strategies to protect from cyber-attacks such a ransomware attacks. There have been instances where a firm did not properly protect their backups and hackers were able to encrypt access to their backups as well, forcing the company to pay the ransom, or even succumb to total loss of systems and resources depending on the cyber-attack. One example of this was a company called Code Spaces, who went out of business after experiencing a cyber-attack that wiped out most of their data, backups, machine configurations, and even off-site backups. The hackers were able to access the Code Spaces' Amazon EC2 control panel, from there they were able to destroy data and perform DDoS attacks that took everything offline. Code Spaces was unable to recover from the attack and ultimately went out of business. (Chauhan, 2020) This adds to the importance of maintaining proper and secure backups in the event they are needed.

Maintenance

Windows Server Update Services can be utilized on dedicated hardware or virtualized. In the case of this firm, it will be virtualized. The Hyper-V staging environment will be the recommended place to test updates and patches before rolling them out to the production environment. According to Barber (2005), one of the major benefits of using WSUS is that it is free and is a good patch management service with many enterprise features for maintaining a healthy server ecosystem. Some of these features include updates for the Microsoft Family of products, control over the installation and removal of updates, flexible and scalable architecture, flexible update storage options, network bandwidth optimization, a web-based management

interface, native integration with automatic update client, and integrated reporting capabilities. (Barber, 2005)

Monitoring

The purpose of monitoring server and network operations is to ensure the ecosystem is operating normally. It is also used to detect issues that can be resolved before downtime occurs. For example, if 2 of the nodes on the Fail-over cluster goes down, leaving the ecosystem on its last leg, without monitoring, it is possible that the firm would not be aware of the issue until the last node goes offline. With monitoring, IT administrators can be notified if a node goes offline or is experiencing high utilization, allowing them to troubleshoot and resolve an issue before it becomes a bigger problem.

Windows Server comes with two useful tools. First, is Performance Monitor, which allows for different metrics to be monitored and measured in a centralized fashion. If any of these metrics exceed a specified threshold such as CPU utilization or Memory utilization, alerts can be setup to notify IT of a potential issue about to occur. Second, Resource Monitor, which shows how processes and services are using system resources. It allows administrators to monitor resources in real time, as well as analyze unresponsive processes, determine which applications are using files, and control processes and services.

In addition to monitoring servers, monitoring network devices is equally as important as it is what connects everything together. Third-party applications such as Zabbix is capable of monitoring devices that fall outside the Windows Server ecosystem. Zabbix is capable of gathering data via ICMP, SNMP, or IPMI to check if a device is online and collect various metrics to compare against specified thresholds. If a threshold is exceeded, it can send alerts by

generating an auto-ticket to a ticketing system the firm uses, email, or SMS. The platform is also capable of storing data for future analysis. Zabbix can also display graphs of metrics for better visualization enhancing the ability for better analysis. (Rihards Olups, 2016)

Another great monitoring option is centralizing logs by setting a centralized log server, this can be virtualized or on dedicated hardware. The main benefit of using a centralized log server is all logs are gathered in one place, and if a server happens to go down, administrators can review logs before the downtime occurred, especially since logs can't be individually accessed when a server is down. This is made possible by using Windows Event Collector(WinRM) protocol to enable centralized logging. This allows Event Viewer to pull logs from multiple servers using the subscription feature. (Sharif, 2023)

Conclusion

There is a lot of planning that goes into the design and configurations of a Windows Server ecosystem, as well as the network devices that connect them all together. One of the most important takeaways is providing a unified template that contains all the information needed for IT administrators and network engineers to refer to when working with the ecosystem. Another important aspect is ensuring that secure backups are effectively implemented into the ecosystem. Also ensuring the right people have proper access to the resources they need, and don't have access to the resources they don't need. And lastly, ensuring all systems and software are kept up to date and patched to reduce cybersecurity risks to the firm.

References

Barber, B. (2005). How to Cheat at Managing Windows Server Update Services. In *Google Books*. Elsevier. https://books.google.com/books?hl=en&lr=&id=qjMIHPPDQGsC&oi=fnd&pg=PP1&dq=benefits+of+using+WSUS&ots=SuALrQqPYV&sig=3hfmjbnQqzKz8le-XHAUUztheBg#v=onepage&q=%22major%20benefit%22&f=false

Chauhan, B. (2020). *4 Times Companies Were Forced to Shut Down Due to Hackers*. Astra Security Blog. https://www.getastra.com/blog/911/4-times-companies-were-forced-to-shut-down-due-to-hackers/

Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. G. (2008). Active Directory: Designing, Deploying, and Running Active Directory. In *Google Books*. "O'Reilly Media, Inc." https://books.google.com/books?hl=en&lr=&id=exlzxcsE-7QC&oi=fnd&pg=PR5&dq=Active+Directory+organizational+units&ots=JIW3G_ImO2&sig=IncqsHihk8U28xc8pUadG99g7c0#v=snippet&q=%22with%20organizational%20units%2C%20you%20can%22&f=false

Finn, A. (2010). Mastering Hyper-V Deployment. In *Google Books*. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=Q5NMwwGDT_8C&oi=fnd&pg=PR21&dq=benefits+of+hyper-v&ots=cD051FiIVZ&sig=_pMawG2hcoDWvVZxjAPZtR5OClg#v=onepage&q=%22live%20migration%22&f=false

Ghillis, A. S. (2023). *What Are Containers (Container-based Virtualization or Containerization)?* SearchITOperations. https://www.techtarget.com/searchitoperations/definition/container-containerization-or-

container-based-virtualization

Hindman, R. (2019). *Configuring IP Addresses and Dependencies for Multi-Subnet Clusters - Part III*. TECHCOMMUNITY.MICROSOFT.COM. https://techcommunity.microsoft.com/t5/failover-clustering/configuring-ip-addresses-and-dependencies-for-multi-subnet/ba-p/371698

Microsoft. (2021). *Network Load Balancing*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/networking/technologies/network-load-balancing

Microsoft. (2023). *Integrating AD DS into an Existing DNS Infrastructure*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/integrating-ad-ds-into-an-existing-dns-infrastructure

Mutuma, J. (2023). *How to Setup Active Directory on Windows Server 2022*. InfraSOS - Active Directory Tools, AD & Office 365 Reports & Management. https://infrasos.com/how-to-setup-active-directory-on-windows-server-2022/

Rihards Olups. (2016). *Zabbix network monitoring* -. Packt Publishing Limited. https://books.google.com/books?hl=en&lr=&id=xgjVDQAAQBAJ&oi=fnd&pg=PP1&dq=zabbix&ots=zSygjsN6lt&sig=a9VM6V-FNp9zX_PrD_Mz8vXeCOE#v=onepage&q=zabbix&f=false

Sharif, A. (2023). *Windows Logging Guide Part 4: Centralizing Logs*. Crowdstrike.com. https://www.crowdstrike.com/guides/windows-logging/centralizing-logs/

Troutman, M. (2021). *High Availability (HA): What Are the Benefits?» LINBIT*. LINBIT. https://linbit.com/blog/high-availability-benefits/