Creating & Maintaining a Successful Computer Network

Matthew S. Almendinger
Published: 9/25/2017
Updated: 5/29/2018

LIGHTHOUSE
IT SOLUTIONS

Contents

LIGHTHOUSE IT SOLUTIONS

WHO WE ARE – Wouldn't it be great if your network worked as hard as you did?

What if it was more than just a necessary component to how you did business, but rather an exciting and integral advantage to your process?
Founded in 2011, Lighthouse IT Solutions provides end-to-end solutions and management of our clients' network-based processes. From desktop management, to implementing an ERP system, we're here to help whenever you need it. For us, it's more than just using buzzwords, it's about becoming an indispensable partner to you and your business--because your success means our success.

WHAT WE STAND FOR – Our mission is to passionately create harmony between technology and our clients.

Lighthouse IT Solutions is a company passionate about technology. We want to be an IT provider committed to serving our clients wholly and eagerly. With a long history in the Small-to-Medium Business market, our engineers have assisted clients in creating and maintaining a network infrastructure that fits their needs; nothing less.

Gone are the days when dealing with an IT specialist is a chore. We love what we do and are excited to be able to show you how it can make your business run better! Stop floating around in the darkness of your IT environment, we can show you the way! Let us help you leverage your infrastructure to create something truly unique to your business.

WHY LIGHTHOUSE IT SOLUTIONS? – Because we care.

That's not just cliché, that's philosophy. At Lighthouse IT Solutions, we've dedicated our business to understanding our clients, their needs, and their goals. As we've grown as a company, our focus has tightened on creating a harmonious interaction between your servers, computers, networks, and people. Our drive to create a world where technology plays well with its mates and its users created our managed services platform: **Harmony**.
Harmony is not just a product, nor is it a series of products. It is an end-to-end solution designed to work together to help your business grow. At the center of it all is us -- the missing piece to manage and maintain all the pieces to work in cooperation.

Introduction

The integrity and smooth operation of your organization's network has never been more important. To help your business do what it does best, it needs a network that is able to not only be reliable, but to be built upon a foundation designed to withstand the test of time.

This guide is intended to help you establish procedures and policies in accordance with best practices so that your network is as resilient as possible. There may also be a time when you need external help – following these tenets will help your business keep consulting costs down when it comes time to engage outside help.

Our goal is to empower you to build the dream network your business deserves because it is our desire to build partners, not just customers.

1. And so it begins...

If you are just getting started with a computer network or looking to do an overhaul of your current network, let us begin by looking at the basics.

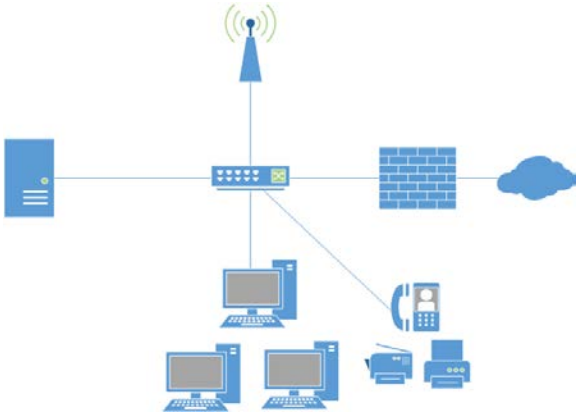

Illustration 1.1 – Basic Network

The most basic network should have:

- A quality firewall
- A network switch (not a hub; may be integrated into the firewall, depending on scale needs)
- A server
- Client computers

You may also want to look at:

- Wireless Access Points (may be integrated into the firewall, depending on scale needs)
- Multifunction Print devices or printers
- Tablets and mobility devices

PRO-TIP: Thinking About Scale

Using firewalls that have wireless integrated and switches can be fantastic to simplify cost in the beginning, but they could limit scalability as your business grows. Consider them with caution.

There are some items to note in the above lists, first and foremost is that you will want a quality, next-generation firewall. A high-quality firewall grants you the flexibility of allowing permissible traffic into your organization, all the while keeping the bad guys out. They can also do

traffic scanning of data coming and going out to make sure there is no malicious software detected. This can protect your company from being compromised or even isolating computers that have already become compromised.

The other important item to note is that we recommend you have an on-premise server. Why have an on-premise server when so many cloud services exist? Simply put, a server allows you to enable centralized management of your organization. It enables you to have centralized security and will become the hub of your successful network. As an added bonus, you will find that many applications integrate with Active Directory, meaning you can reduce the number of logins your staff has, plus simplify managing the number of accounts you need to maintain! Since entry-level servers have become very reasonably priced, there isn't really a reason not to have an on-premise server to start your network.

Consider This… Network Firewalls	
Sophos XG 105/105W	http://www.sophos.com
Cisco Meraki MX65/65W	http://meraki.cisco.com
Draytek Vigor 2925	http://www.draytek.com
Cisco 5506-X or 5506W-X	http://www.cisco.com
Sonicwall TZ300	http://www.sonicwall.com

PRO-TIP: Setting it all up

As tempting as it is may be to try to set up Active Directory on your own, you'll want to have a trustworthy service provider set it up for you. Just like a building, everything we do from here sits upon this foundation.

Whitebox vs. Brand-name: Does it matter?

There is an age-old debate as to whether brand name computers and servers matter, or if you should build your own. The first consideration is whether or not you have the technical expertise to do so, but to us the biggest consideration is long term support.

When building your systems (whiteboxing), you may be able to get more for your money per computer, however it comes at the expense of long term support. Hardware components go through refreshes several times per year. As they do, old models are pushed out the door in favor of new models. This rapid lifecycle means that replacing components that are like-for-like becomes extraordinarily difficult. Since you are the builder of these machines, it also means that you need to

either purchase an appropriate number of spares or be subject to replacing a system far earlier than the recommended cycle, which is 36-48 months.

Manufacturers that specialize in businesses do rigorous testing and engineering on their equipment to ensure lower failure rates because they typically offer longer warranties – 3 years being standard. In the event that you do need a replacement part, you (or really anyone capable of using the phone) can contact the manufacturer and have an identical component installed, meaning downtime is minimized.

At Lighthouse IT Solutions, we recommend brand-name equipment so that you are not tied to a single service-provider. We also encourage our clients to look at system lifecycles of 36-48 months for desktops and 60-84 months for servers to ensure optimum reliability.

2. Centralizing Management Using Active Directory

The very heart and power of a successful network comes from simplifying management. Active Directory makes managing servers, clients, security and policies extremely simple and yet highly scalable. This is likely one of the major reasons that most companies choose to adopt Windows as their operating environment for their desktops and servers. By using Active Directory, you can centralize security, manage resource locations, manage clients and apply security and policies to your business by using an already established hierarchy.

Making Active Directory Look Like Your Business

The most common use for Active Directory is to centralize security. This means that your users, computers and security groups are stored in a common database. This allows a user to log in to any computer as him/herself. It also allows you to restrict or allow computers access to resources (computers have accounts too!), create common groups to simplify permissions assignments, as well as create Organization Units to contain those items. Those Organization Units can be used to apply policies to users and groups, or just better organize your directory to make more sense according to your business.

As we start building an Active Directory that's made for your business, we'll use one for *LabCo* for illustrations.

Consider This… Computer & Server Manufacturers	
Hewlett Packard	http://www.hp.com (Desktops/Laptops) http://www.hpe.com (Servers)
Dell	http://www.dell.com
Lenovo	http://www.lenovo.com

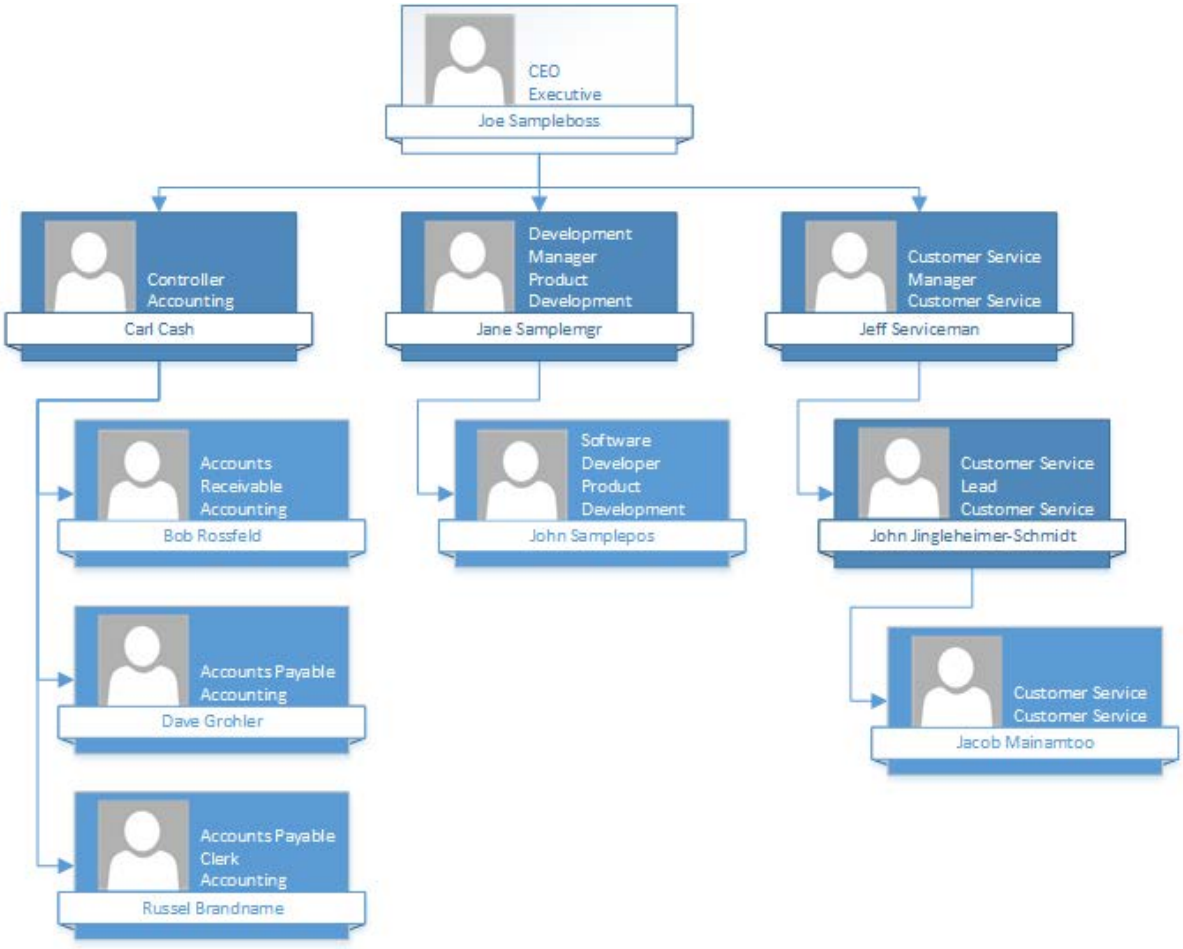

Illustration 2.1 – Sample Active Directory

In the example above, we see that *LabCo* has three departments – Accounting, Product Development and Customer Service. If we look at **Illustration 2.2**, we could just create all of our users in the Users folders and organize the departments into groups, but that actually makes it hard to visualize and manage our users as we grow. It also adds complexity to creating security

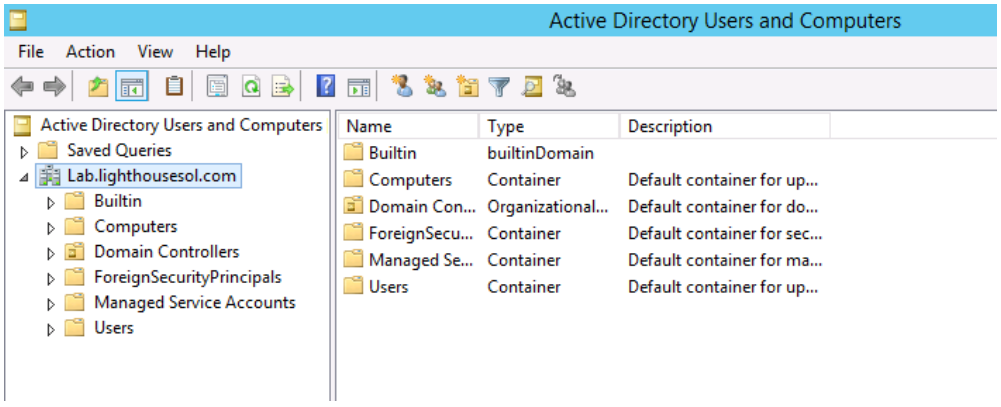

Illustration 2.2 - Active Directory Fresh from the Install

groups as we may need to apply some groups to users in other departments. Instead, what if we created our own "folders" for the three departments? This is where Organizational Units come in handy. Organizational Units (OU) are effectively containers that allow you to house objects for the sake of organization. Outside of making your Active Directory structure look pretty, the only other use for OUs is for assigning policies to objects – they have no other impact to your network.

In the adjacent figure, you will see we have done just that – a separate OU for Accounting, Customer Service and Product Development. We have also added a fourth called Global Security Groups, which we can use to hold Security Groups that do not necessarily make sense being stored under a specific department. Again, this is all preference, but the cleaner your organization's structure is, the easier it will become to manage and automate. Now that we have our organization plotted out in Active Directory, let's create our users.

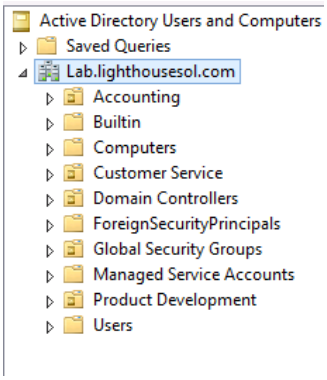

Illustration 2.3 – Active Directory Users and Computers Tab

You can see in our example that now if we wanted to find a user – or copy a user from a similar role, it is much easier to find exactly what we want.

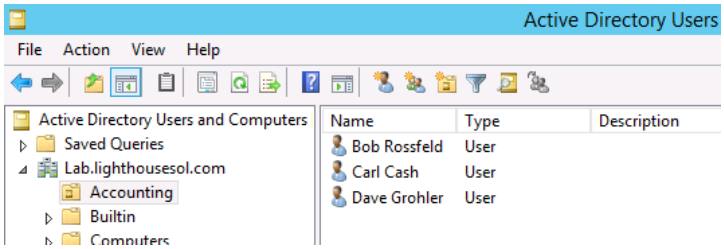

Illustration 2.4 – Active Directory Organization

Adding Computers to Active Directory

As mentioned earlier, just like users, computers also have accounts in Active Directory. This allows your workstations to be authorized or denied access to network resources just the same as any other object. Just like users, they can also be added to groups if desired, or organized into OUs. Unlike users, however, computer accounts are typically created by the computers themselves when they are connected to the domain in a process called "Joining." To get the most from your network, you will want your computers to be joined to your domain.

To Join a Computer to Your Domain:

- Open the System properties Windows (Windows 10: Right-click start, go to System; Windows 7: Right-click computer and choose "Properties")
- *For Windows 7, Windows 8 and Server 2012 R2*, you will see a link named "**Change Settings**" under Computer name, domain and workgroup settings. Click this link.

- Under the computer name tab, you will find a button named "**Change**."
- Enter your domain information, either the fully qualified domain name or the NETBIOS name given to you when Active Directory was installed. Click **OK**.
- Provide your credentials. Any set of credentials may be used to connect a domain, however, domain users have only a handful of usages. Domain Administrator accounts can add an unlimited number of computers and is typically the credentials used. Click **OK.**
- Restart your computer when prompted.

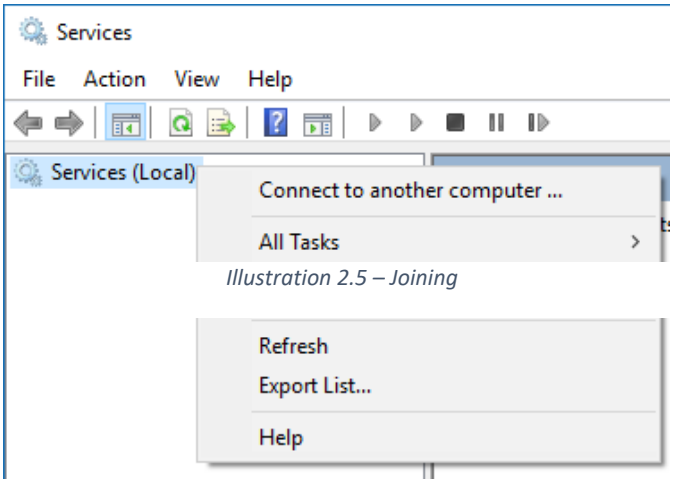

Illustration 2.5 – Joining

- *For Windows 10*, click "**Join Domain**"
  - Enter the fully qualified domain name or the NETBIOS name given to you when Active Directory was installed. Click **Next**
  - Provide your credentials. Any set of credentials may be used to connect a domain, however, domain users have only a handful of usages. Domain Administrator accounts can add an unlimited number of computers and is typically the credentials used. Click **OK.**
  - Press **SKIP** to skip user assignment.
  - Restart your computer when prompted.

Managing Domain Joined Computers

Congratulations, you have an Active Directory network! Now that the hard work is done, you can revel in the power that comes with centralized management. One of the greatest features comes from being able to manage many aspects of your network from a central location.

If you have ever opened Computer Management, Services, or nearly any other administrative console, you have interacted with the Microsoft Management Console. Microsoft Management Console is a shell for various snap-ins that talk directly to the operating system, enabling you to control your system with ease, but did you know that the Microsoft Management Console can also be used to connect to other systems and perform the same functions?

For instance, you could restart the DNS Client service on Bob's computer or check the event log of Dave's without ever leaving your desk. It's simple, too! Once you have opened up your management console of choice, the treeview at the left will typically start with the name of the Management Snap-in

and Local in parenthesis. This is because you are viewing the console while connected to the local computer. If you right-click on this top-level item, however, you will see an option to "connect to another computer." From there, you can type (or pick from Active Directory) the computer you want to connect to and see the status of the console and perform operations (as in our Services example, you can restart services). Please note that software firewalls and your local permissions may limit what you can do, but try it out while logged in as a Domain Administrator.

The fun doesn't stop there, though! You can also launch Microsoft Management Console as an empty console. Go to File > Add/Remove Snap-ins and create a custom console just for you. Save the console to your desktop and make your own management portal for your organization.

Managing Servers & Server Roles

While using the Microsoft Management Console is useful for troubleshooting, it is not necessarily as useful when you are checking up on your servers when you don't have problems or need to make configuration changes. Starting with Windows Server 2012 and later, Microsoft introduced a new and revamped Server Manager. Server Manager allowed you to connect all your servers to one management interface and gather basic details and configuration about all of the servers in your network. It also provides a list of all the roles offered by those servers and enables you to configure them or view the status – from one single spot. You can use Server Manager to Add or Remove roles from your servers or launch the various administrative consoles, all without ever leaving the program.

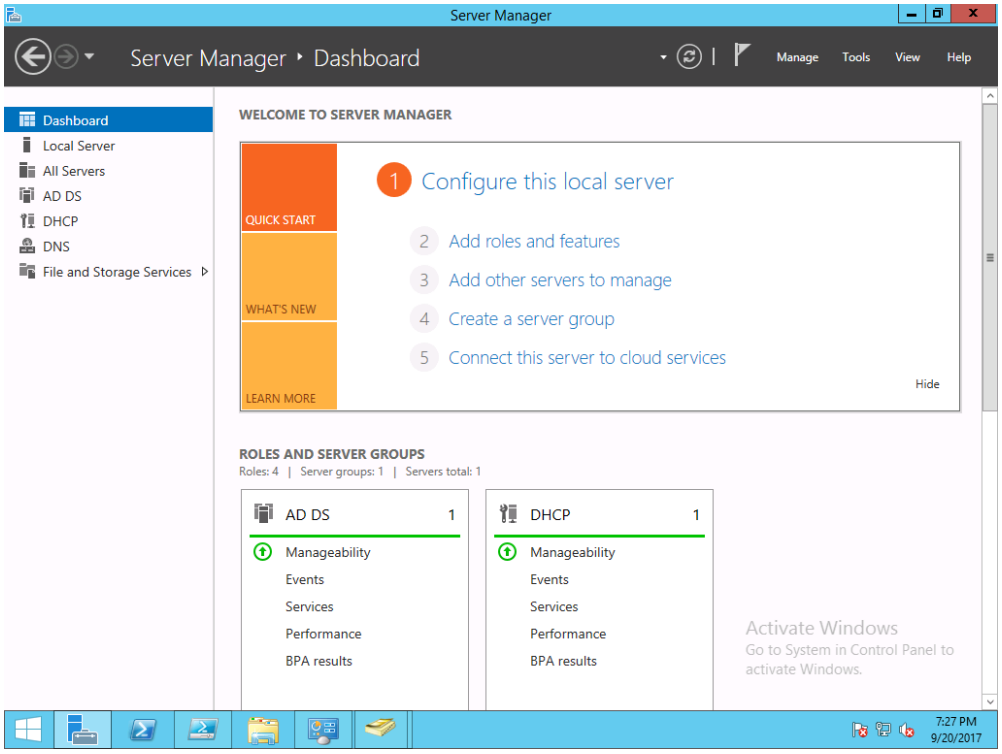

Illustration 2.6 - Server Manager

Managing Your Servers from Non-Server Windows

Server Manager is built-in for all server platforms starting with Windows Server 2012, but what if you want to sit at your desk and manage your workhorses? This is where RSAT comes in.

Remote Server Administration Tools (RSAT) is a software package for your Windows desktop. By installing RSAT, your desktop will have access to Server Manager, as well as all the administrative tools that come with the servers – allowing you to connect, manage and monitor all from your desk. RSAT is available for the non-home editions of Windows 8, 8.1 and Windows 10 operating systems.

3. Protecting Your Network: Windows Updates

Software is fallible. There are bugs, glitches and holes that exist because they were created by imperfect beings, but software is also living – that is to say, it is always being updated and made better, more secure and more resilient.

Unfortunately, though, there are people who exploit these gaps to compromise your systems. Whether it is direct monetary gain, such as ransomware, or indirectly by harvesting data about you, your clients, or your staff, bad people love unpatched systems.

Unpatched systems account for one of the largest security concern on most organizations, second typically to only user account issues (easy passwords, open accounts and etcetera). Therefore, it is extremely important to make sure that your systems are kept up to date.

PRO-TIP: Windows Server Update Services

While not as common, some administrators prefer to wait before updates are installed. Using tools like Windows Server Update Services (WSUS), you can incorporate approval workflows and roll out updates in a controlled fashion. WSUS can also cache the updates to itself to reduce internet traffic load caused by updates. WSUS is a Windows Server Role.

Enabling automatic updates on your computers will help you mitigate the threat of compromise due to known bugs. Software patches are also designed to help your systems run more reliably. Just as important as your desktops is your servers, so don't forget to make sure that they are fully patched as well!

4. Protecting Your Network: Endpoint Protection

Your client machines are the endpoints of your network. Your network exists to service them and their needs so that your business can flourish, but endpoints are also the most exposed of all your equipment to malicious software. Why? Because your endpoints are utilized by your end users, who are not as security minded as we are. Authors to malicious software (or "malware") design their code to trick or confuse your users into doing something they did not actually intend to do – and once they do, you have a new mess on your hands.

Endpoint Protection software is designed to monitor processes and communication on your client computers to make sure that nothing bad gets into your network – keeping you and your data safe.

Choose an endpoint protection program (EPP) designed for businesses – EPPs designed for businesses typically allow you to view all your computers at a glance to make sure that they are receiving the most recent updates and alert you to any detected threats. Make sure that you deploy your endpoint to every machine, especially those like laptops that leave your network. Periodically check your Endpoint Protection Console to verify that it is working properly.

Consider This… Endpoint Protection	
Sophos Endpoint Protection	http://www.sophos.com
Symantec.cloud	http://www.symantec.com
Panda Cloud Security	https://www.pandasecurity.com
ESET	http://www.eset.com
Trend Micro	http://www.trendmicro.com

5. Protecting Your Network: Backups & Disaster Recovery

Despite all our planning, let's be real – something we do not want is bound to happen. Having the right disaster recovery plan and implementing the software to help you automate it is very key. Think of Backup & Disaster Recovery software as being an insurance policy: something you hope you never have to use, but make sure that you have the right coverage. Checking your backups is something that should be a priority to your organization and seeing a failed backup should be akin to treating a server being down. That is to say – a nonfunctioning backup should be a critical issue.

Picking a Solution

Your reliable Disaster Recovery Plan starts with a software solution/strategy.

When choosing a backup solution, make sure of the following:

- **The backup solution supports image-level backups**: The backup includes the server's system state, which allows the backup set to restore the server fully – including everything needed to make that server turn on.
- **The backup solution supports bare-metal restore to dissimilar hardware**: This feature allows you to take a backup set and boot up a server that is fresh from the factory, perform the restoration directly (even if it is not identical hardware). In case of damage to the original hardware, this feature will enable you to restore your previous server to brand new hardware
- **The backup solution supports Volume Shadow Services**: Microsoft VSS is a special engine that allows backup software to capture files that are in use. VSS is supported by all the major backup software publishers, but it is important to make sure that it is in the one that you select.
- **Your solution supports encryption**: Enabling encryption is very wise, especially should your replicated or off-site media become lost or stolen.
- **It should be simple to use and easy to understand**: You may have to go on vacation, so choosing a solution that is easy to use makes it easier for those responsibilities to continue by others who aren't used to doing them. It should also be easy to understand whether it is working properly.
- If you use Line of Business Applications, **make sure that the solution can back up the data stored within it** – for instance, you may need SQL Server, Oracle, or another database integration to capture the data.

There are three very common types of backup software methods that exist today. The first and most prevalent are disk-based backups. Disk-based backups are extremely convenient and easy to use. Nearly all of them use bit-level backups to produce extraordinarily efficient backup sets and can run nearly in real time. They require no media to swap and are a "set and forget" style. They tend to require a dedicated server or hardware appliance to store the backups locally. You will also find that you will either need to pay for an archiving service or a second appliance/server altogether in order to replicate the data off-site.

The second common backup strategy is cloud only. These backup solutions will capture and send the bit-level changes directly to a cloud-service provider. Unlike the disk-based method, there is no locally stored backup, so restorations must be performed from the cloud or media requested from your provider. Cloud-only solutions are very limited but also tend to be the easiest to implement and maintain.

The final common strategy that you will see is media-based, such as RDX or tape. These old-school methods used to be extremely common, however, the cost of media tends to be quite high and the risk to forget to swap a tape or cartridge is much higher than most want to admit. That said, off-site backups are much easier with media and can be taken directly from the drive to a bank vault or safe place. With media-based backups, it is strongly recommended that you enable encryption.

Defining Your Backup Strategy

Once you have chosen a solution, much of the strategy will be outlined for you, however, you may find that questions regarding off-site storage, or backup frequency will come into play.

Choosing to backup too frequently, may cause your servers to slow down due to load put on by the constant backup. Too infrequent, however, may cause you to lose data in the event of an emergency. Consider the following when defining your backup strategy:

- **Include everything**. A backup that requires you to pick and choose what data to backup could cause problems down the road. Exceptions can be considered for temporary files or possibly downloads, but your missing download may be necessary for repair should there be an issue with the restore process.
- **Choose Backup Intervals based on how often data changes**, or as we often describe it, what is an acceptable data loss in the event of an emergency? Servers that backup every 15 minutes will cause a loss of productivity of around 15 minutes (give or take when data was updated), while a server backed up every week will experience data loss of up to a week. Your basic web server may be okay to backup weekly, but your database server should be much more frequent.
- **Where is your offsite data?** Sure, deleted files happen, but what if something happens to the server itself – or the room it resides in. Offsite backups are additional safe-havens – but make sure that they are secure and that you know how to retrieve the data in time of need (for instance, a cloud provider may be able to Next-Day-Air a hard drive with your backups, but there are often additional costs associated).

PRO-TIP: Business Continuity & Disaster Recovery

Disaster Recovery is part of a much bigger idea: Business Continuity. To learn more visit:

http://blog.lighthousesol.com/backups-business-continuity.-whats-the-difference

- **Perform a test restore:** If you can, use a test lab to tryout a full restoration of your servers to non-production equipment. This provides you not only with assurance that your strategy works, but confidence that you know what to do should the time come. If you are unable to perform a lab restore, consider creating folders with non-critical data. Delete them then restore the folder.
- **Document your strategy as much as possible:** The more you can document, the more likely you will be successful when a disaster happens. Disasters are highly stressful, but a well-written action plan can make it easier.

Consider This… Disaster Recovery Solutions	
Quest Rapid Recovery	http://www.quest.com
Microsoft Azure Backup	https://azure.microsoft.com
Storagecraft - ShadowProtect	http://www.storagecraft.com
Acronis	http://www.acronis.com
Veritas BackupExec	http://www.veritas.com
Carbonite	http://www.carbonite.com
Veeam	http://www.veeam.com

6. Monitoring Your Network

We've now got all the foundational items covered and can focus on where the majority of time spent on IT-related items – maintaining your network.

To best maintain your network, knowledge is power and the best place to gain that knowledge is by implementing a solution that enables you to monitor what is happening with your various clients is network gold. While there are many integrated solutions that you could choose to implement using Microsoft's tools, most of them require a significant amount of individual configuration and end up relying on using email. Instead, we encourage you to choose and select a tool to perform this work for you. There are many free solutions that can give you the basics, as well as reasonably priced paid for programs that can offer you some more advanced features. When looking for a solution consider the following:

- Identify important devices and determine that they are online (Uptime Monitoring)
- Eventlog Scanning
- Resource Utilization
- SNMP
- Easy deployment (either installable agent, or even better is WMI integration)
- Event Triggers & Notifications (for letting you know when something has crashed)
- Asset tracking & auditing (this is especially useful down the road for documenting your environment and software)

Consider This… Network Monitoring	
Spiceworks	http://www.spiceworks.com
PRTG Network Monitor	https://www.paessler.com
ManageEngine	https://www.manageengine.com

As a guideline, configure alerts for common things such as resource utilization and uptime monitoring – especially for servers will let you know about critical issues as they happen (and hopefully before the rest of your staff notices). You will find below a table for some common settings for thresholds.

Monitored Items	Desktop	Server
Disk Utilization	<90% used	<95% used
Memory Utilization	<95% used	<95% used
CPU Utilization (per 5 minutes)	<95%	<95%
Antivirus	Enabled/Updated	Enabled/Updated
Connectivity (per 15 minutes)	---	Present

Using the data collected by your monitoring environment, you should be able to see if there are memory and hardware deficiencies, as well as if you see many issues with a computer, make a determination that the computer should be marked for replacement. However, as powerful as these tools are, they are passive tools designed to inform, not to correct issues. To get the most out of monitoring your network, you will need to proactively review your notifications, the platform and the data it provides and determine actionable steps to resolve problems as you see them.

7. Supporting Your Network

All the tasks that we have discussed so far are designed to minimize issues that arise. There are moments, however, that you will need to correct issues that were not foreseeable. Properly supporting your network provides you with the organization and fluidity that you need to get issues resolved.

Help Desk/Issue Tracking Systems

This may sound like overkill, however, implementing a system that allows you to track issues against users and devices is extremely useful. First off, it may help you discover deficiencies in your training process. Secondly, devices with many issues on a regular basis may need re-imaged or replaced. This

data is not easily accessible if you work from just straight email or text messages and can create a hectic workflow followed up by stress and chaos. Another important key when implementing a help desk… Make your users utilize it. Feel free to explain the importance but letting them slide could prevent you from making an important decision down the road. An issue tracking system will also help you identify how much of your efficiency is being lost to IT needs, allowing you to justify hiring additional help or managed service provider.

Consider This… Issue Tracking	
Spiceworks	http://www.spiceworks.com
Freshdesk	http://www.freshservice.com
ManageEngine	https://www.manageengine.com

Desktop Support

The easiest form of desktop support is for computers that exist in the same building as you, however, you may need to implement some form of remote support capability.

VNC is an open-source, agent-based remote utility that has been around for a long time. It installs on the computer and allows you to connect from another computer with ease. It is super-simple to setup and requires no interaction from your users, however, you may find that you need a product that works across the internet. Products such as TeamViewer or using conferencing and collaboration tools such as Join.me can help you connect from anywhere with ease, though, your use case may require a subscription.

Consider This… Remote Desktop Support	
VNC	http://www.tightvnc.com
TeamViewer	https://www.teamviewer.com

8. Documentation & Reporting

One of the best things you can do for your network is maintain good documentation. There are many reasons for this, from transition of administration, to just keeping important information handy for when you or a vendor needs additional information. The type of information you choose to document is entirely up to you, but we strongly recommend that it include the following:

- Asset Inventory
- Software Inventory
- Vendor Contact List
- Procedural Documentation
- Important Logins/Password

How you store this information is also up to you, however, it should be accessible to those that need it, while hidden from those that don't. Excel is an excellent choice for this purpose, since nearly all the data can be tabular. You could also add a password to restrict, or store it in a folder with restricted permissions. Another great system could be to use OneNote – this program allows you to include tables, procedures, task lists and more from a single notebook. Did I mention that this notebook can also be shared? Sharepoint may also be a great option since you can create custom lists and store information about your network from there. The Sharepoint site could have custom permissions as well as a document repository for storing procedures and reports. Last but not least, there are certainly programs that can be purchased that maintain inventories for you, as well.

Asset Inventory

Maintaining an asset inventory will enable you to see all your hardware at a glance and allow you to make educated decisions on equipment that should be replaced, upgraded, or disposed. It can also be used for maintaining a list of owned hardware for insurance compliance purposes should anything happen to the asset or your business. How detailed you want to document is completely up to you, but consider these items as starting points for your documentation:

Name	What it is or why you should track it…
Hostname	Useful for identifying the computer by its network name
Asset ID/Tag Number	If your business assigns asset tags, this makes it easier to identify an asset in an accounting or other asset management system.
Device Type	Great for sorting/filtering and identifying the type of device (i.e. Computer, Server, Firewall, Switch, Printer/MFP, Time Clock, etcetera).
Primary User	Useful for troubleshooting or locating a device.
Operating System	Standardization and Troubleshooting
Make, Model & Serial Number	Very useful for warranty reporting, troubleshooting, as well as assisting with purchasing decisions.
Purchase/Acquisition Date	Great for determining if an asset should be upgraded, replaced, or other financial decision.
Basic Specifications	Also great for making financial decisions. Include fields like Memory, storage, special features, etc.)
Original Purchase Price & Useful Life Information	Use to track when a device should be phased out or replaced.

PRO-TIP: Hit the Ground Running

Software Inventory

Software Inventories are not just a good idea, they could save you a significant amount of time should your organization get selected for a Software Asset Management Review. This is especially likely if your organization uses Volume Licensing-based products on your systems. At the very least, you'll only need to know what the product is and how many times it is installed, but you could consider the following list:

If it sounds too daunting to create such a big document, we've created a **template** just for you that helps track lots of valuable information about your network based on the guidelines provided in this book.

Get it here:
https://blog.lighthousesol.com/creating-and-maintaining-a-successful-network

Name	What it is or why you should track it…
Product Name	For tracking based on a single product type.
Publisher Name	Useful for filtering if selected for a Software Asset Management Review.
Volume License Program	Some VL programs may be subscriptions or not count towards purchase quantities/incentives.
Agreement Numbers	For tracking entitlements and their effective date.
Entitled Licenses	The number of licenses that you are entitled to for the product.
Installed Licenses	The number of licenses that you are actually using – or the number of times the software has been installed.
Assets Licensed	Names of devices that are using the license.

Vendor Contact List

By keeping a list of vendors handy, you will always have the pertinent information at your fingertips. You can also use this list to keep track of what each vendor handles, include account numbers, notes and anything else you may find important.

While this information could be just as handy in your Outlook contacts list, storing a copy with the rest of your IT documentation will allow you to share that information should you be out of the office or unavailable to handle an issue. This empowers another person on staff to request assistance (for instance, if the internet goes out).

Name	What it is or why you should track it…
Vendor Name	Hopefully this one's importance answers itself
Account Number	The account number, if any, is useful for ensuring that you are able to get support.
Primary Contact Name	If possible, direct to a specific person that you regularly deal with.
Phone Number & Email	Phone number and email addresses allow your staff to pick based on what the priority may be.
Scope	Provide an idea of the vendor's role to servicing your organization (i.e. Internet Provider, IT help, printers, software vendor, etcetera).
When to Call/Notes	Perhaps provide situations as to when it is best to call the vendor instead of hassle with correcting on your own, or include any contract or billing information.

Procedural Documentation

There are lots of good reasons to document procedures – from bad memories to being able to employ assistance, storing a list of standard procedures in your organization can save you a lot of time and potentially even money.

Make the documentation as consistent across all procedures as possible so that anyone reading it can feel some familiarity towards it. You will also want to include specifics regarding the procedure, such as the exact version of the software you are describing to install, as well as the last edit date of the document so that the accuracy and reliability of the document can be verified.

Identify repeatable procedures in your organization and make a list. This list should be the starting point of your documentation. If you have to do it more than 3 times, you should probably document it.

Consider these common procedures:

- Creating a user
- Setting up a new computer
- Installing line of business software and/or configuring it
- Running a report
- Disabling a terminated user

Writing Documentation

As you write your documentation, split the tasks up into their simplest element and write them as steps. For instance, the following is chaining several items together and could be confusing.

1. Click on Start, go to programs, click Accessories, then System Tools and pick Remote Desktop Connection. Enter the Hostname "mycomputer" and click Connect

Instead, it is common practice that chained items with a mouse, such as navigating a menu, or using the Start menu, can be short-handed by using a right-angle bracket (">"). Separate the physical clicks and data entry into their own steps. Use formatting to call out important information but be consistent as you do.

Let us see how our example above would look:

1. Open **Remote Desktop Connection** by going to **Start > Programs > Accessories > System Tools**
2. Enter the hostname "*mycomputer*" in Computer Name
3. Click **Connect**

By simplifying the steps and including consistent formatting, it makes it easier to glance back at the step and move along the document. Adding screenshots to the steps is also a terrific way of confirming what is being seen by the reader.

For more information please contact:

Griffin Ball

Email: griffinb@lighthousesol.com

Lighthouse IT Solutions | https://www.lighthousesol.com