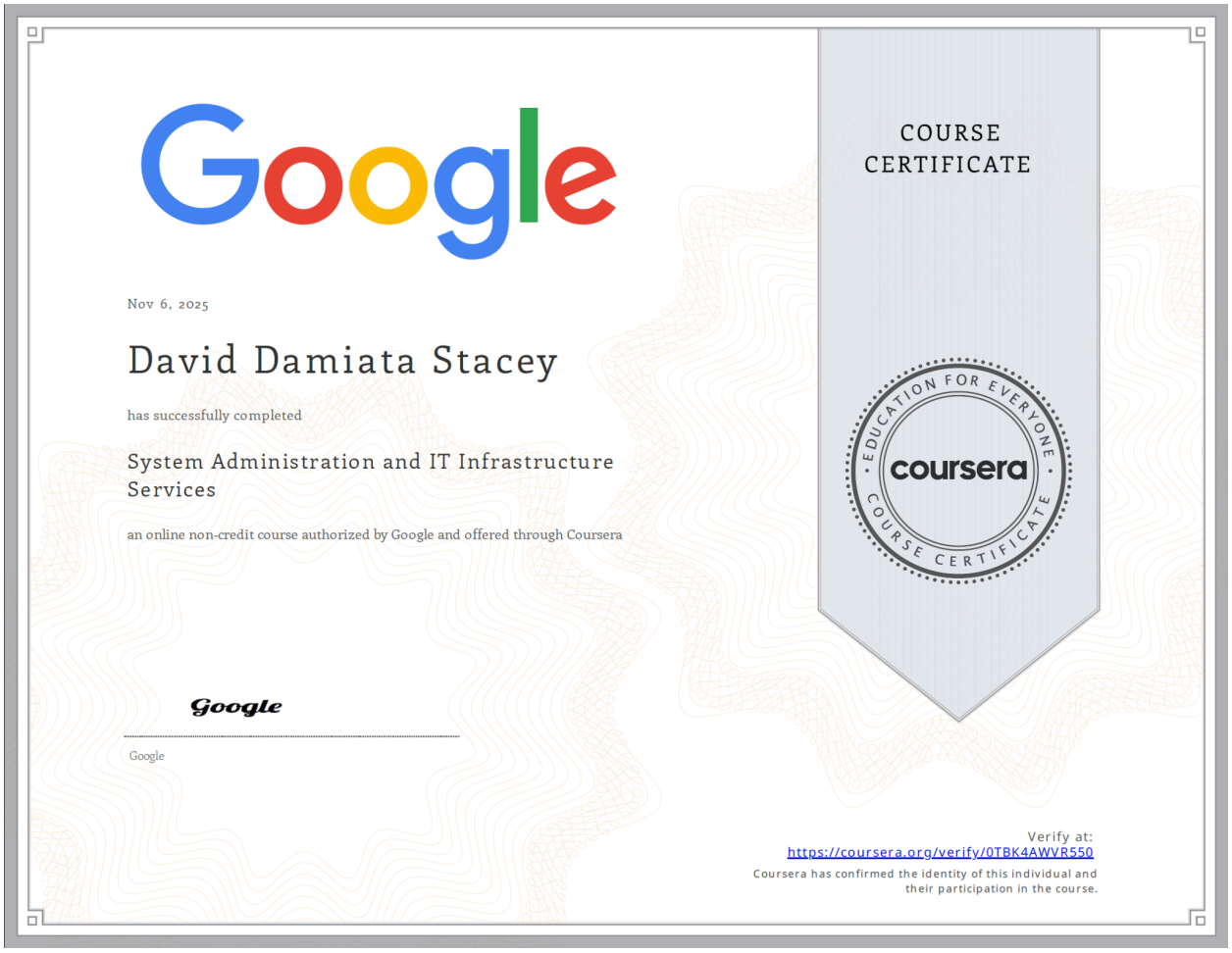
System Administration and IT Infrastructure Services

Course 4 of the Google IT Support Professional Certificate

Completed on 11/6/2025



All associated videos are within **OneDrive/Coursera/Google IT Support/SysAdmin_101**

Module 1: What is System Administration?

What is Systems Administration?

IT Infrastructure encompasses the software, hardware, network, and services required for an organization to operate in an enterprise IT environment.

Videos "**A01 Course Introduction**" - "**A09 Vendors**" cover a lot of ideas and concepts about life as a SysAdmin.

Vendor Life-Cycle for Custom Services and Products

Another important vendor life-cycle involves the engagement and management of service vendors. IT Support professionals may need to engage and/or manage service vendor relationships as part of their job responsibilities. Service vendors are often businesses that offer specialized services, products, and/or skilled labor to other businesses. Many organizations outsource business needs to these types of vendors as cost saving measures to temporarily augment staff, and to more efficiently manage company time and resources.

Hiring temporary contractors on an as-needed basis can be a disruptive, lengthy, and expensive process. Employing a full-service vendor, on the other hand, simplifies the process to a single contract agreement, allowing the vendor to assume responsibility for supplying and managing the resources necessary to carry out your project. For example, your organization may choose to outsource a company-wide computer system upgrade to a vendor that can supply a temporary IT workforce to implement the large-scale project. Using a vendor for this project may save your organization the time, expense, effort, and liability associated with hiring, training, and managing individual contractors.

Vendor life-cycle management for custom services and products

Vendor life-cycle management is an end-to-end standardization for conducting business partnerships with vendors. As a best practice for business management, organizations should develop standard policies and procedures for the procurement and management of vendors.

The standard vendor lifecycle can be categorized into three contract phases and eight management steps:

Phase one - Pre-contract

Phase one of the vendor lifecycle management process begins with an organization identifying the need to outsource a process or project to a services vendor.

1. **Vendor identification and engagement**: An organization identifies potential vendors and engages them to collect more information about the vendor's business offerings and capabilities. The organization will inform the vendors of the service needs and will solicit "requests for proposals" (RFPs), "invitations to bid" (ITB), or other similar proposal documents from the vendor. The organization will select a small number of promising proposals to analyze in greater depth. Some organizations may have official procurement officers to ensure fair and ethical vendor selections.
2. **Vendor qualification and risk mitigation**: The organization advances the shortlisted proposals to the qualification stage. In this stage, the organization and/or procurement officers request additional information from the vendor to help exclude vendors that might pose a risk to the organization.
3. **Vendor evaluation and selection**: The organization and/or procurement officers evaluate the vendor information collected during the qualification phase. The organization's vendor selection team analyzes the vendor information to determine each vendor's health and stability as a business, as well as their ability to deliver on the organization's request. Some of the data points used in this evaluation and selection may include the vendor's:
    a. **History**: Does the vendor have a clean business record?
    b. **Ratings and quality**: What are other customers saying about the vendor online and through services like the Better Business Bureau?
    c. **Expertise**: Does the vendor have the experience, skills, talent, and/or expertise to deliver on needed services?
    d. **Cost**: Will the vendor's proposal fit into the organization's budget?
    e. **Offer compliance**: Does the vendor's proposal fulfill all of the requirements of the organization's request?
    f. **Responsiveness and customer service**: How long does it take the vendor to respond to the organization's requests? What is the vendor's approach to offering timely customer service?

Once a vendor is selected, the organization will negotiate a statement of work (SoW) and contract terms with the vendor. Performance criteria, milestones, and deliverables should be well-defined in the SoW and contract.

1. **Vendor information management and onboarding**: The selected vendor goes through an onboarding process with the organization. Information about the vendor is recorded in the organization's procurement system and provided to the appropriate stakeholders for the engagement. Information management is important to the vendor life-cycle management and maintaining strategic relationships with vendors. The organization's IT department may issue IT equipment to the vendor for establishing secure and monitored connections to the organization's network. The organization might also offer vendors training sessions for the organization's relevant policies, procedures, expectations, systems, network, tools, etc.

Phase two - Contract delivery

1. **Performance management monitoring**: Organizations often assign a project manager to monitor the performance criteria, milestones, due dates, and deliverables defined in the SoW and contract. It is vital to vendor and project management to ensure the vendor is meeting the contracted expectations on time and on budget. The organization should conduct regular performance reviews and may request improvements to the vendor's performance. How the vendor responds to improvement requests is important to the business relationship and can positively or negatively affect opportunities for future engagements.
2. **Risk management**: Organizations and project managers should also monitor and analyze potential risks during the course of the vendor engagement.
    a. **Supply chain risk management**: If the vendor's product or service depends on a supply chain, contingency plans need to be in place to prevent negative impacts to the project if a disruption to the supply chain occurs. Additionally, it is important to ensure the vendor does not create compliance problems with supply chains, as this risk might impact the organization's reputation.
    b. **Product upgrade limitations and other risks**: Organizations must monitor risks related to updating, maintaining, and upgrading the vendor's deliverables. Especially important is the availability and capability of the vendor to provide these periodic updates or upgrades. Contingent plans should be defined in case the vendor cannot meet this need.
3. **Vendor relationship management**: Organizations can support their relationships with vendors by:
    a. Developing a communication plan with frequent check-ins
    b. Building and maintaining healthy partnerships
    c. Ensuring all parties benefit from the engagement

Phase three - Post-contract

1. **Vendor offboarding**: When the vendor project comes to an end, the post-contract closing process is initiated. The organization's project manager and/or a procurement officer are often assigned to facilitate the vendor offboarding. In this phase, the organization performs an analysis to ensure the vendor has met all contractual obligations. Any residual obligations, like warranties and post contract support are revisited, and sometimes revised, with the vendor and relevant stakeholders of the organization.
    a. **Warranties**: The organization should keep detailed records of any vendor or third-party warranties provided for the deliverables from the vendor engagement. All stakeholders should be made aware of the inclusions, exclusions, and expiration dates of the warranties.
    b. **Post-contract support**: The organization should keep detailed records of any services, like technical support, supplied in the post-contract phase. The organization's contract with the vendor should have a clearly defined maintenance clause or a statement that post-contract support is not included.

Finally, the organization's project manager and/or a procurement officer uses the organization's offboarding checklist to complete the post-contract closing. The checklist might include requesting the vendor return IT equipment and removing the vendor identity profiles on the organization's network. IT Support professionals might also be enlisted to ensure any intellectual property belonging to the organization is stored properly with necessary security precautions.

Vendor Life-Cycle for Support of Commercial Products

Commercial vendors of computer operating systems, software, products, peripherals, and other IT equipment plan life-cycle schedules, or product roadmaps, for supporting their products. It is important for IT Support professionals to keep track of these life-cycle schedules, especially the date when the product will reach its end of life (EOL). The EOL date is the point at which the vendor plans to end all support for the product and it is reclassified as a legacy product.

IT Support professionals should plan to update, upgrade, or replace a product before it reaches its EOL date. Once the EOL date has passed, the vendor will no longer provide technical support, security patches, or driver or firmware updates for the product. This lack of support can create a security risk for computer systems and networks. Cybercriminals take advantage of legacy products that are no longer being patched or updated. Warranties can expire on or before a product's EOL date as well. This can disrupt normal IT operations if the product fails, as IT Support professionals must expedite purchasing, implementing, and providing training for the legacy product's replacement.

The details of product life-cycle support policies vary from vendor to vendor. However, some life-cycle phases are common to most vendors:

1. **Beta testing phase**: Often, the first introduction of a vendor's product to the public occurs through a beta testing phase. Beta testing is used to collect product feedback from early adoption tech users. This feedback is used to improve the product before it is available to the general public. For example, you might be familiar with Microsoft's Windows Insider Program. Early adopters of Microsoft products can sign up to beta test the latest updates to the Windows operating systems.
2. **Product release and primary support phase**: When the beta testing phase ends and the vendor has updated and repaired reported defects, the product will then become available and marketed to the general public. It is normal for products to experience problems as a larger group of end users implements the product into their unique computing environments. Vendors respond by developing and releasing regular updates and security patches for the product during this supported product life-cycle phase. It is critical that IT Support professionals update the product regularly to prevent security breaches and other disruptions to the product's usability.
3. **Extended support phase**: Product roadmaps also include a phase-out period when vendors introduce their next generation products. The vendor normally continues support for the older product during this phase by releasing critical patches. The product is often phased out of the primary commercial market, but resellers may continue to sell it as a used or unused surplus product. Buyers should carefully investigate the warranty and support for the product if purchased from a reseller.

End of life (EOL) phase: When a product has reached its scheduled EOL date, the vendor will end support for the product. Tech support and warranties will expire. The vendor will no longer release product updates, security patches, drivers, firmware, etc., leaving the legacy product vulnerable to security attacks. Vendors encourage customers to buy the new, next generation product as a replacement for the legacy product.

Change Management

IT change management is a standardized process for planning, communicating, and implementing technical changes to information systems. IT Support professionals are often responsible for installations, updates, upgrades, migrations, etc. to an organization's software, hardware, network security policy, data storage policy, cloud platforms, and more. IT Support staff are expected to make these changes while also minimizing disruptions to the organization's IT services. By following IT change management best practices, IT Support professionals can create robust plans for change rollouts that protect business continuity. The change management plan is often reviewed by change board approvals, management teams, and/or project stakeholders for risk assessment, feedback, and plan approvals or rejections.

IT change management plans

Each organization will have their own change management policies, processes, and procedures. However, there are several common items that should be included in change management plans as a best practice. When proposing a change, IT professionals may create documentation or use change request forms to detail the following elements:

- **Person/team responsible for the change**: Names at least one person as the responsible party for overseeing the change management plan.
- **Change priority**: States the urgency of the change. For example, critical security patches would have a high priority and need to be scheduled ASAP. Whereas, a software update that merely adds new features might be a very low priority and can be scheduled for a convenient future date.
- **Change description**: Gives an overview of the planned changes. The change description should also provide a list of the planned changes. For example, if the change involves updating firmware on several router models, the description should include which routers and models will be updated. Additionally, the plan should list the old firmware versions currently on the routers along with the new firmware versions to be applied during the update.
- **Purpose of the change**: Explains why the change is necessary. For IT Support professionals, the most common reasons for changes are operating system, software, driver, and firmware patches and updates, as well as hardware and peripheral upgrades. Installations, implementations, and redesigns of software and hardware systems are also common IT changes. IT Support professionals should regularly evaluate the need for improvements and changes to network security policies and procedures. Laws, regulations, and company policies may also require changes to how organizations store, transmit, and protect data.
- **Scope of the change**: Describes the extent of the changes. The documentation should include a list of all IT systems (hardware, software, etc.), locations, departments, individuals, vendors, partners, customers, and others the changes affect, whether directly or indirectly. Any changes to policies, processes, or procedures should also be recorded.
- **Date, time, and duration of the change**: Indicates when the change is scheduled to take place and the duration of the change rollout. If the change is expected to create service outages, the person or team responsible for managing the change should inform all affected staff about the outage before the systems are taken offline. IT changes are often implemented outside of normal business hours, when systems can be taken offline with minimal disruption. For organizations with traditional Monday through Friday, 8 a.m. to 5 p.m. business hours, changes are usually planned to begin in the early evening on a Friday, after end users have logged out for the weekend. The change implementation process should include plenty of contingency time before the next business day in order to test, troubleshoot, repair, and roll-back any changes that are not successful. When an unsuccessful change occurs, IT Support professionals may need to work through the night and into the next morning. Organizations and IT departments may opt to hire a vendor to perform overnight system changes to adhere to company overtime policies and labor laws.
- **Change rollback or backout plan**: In case of primary plan failures, details a rollback plan to return the affected systems back to their original state before the changes were attempted. Additionally, a secondary or alternative plan may be included. This could be a plan to activate a failover system to replace any problemed systems until they are repaired. IT Support professionals should detail the steps involved in the rollback and/or alternative plans, including the original configuration settings and software, patch, driver, and/or firmware versions. Files needed to rollback updates and patches should be downloaded and stored in an accessible location to simplify rollbacks. Cloud-based virtual systems can be restored in seconds by simply using clones of saved previous VM states.
- **Technical evaluation**: Records the results of any testing performed on the proposed changes in a lab or sandboxed environment. The testing environment should be as similar to the target environment as possible. For example, the same operating system versions, hardware parts, drivers, firmware, etc. of the target system should be reflected in the lab/sandbox testing environment. Setting up a testing sandbox for cloud platforms should be as simple as cloning the virtual system(s) targeted for updates. The plans should also include metrics for evaluating if a change is successful or not.
- **Systems affected by the change**: Lists all IT resources (including hardware, software, networked, and cloud systems) that will experience direct or indirect changes as a result of the change rollout.
- **Anticipated impact of changes**: Describes how the planned changes are expected to impact the affected systems. For example, if the change involves adding new servers to a resource pool, the plan might describe that this increase in load capacity will result in system performance improvements and faster server response times.
- **Resources needed to implement the change**: Lists the human resources, budget, time, management oversight, subject matter expert (SME) consultations, training, equipment, hardware, software, parts, systems, tools, insurance policies, and any other resource needed to complete the planned changes.
- **Training for users impacted by the change**: Outlines any training needs to help users adapt to the changes. This might include classes on how to use new software applications, hands-on practice with new hardware, a company-wide announcement for security procedure changes, and more.
- **Risk level for change**: Describes how much risk is involved in making the proposed changes. Some changes are high risk and might cause catastrophic failures if the plan goes wrong. For example, an upgrade involving a single point of failure on a critical system could create a system-wide outage. In this case, it would be wise to implement a redundant failover system for that critical system before attempting any other changes.
- **Change instructions**: Details each step of the planned changes. This should be formatted as an instruction manual for the IT Support professionals to follow to ensure there is no guesswork involved in implementing the changes.

Change board approvals

Some large organizations may have a **Change Advisory Board (CAB)**. The CAB is a board of directors appointed to oversee all implemented IT changes in the organization. The CAB can be the official governing body to approve or deny change management plans. They may advise on needed adjustments to the plan to meet business goals or to comply with regulatory compliance criteria. The CAB may also assist with mitigating risk brought about by proposed changes.

User acceptance

Including a user acceptance process for information system changes is a best practice in IT change management. IT change management plans can include a beta testing period similar to software development user acceptance testing. This plan might include several days of testing by a select group of users to ensure that the changes have been successful and that there are no hidden surprises caused by the changes. The change management team for the plan should develop user acceptance criteria forms for the beta testers to complete. The criteria normally includes common activities that all end users should be able to perform successfully in the new or changed environment. A period of time should be reserved for fixing any problems the beta testers find. When beta testing is successful and the changes have been accepted/approved by the users, the changes should become available to all appropriate end users.

Recording Your Actions

When you are going to make changes in a machine, it's very important to have a clear plan of what you are going to do and to store the actions that you actually took.

A common practice for system administrators that work with bug queues or ticketing systems is to include the commands executed and the output obtained in the corresponding bug or ticket. This is recommended if the commands that need to be executed are few and straightforward.

However, there are situations where you don't yet know which commands exactly you'll need to execute because there's some investigation that needs to happen. In cases like that, it can be helpful to use a command like script for Linux or Start-Transcript for Windows.

script

In the case of script, you can call it like this:

```
script session.log
```

This will write the contents of your session to the session.log file. When you want to stop recording, you can write **exit** or press **Ctrl-D**. The generated file will be in ANSI format which includes the colors that were displayed on screen. In order to read them, you can use commands like ansi2txt or ansi2html to convert it to plain text or HTML respectively.

Start-Transcript

In the case of Start-Transcript, you can call it like this:

```
Start-Transcript -Path C:\Transcript.txt
```

This will write the contents of the session to C:\Transcript.txt. When you want to stop recording you need to call Stop-Transcript. The file created is a plain text file where the commands executed and their outputs are stored.

Recording Graphical Sessions

Performing system administration actions through a Graphical user interface is less common (as it's harder to automate and to perform remotely), but it's still something that may happen sometimes.
If you are going to be performing an action that needs to be done graphically and you can document what you are doing, you can use a specialized tool like recordMyDesktop for Linux, or general video tools like OBS or VLC.

Module 2: Network and Infrastructure Services

Supplemental Reading for IT Infrastructure Services

For more information on the following topics check out the following links: IaaS, NaaS, SaaS, and PaaS Providers.

For more detailed information on DaaS Providers check out Amazon here, Jumpcloud here and the Azure Active Directory here.

Supplemental Reading for Server Operating Systems

For more information on Server Operating Systems check out the link here.

Remote Connections

Remote connections can be used by IT Support professionals to troubleshoot remote systems. Remote systems may include laptops, PCs, workstations, servers, data center machines, and other IT equipment that supports remote access. Additionally, remote connections can be used for file transfers and terminal emulations. IT Support professionals often use remote access software to save time by eliminating the need to travel to the computer system's location.

Remote access software can also be used for remote and flexible work arrangements, which have been increasing in popularity in recent years. Numerous organizations have developed remote, hybrid, and flexible work opportunities to give employees the option to work from home. Through these arrangements, employers and employees have discovered the benefits of remote work. Employees save time and money by avoiding the commute to work. Employees also report an improvement in their work-life balance. Employers can save on the costs of maintaining physical offices. Employers can opt to expand their hiring pool far beyond their physical locations by hiring talent in other cities, regions, states, or even countries.

Multiple surveys have revealed that up to 95% of employers and employees in the United States would like to keep remote, hybrid, and/or flexible work options permanently. Recently, Microsoft reported that 66% of employers around the world are adapting their workplaces to support hybrid work models (see the Resources section at the bottom of this reading for more information). Given this workplace transformation, organizations are likely to ask IT Support professionals to design, configure, manage, and/or troubleshoot remote connections for business networks.

Remote access software for IT management

Unlike RDP and VPN, there are some types of remote access software that are typically used only by IT management and other computer support professionals. These remote applications help IT Support teams manage and monitor large networks more efficiently.

- **Secure Shell or Secure Socket Shell (SSH)**: SSH is a network protocol and suite of tools that can be used to establish a secure connection between a computer and a private network over the internet. SSH is included with Linux/Unix and Mac Server operating systems. SSH provides identity and access management protocols through robust password authentication and public key authentication. SSH also encrypts data transmissions over the internet. Sessions are established by using an SSH client application to connect to an SSH server. For security, SSH keys are used to provide single sign-on (SSO) services and to automate access to servers for running scripts, backups, and configuration tools. SSH is primarily used by IT Support professionals to remotely manage file transfers and terminal emulators on Linux/Unix systems. For example, IT Support staff can use the SSH network protocol tool to establish an encrypted tunnel from their computer to a remote server over a network. The SSH file transfer tool can then be used to transfer a file, like a firmware update package, to the remote server. Finally, the SSH terminal emulator can be used to issue command lines to install the firmware onto the remote server.

Remote Monitoring and Management (RMM): RMM is used by IT Support professionals to remotely monitor and manage information systems. Implementing RMM involves installing an RMM agent on each endpoint within a network, including servers, workstations, and mobile devices. The agents then send periodic status reports about the health of each endpoint to IT Support staff. RMM tools also help IT Support professionals proactively maintain the network by facilitating the remote installation of security patches and updates. If a problem occurs on an endpoint, the RMM agent will create a ticket, classify the problem type and severity, and then forward the ticket to IT Support staff. RMM systems enable IT Support providers to improve efficiency in information systems management. IT Support providers can manage and even automate routine maintenance for multiple endpoints simultaneously through a unified RMM dashboard.

Remote access software

End user remote connections to business networks can be established using remote access software. IT professionals can also use this software to manage business networks remotely. There are multiple options available for remote access software, each with their own benefits and disadvantages. The following list provides a few options for various uses, workforce sizes, and network environments:

- **Remote Desktop Protocol (RDP)**: RDP is a remote protocol developed by Microsoft. It is compatible with most Windows and Mac operating systems. An RDP solution may work well for flexible or hybrid work environments where employees split their work schedule between being physically in the office and working remotely. With RDP, end users can remotely access the physical computers housed at their offices, in addition to the desktop, software, files, and network access available to those systems. IT Support professionals can also use RDP software to troubleshoot, repair, patch and update end user computers without needing to be in the same room as the PCs.

RDP works by encrypting and transmitting the user's desktop, data, keystrokes, and mouse movements over the internet. Users may notice delayed responses to their keystrokes and mouse activity during the transmission process. RDP creates a dedicated network channel and uses network **port 3389** to transmit this information using the TCP/IP protocol standard. Unfortunately, using a single dedicated port creates a security weakness that cybercriminals can target for on-path attacks. Further, RDP does not enforce strong sign-in credentials, which leaves RDP systems vulnerable to stolen credential and brute force attacks.

- **Virtual Private Network (VPN)**: VPNs are often described as private tunnels through the public internet. Organizations can use VPNs to create encrypted connections over the internet between remote computers or mobile devices and the organizations' networks. VPNs can be implemented as software running on networked servers or on network routers with VPN features enabled. When the employees remotely connect to their VPN, they are able to access their organization's network as though they were physically in the office, eliminating the need to travel to the office in person. VPNs work well for small to medium sized organizations, but may not be adequate for large enterprises. Additionally, VPNs might not be the right solution for organizations that need to provide restricted levels of network access to groups like contractors or vendors.

Third party tools

- **Integrated video conferencing, screen sharing, and desktop management apps**: Video conferencing apps like Google Meet, Zoom, Microsoft Teams, Skype, etc. are growing in popularity as remote work tools. Video conferencing allows two or more people to meet "face-to-face" in a virtual environment. Some video conferencing apps also offer screen sharing tools, remote desktop control, polling tools, text messaging, meeting transcripts, webinar management options, the ability to record meetings, and more. The growing popularity of these tools for remote work has also invited an increase in related security attacks. Fortunately, the major providers of video conferencing software continuously update and patch their applications in response to these attacks.

- **File sharing and transfer platforms**: Cloud storage platforms, like Google Drive, Microsoft OneDrive, and Dropbox, have largely replaced file transfer protocol (FTP) tools. File sharing through a cloud platform provides the benefits of asynchronous file transfers, file transfer and data encryption, customizable security and authentication settings, and the ability to file share with multiple users simultaneously. File owners can share individual files, folders, or entire drives. However, cloud storage might not be an appropriate option for organizations affected by certain privacy laws, regulations, or other security concerns. These organizations can still use FTP applications based on SSH or HTTPS protocols for secure file transfers over the internet.

Resources for more information

- How to use Remote Desktop - Walkthrough from Microsoft on how to use Remote Desktop to connect to a remote Windows 10 or 11 computer from a device running Windows, Android, or iOS.
- The Next Great Disruption Is Hybrid Work—Are We Ready? - Microsoft's Work Trend Index report on global workplace trends regarding hybrid work environments.
- Remote Work Stats & Trends: Navigating Work From Home Jobs - Provides findings from multiple surveys about attitudes and growing prevalence of remote work.

Module 3: Software and Platform Services

Module Introduction

Software Services
Services that employees use that allow them to do their daily job functions.

Platform Services
Provide a platform for devs to code, build and manage software applications.

IRC (Internet Channel Relay)
A protocol that's used for chat messages, primarily used in the 90's.

OpenIM Protocols
Widely used and integrated into different communication applications.

XMPP (Extensible Messaging and Presence Protocol)
An open source protocol used in instant messaging applications and social networking services.
- Pidgin and ADM are examples

Supplemental Reading for Chat Communication Services
For more information on Paid for chat applications click here and for Open IM chat applications click here.

Spam Management/Mitigation

Spam is defined as any unsolicited message or call that is sent to a large number of recipients. Spam is a prevalent security concern for organizations. Cybercriminals use spam to steal important information from victims. Excessive spam can slow down mail servers and even cause the servers to crash. IT Support professionals must know how to mitigate and manage spam problems.

Types of spam

There are several different types of spam. Some spam is mass marketing from legitimate businesses. Legitimate spam is simply a nuisance, especially when it is unsolicited. Other spam can be malicious and criminal.

- **Phishing emails** attempt to trick recipients into providing personal information, credit card numbers, login credentials, etc. One famous phishing racket is the Nigerian royalty scam that asks victims to help a member of a royal family to move a large amount of money out of Nigeria. The story includes an excuse for why the royal person cannot do this for themselves and needs the victim's assistance. The cybercriminal requests the victim's bank account information for the purpose of wire-transferring the fictional royal money to the victim's account. However, the cybercriminal drains all of the money from the victim's bank account instead.

  Phishing emails can also include clickbait links, which offer the victims something enticing, such as celebrity gossip, tabloid scandals, lottery winnings, etc. Cybercriminals even use spam to lure in victims by appealing to people's vices. Once the recipient clicks on the emailed clickbait link, they become victim to a number of malicious attacks. The attacks can include exposure to malware, ransomware, viruses, keyloggers, trackers, information phishing, and more.

- **Text spam** is another method used by cybercriminals to send phishing scams. Text message spam is normally less elaborate than email spam. The texts often contain a brief clickbait message followed by a link.
- **Email spoofing** is a type of phishing where emails appear to be from reputable companies, like banks, well-known brand names, government agencies, charities, etc. The "From" address of spoofed emails is forged to look like it came from the reputable company. Additionally, spoofed emails often use stolen company logos, verbiage, and formatting to appear authentic. A couple of common email spoofing scams include:

    - **Fake job opportunities** - Cybercriminals send emails with fake job opportunities and ask victims to provide all of the personal information that is normally requested in a job application and background check. This data may include the victim's social security number, government-issued ID info (e.g., driver's license or passport), current and former addresses, current and former employers, etc. The goal of the cybercriminal is to obtain all of the information needed to steal the victim's identity.
    - **Fake credit card charges** - Cybercriminals send emails that appear to be purchase receipts or alerts stating a business will be charging a large amount of money to the victim's credit cards for items the victim never purchased. The goal is to get the victim to reply or call a fake customer service line listed in the email to dispute the charges. The cybercriminal, posing as a customer service representative, asks the victim for their personal and credit card information to look up the bogus charge and pretend to cancel the fake order. Then the cybercriminal will either use the stolen credit cards or sell the victim's credit card information on the black market.
- **Tech support scams** are used to trick people into creating a security weakness for cybercriminals to hijack their computers. The cybercriminals introduce themselves as technical support for Microsoft, Dell, or other well-known computer companies. They claim that the victim's computer has been sending the company alerts about some type of fictional computer problem. The cybercriminal will direct the victims to change system settings or even set up remote sessions for the cybercriminals to change the settings themselves. The changed system settings open a door for the cybercriminals to hijack the computers to steal information, install ransomware or malware, or even to use the victims' computers as a vehicle to commit other crimes.
- **Call spam or robocalls** mimic telemarketing-type calls to collect personal information, bank or credit card numbers, and other criminally useful data from victims. Robocalls are also used to test databases of phone numbers to determine which are legitimate numbers. The phone numbers that are answered by a live human are sold to telemarketers as customer leads or on the black market to cybercriminals, who use the numbers as lists of potential victims.

One of the largest spam call scams was based out of India where 700+ employees in a call center in India were arrested or detained for impersonating the United States Internal Revenue Service (IRS). This criminal organization targeted Americans with phone calls claiming that the victim owed back taxes to the IRS and must pay hundreds or even thousands of dollars immediately to avoid arrest. The criminal organization stole up to $150,000 USD per day using this extortion scam.

Spam mitigation and management solutions:

Fortunately, many cloud platforms offer services and tools to help minimize these types of attacks. The following security measures are offered by platforms like Google Workspace. Google Workspace Administration Help guides are listed with each item below. These guides provide more information, as well as the instructions for implementing these security measures in Google Workspace.

- **DomainKeys Identified Mail (DKIM)**: Helps to protect victims against phishing, email spoofing, and other email spam by preventing sender address forgery. DKIM attaches a header that contains a cryptographic private key to each email sent. This key is used to verify the identity of the sender and to detect if the email message was manipulated while in transit across the internet. Receiving email servers will usually designate emails without legitimate DKIM keys as spam. For more information and instructions to implement DKIM in Google Workspace, please see the article: Help prevent spoofing and spam with DKIM
- **Sender Policy Framework (SPF)**: Used to control which domains, email servers, and IP addresses can send emails for an organization. SPF is examined by the receiving email servers to verify that the domains, email servers, and IP addresses from incoming emails are from approved senders. For more information and instructions to implement SPF in Google Workspace, please see the article: Help prevent spoofing and spam with SPF
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC**): Defines how the receiver should treat email messages depending on the results of DKIM and SPF checking. For more information and instructions to implement DMARC in Google Workspace, please see the article: Help prevent spoofing and spam with DMARC

Resources for more information

- Stop Unwanted Robocalls and Texts - The United States Federal Communications Commission offers tips for stopping robocalls and phone scams.
- 10 tips on how to help reduce spam - Microsoft's tips on how to handle email spam. Some items suggested are specific to Microsoft Outlook.
- How to stop spam texts: 8 do's and don'ts - Norton's advice on preventing attacks from spam texts. Some of the methods listed for combating text spam are specific to the United States.

Supplemental Reading for File Services

For more information on File services check out the link here.

Supplemental Reading for Network File Storage

For more information on SMB click here and for NFS server software click here.

Mobile Synchronization

Mobile devices present some challenges for IT professionals. Mobile devices are easily lost, damaged, or stolen. With mobile synchronization, an IT professional can easily restore all the data stored on a lost or damaged device to a new device. This reading covers mobile synchronization on devices for collaboration with productivity platforms.

Mobile synchronization as backup

Most mobile OS platforms have built-in ways to backup mobile data to the cloud. For detailed steps on how to back up an Android or iOS device click below:

- Back up or restore data on your Android device
- How to back up your iPhone, iPad, and iPod touch

These backup methods help preserve the data carried on a mobile device and exchange it with other devices. They preserve the key types of data that a user wants to have backed up:

- App data
- Call history
- Contacts
- Settings
- SMS messages
- Pictures and videos
- MMS messages

As a backup method, mobile synchronization allows an IT professional to move the user's data seamlessly to a new device.

Mobile synchronization for collaboration and productivity platforms

Mobile synchronization is essential to today's collaboration and productivity platforms, such as Microsoft 365 and Google Workspace. These are account-based platforms that allow the user to link familiar productivity software and apps to a particular user or company profile. This way one username and password connects the user to the files, photos, people, and content needed to sync across different instances of the software or app.

Sync Microsoft 365 to a mobile device

To sync Microsoft 365 to a mobile device, the user needs to have a Microsoft account. With a Microsoft account, a user can set up Office apps and email on an iOS or Android mobile device. This setup process typically involves installing and setting up the Outlook mobile app for email, and the Office mobile app for other Microsoft tools, like Word, Excel, and PowerPoint. The following link provides detailed guidance on how to set up these capabilities on a device:

1. Set up Office apps and email on an iOS or Android mobile device
2. Use apps provided by Microsoft to sync the account with your device (consult your app store to find apps developed by Microsoft).

Sync Google Workspace to a mobile device

To sync email, calendar, and contacts using Google Workspace on an iOS or Android mobile device:

1. Set up Google Workspace on a device
2. Use apps provided by Google to sync the account with your device (consult your app store to find apps developed by Google).

To ensure that users have the most up-to-date information it is important to synchronize mobile devices on a regular basis.

Key takeaways

Mobile synchronization allows for data to be recovered if a mobile device is lost or damaged. It also ensures users have the most up-to-date information on any platform they use.

- Mobile OS platforms have built-in ways to backup the data carried on your mobile device and exchange with other devices.
- Account-based platforms link familiar productivity software and apps to a particular user profile. One username and password syncs files, photos, people, and content across different instances of the software or app.

Supplemental Readings for Mobile Synchronization

Check out the following links for more info on setting up device backups to the cloud:

- Android
- iOS

Print Services

IT professionals are often responsible for adding and updating printer drivers and settings. This may occur when a printer is added to a network, moved to a new location, or there is a software update. Along with updating drivers and settings on printers, IT may also be responsible for adding network printers to employee computers. Correct printer configuration saves time, supplies, and effort. This reading covers printing languages, basic printer configuration settings, printer sharing, printer security, and network scan services.

Printing languages

When choosing a print driver or troubleshooting issues with one, it is important to know which printing language the printer and computer operating system are using. Printing languages describe images on a screen to a printing device, so the printed output matches what is on screen. Printing languages are also called page description languages. Two of the most common printing languages are Printer Control Language and PostScript.
Printing languages can be either device-dependent or device-independent. Device-dependent means both the printer and computer are responsible for creating parts of the printed data. Device-independent means that the computer is solely responsible for creating the printed data. It is helpful for IT to know if the printing languages used are device-dependent or independent as it can help them troubleshoot whether printing errors are occurring because of the driver on the computer or the printer's hardware.

Printer Control Language (PCL)

Printer Control Language (PCL) is a printing language created by Hewlett-Packard that is used by many printer brands and computer operating systems. PCL is printing device-dependent because both the printer and computer are responsible for creating parts of the printed data. Because PCL is device-dependent, the output may not be the same on every printing device.

PostScript (PS)

PostScript was created by Adobe and is a printing language used by many printer brands but most commonly used in Macintosh systems. Unlike PCL, PostScript does not use the printer to create data. PostScript is device-independent, and the output is the same on any printer. If an error arises when PostScript is used, then it is usually an error with the driver on the computer.

Basic printer configuration settings

Configuration settings tell a printer how to complete a print job including the size, type of paper, number of sides, and use of color. IT professionals help employees change and select the correct settings for their document. The following are basic configuration settings that can be adjusted using printer settings.

- Orientation is the direction in which a document is printed. The main options for most printers are portrait (vertical) and landscape (horizontal).
- Print Quality refers to the level of detail that both the paper and the print settings are set to. The higher the DPI (Dots Per Inch), the higher the resolution or quality of the print.
- Tray settings tell the printer which tray of paper to use for the print job. Different trays can hold different paper sizes and types. Telling the printer to select paper from the correct tray ensures that the document is printed as it was designed.
- Duplex allows for printing on both sides of the paper. Printers can print information on one side (simplex) or both sides of the paper. Many brochures, booklets, and packets are printed on both sides to save paper.

For more information on how to update printer settings for high-quality printing see the article in the reference section below.

Sharing a printer on a network

Printers can be shared on a network allowing multiple computers to access one printer across the network instead of having to be wired to the computer directly. IT professionals maintain and set up networks that include shared printers. For more information on sharing printers on your network read the article in the reference section below.

Network scan services

Network scan services allow a printer with scanning capabilities to create a file of a scanned image and upload or send it to a location on the network or in the cloud, or attach the file to an email and send it. Employees often need IT support for ways to use this type of technology. The following network scan services can be used for fast file uploads or attachments.

- Email scan service allows a document to be scanned directly from the printer to email.
- Server Message Block (SMB) protocol allows a document to be a shared resource once scanned by the printer.
- Cloud services enable a document to be scanned from the printer and uploaded directly to the cloud.

Printer security

Printer security protects access and tracks the activity of a print device. Printer security aims to ensure that only authorized users can use a printer. Setting up and monitoring proper security permissions falls under the job of an IT professional.
Some basic measures for limiting access to printers and tracking print activity are:

- User authentication commonly requires a user to enter a username and password before completing the print job.
- Badges are usually a physical card a user must scan at the printer to complete the print job.
- Secured prints require a user to enter a user-created code at the printer to complete the print job.
- Audit logs track users that have accessed the printer, including the date and time of use.

Key takeaways

IT support professionals are often responsible for printer management. It is helpful to know about printing languages, printer configuration, networking, and security.

- Printer Control Language is device-dependent, while Postscript is device-independent.
- Some basic printer configuration settings are orientation, print quality, tray settings, and duplex.
- Having a printer on a network enables multiple users to share printers.
- Network scan services allow a printer with scanning capabilities to create a file of a scanned image and upload or send it to a location on the network, on the cloud, or email.
- Printers have security and tracking features such as user authentication, badges, secured print, and audit logs.

Resources for more information

For more information about software and driver downloads for specific brand devices, review the links below.
HP Customer Support - Software and Driver Downloads
Cannon Customer Support - Software and Driver Downloads
Xerox Customer Support - Software and Driver Downloads
Ricoh Customer Support - Software and Driver Downloads
HP - How to Update Printer Settings for the Highest Quality Printing
Microsoft Support - Share your network printer
Xerox - Scan a Document to an Email Address
HP Customer Support - Set up Scan to Network Folder
Dell - How to Configure Your PC or Server for SMB (Server Message Block) Scanning on Dell Laser Printers
Xerox - Scan to Cloud or Enable Remote Destination

Supplemental Reading for Print Services

Printers

Sometimes you just need to create a hard copy of something on a computer. You need to be able to pass it around, mark it up, or store something as a physical copy. This is where a printer comes in! Printers work in a lot of different ways. In each case, the printer uses some type of printing technology to apply an image to a printing substrate such as paper, plastic, cloth, or just about any sort of surface you can imagine!

Printer technologies

Over time, many types of printing technologies have been developed. Here are some of the most common types:

Inkjet printers use arrays of very small nozzles to spray ink onto the printing substrate. These are very versatile printers that can print onto a lot of different surfaces.
- https://computer.howstuffworks.com/inkjet-printer.htm

Laser printers use a laser to draw an image in static electricity on a photosensitive drum. The statically charged image on the drum attracts a powdered pigment called toner, which is transferred onto the paper and fused in place!
- https://computer.howstuffworks.com/laser-printer.htm

Impact printers work sort of like a typewriter. A dot-matrix printer, for example, has an array of small pins that press against the paper through an inked ribbon. Dot-matrix printers used to be very common, but now are only used in special situations. One example of this is when you need to print on carbon (or carbon-less) copy paper. Thermal printers apply heat to special thermochromatic paper. Thermochromatic paper changes color when it is heated, so thermal printers don't require any ink! Thermal printers are very commonly used as receipt printers. 3D printers don't apply an image to a substrate. 3D printers slowly layer small amounts of material at a time to create 3-dimensional objects! There are a lot of types of 3D printing technologies, and you need not only drivers, but other special software to build the instructions for your specific 3D printer.
- https://3dinsider.com/3d-printer-types/

Viewing your printers

To see what printers are already installed in your operating system, navigate to the OS's printer settings. You can also add new printers, and manage existing printers from there.
- In Windows, you will go to one of two places, depending on the version of Windows that installed. You will go to either **Settings > Devices > Printers & Scanners, or to Control Panel > Printers and Devices.**
- In MacOS, navigate to **System Preferences > Printers & Scanners.**
- There are a lot of different utilities for configuring printer settings in Linux. Take a look at the documentation for your version of Linux to be sure. Just as an example, for one common distribution of Linux, Ubuntu, you will navigate to **Activities > Printers.**

Each printer in your OS has a print queue, or print spool. If you send multiple print jobs to a printer, those jobs will line up in the queue to be handled, one at a time. Print jobs can be reordered or cancelled while they are in the print queue.
- Windows - View the print queue
- MacOS - Use the Dock on your Mac to check on a printer or print job
- Ubuntu - Cancel, pause or release a print job

Your operating system will have a default printer. If you only have one printer, then that will be the default printer. If you have multiple printers configured, then you can select one to be used, well, by default!

- Windows - How to set a default printer in Windows 10
- MacOS - Change the default printer or a printer's name on your Mac
- Ubuntu - Set the default printer

Installing a printer

Printers can be pretty complicated devices, with lots of settings. There are dozens of common printer brands and thousands of printer models. Your operating system has a printer service, and knows how to talk to many printers, but it might not know how to talk to your printer. Operating systems have generic printer device drivers that will work for many common styles of printers. Beyond this, major operating systems will also understand how to search catalogs of device drivers in order to find the correct driver for a given printer. If your operating system does not automatically locate a driver for the printer you are trying to install, then the best place to look is on the printer manufacturer's support website. Remember, device drivers are specific to your operating system, so be sure to use the correct drivers for your OS.

- Windows - How to install a printer in Windows 10
- MacOS - How to add a printer on your Mac
- Use your Mac to print to a printer connected to a Windows computer
- Ubuntu - Printing

One thing you may notice when you are looking at printer device drivers is that some printers can speak more than one page description language. The most common of these languages are PostScript (PS), and Printer Command Language (PCL). Some printers will work better with one language than another. Most of the time, whatever is default or recommended by the printer manufacturer is what you should go with. Sometimes, the applications that you are printing from will prefer one language over another. If your printer supports multiple languages and it is failing to print certain documents, or failing to print from certain applications, you might try a different language.

Virtual Printers

What do you do if there is an important document that you want to save, but you don't need a paper copy? You can use a virtual printer. A virtual printer is a printer driver that looks like a real printer to the operating system, but instead of printing print jobs onto paper, it creates a file! Virtual printers have names like "Print to PDF", or "Print to File". You can use virtual printers to create documents like PDFsor XPS files, or just about any type of image file!

- Microsoft XPS Document Writer
- Save a document as a PDF on Mac
- Ubuntu - Print to file

Printer Sharing

What if you have a printer attached to your computer, and you want to share that printer with someone who is using a different computer? You can! You can share your printer! When you share your printer, you are making it available to other computers as a shared printer. With a shared printer, other computers will send print jobs across the network to the computer that is attached to the printer. Take a look at these instructions on how to share your printer, and connect to the shared printer:

- Windows - How to share your network printer
- MacOS - How to share your printer on Mac
- MacOS - How to add a printer on Mac

Network Printers

Some printers can be directly attached to the network without having to be shared by a computer's operating system. These are standalone network printers. You can add network printers to your computers in a very similar way as a shared printer:

- Windows - How to install a printer in Windows 10
- MacOS - How to add a printer on Mac
- Network printing from Ubuntu

Watch out! Some network printers contain hard drives or other storage that are used to hold jobs in a print queue. This storage can end up holding on to some pretty sensitive information! Make sure to control access to this storage. Destroy the storage or securely delete any data from this storage before servicing, selling, or disposing of a network printer!

Print Servers

What if you have just a few printers, and a several people who need to share those printers? You might need a print server! Print servers work similarly to a local printer share, but on a larger scale. They can accept many print jobs at once, and will queue or spool the print jobs so they can be processed one at a time by the printer(s).

- Print and Document Services Overview
- Ubuntu - CUPS Print Server

Load Balancers

In this reading, you will learn about load balancers and their importance in cloud computing. You will become familiar with load balancing components and the benefits of utilizing load balancers.

IT Support professionals who manage cloud environments and/or physical servers in enterprise networks will likely need to configure, manage, or troubleshoot load balancers. Load balancers monitor and route network traffic flowing to and from a pool of physical or virtual servers. Load balancers can be hardware (e.g., load balancing routers) or software (e.g., Citrix ADC Virtual Platform). Load balancers distribute the traffic evenly, or by customized rules, across multiple servers. This function maximizes server performance and prevents the flow of traffic from overwhelming any one server and its resources. Basic server resources normally include CPUs, RAM, and network bandwidth. Servers can also offer other resources, like applications, file servers, database services, and more.

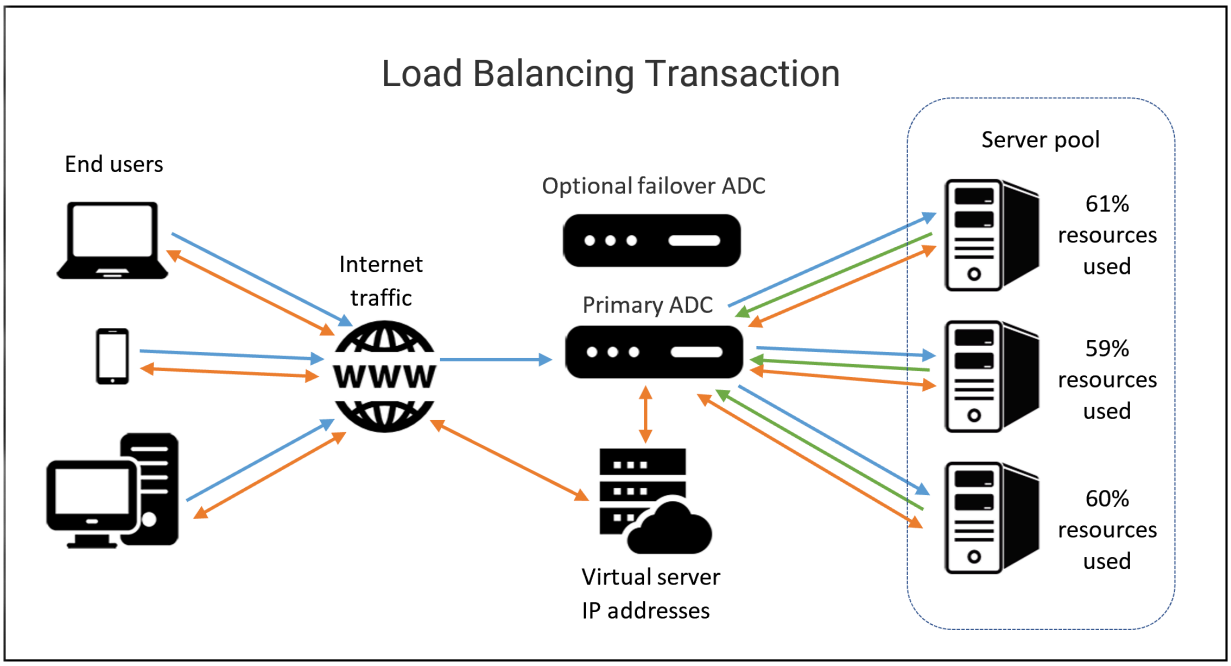
Load balancers can also detect when a server has failed and can reroute and balance network traffic across the remaining servers. This important business continuity and reliability function is often referred to as high availability. Additionally, load balancers provide IT Support professionals with the ability to add and remove servers to the pool as needed.

Load balancing terminology

The following short glossary includes some common terminology for several concepts related to load balancers:

- **Client**: A computer or program that sends requests to a server. For example, a client could be a browser that requests a web page from a web server. It could also be a workstation requesting a file from a file server.
- **Host/node**: A physical or virtual server that receives network traffic from an **Application Delivery Controller (ADC)**. The server is identified by its IP address. Whether the server is called a “host” or a “node” depends on the terminology used by the vendor of the load balancing solution.
- **Member**: A host/node that receives network traffic on a specified TCP port. The host/node is identified by its IP address plus the TCP port of the app that should receive network traffic.
- **Pool/cluster/farm**: A grouping of hosts/nodes or members that offer similar services, such as application or web services.
- **Application Delivery Controllers (ADC)**: Physical appliances, virtual appliances, or software that provide load balancing services by managing traffic between clients and host/node or member pools. ADCs can also provide other important services such as security and encryption.
- **Path-based routing**: Routes network traffic based on URL paths.
- **Listener**: A software process that checks network traffic for client requests and forwards them to target groups.
- **Open Systems Interconnection (OSI) model**: Model that depicts the seven layers of computer data communications: 7-application, 6-presentation, 5-session, 4-transport, 3-network, 2-data, and 1-physical.
- **Front end**: In load balancing environments, the front end can include the ADC system and any virtual servers that act as proxies for client communications with the ADC system and the back end servers.
- **Back end**: In load balancing environments, the back end normally includes the pool/cluster/farm systems. The back end can also include disk storage systems.
- **Distributed applications**: Software stored on cloud platforms or physical servers that can run on multiple networked computers at the same time.
- **Containerization**: Isolated runtime environments that can deploy and run distributed applications through application virtualization. This method is faster and is more scalable than older load balancing solutions.
- **Availability Zones (AZs)**: Regional data centers that host cloud platforms and are configured for high availability.
- **Elastic Load Balancer (ELB)**: Enables the use of more than one Availability Zone.
- **SSL/TLS**: Network protocols for encrypted communication.

Example ADC process for load balancing



The following steps are an example of one possible load balancing configuration using an ADC solution:

1. [Blue arrows] The client sends a connection and an information request to the ADC service.
2. [Blue arrows] The ADC listener detects and accepts the connection. Then the ADC load balancing service analyzes the best host (or member) routing path for the client request. The ADC changes the destination IP to the address (and possibly the TCP port) of the selected host (or member).
3. [Green arrows] The host or member approves the client connection and routes a response to the client through the ADC.
4. [Orange arrows] The ADC changes the source IP (and TCP port, if applicable) to a virtual server IP (and port) before forwarding the response to the client. The clients will continue to use the IP address of the virtual server for further communications.

Load balancing types

- **Application Load Balancer**: Operates at the **application** layer (HTTP and HTTPS) of the OSI model. Application load balancers also scan traffic for HTTP errors and coding bugs, as well as guard applications against distributed denial-of-service (DDoS) attacks.
- **Network Load Balancer**: Operates at the **transport** layer (TCP/UDP) of the OSI model. Network load balancers can route millions of client requests per second and handle volatile workloads. Network load balancers also support static IP addressing and containerization, among other services.
- **Classic Load Balancer**: Can operate at either the **application** layer (HTTP/HTTPS) or the **transport** layer (TCP/SSL). Classic load balancers use fixed ports for communication.
- **Gateway Load Balancers**: Operates at the **network** layer (IP) of the OSI model. Gateway load balancers have listeners on all ports that scan every IP packet in the network traffic and route each request to the target pools, as defined by the listener configuration. A gateway load balancer is the only point of entry and exit for network traffic.

Load balancers in cloud environments

In cloud environments, load balancing across virtual servers is configured through the cloud platform. A few of the load balancing options offered by several top cloud platforms include:

- **Google Cloud**: Google offers an array of options for load balancers, such as application and network level load balancing, software-defined load balancing, multi-region failover, and seamless autoscaling. Google Cloud also offers external, internal, global, and regional load balancing. For security measures, the load balancers are integrated with Google Cloud Armor, which protects against distributed denial-of-service (DDoS) attacks.
- **Amazon Web Services (AWS)**: AWS offers three ELB solutions: an Application Load Balancer, a Gateway Load Balancer, and a Network Load Balancer. AWS ELBs provide security through user authentication, certificate management, and SSL/TLS decryption.
- **Microsoft Azure**: Operates at the **transport** layer of the OSI model. Azure load balancer is the only front end point for accepting client requests to route to the back end server pools. The backend pool may

consist of Azure Virtual Machines (VMs) or instances running in Azure virtual machine scale sets. Azure offers public load balancers for internet traffic and private/internal load balancers for private virtual networks. Azure's Standard load balancer uses the zero trust security model.

Load balancers in physical environments

In physical environments, such as server rooms and data centers, load balancing can be configured across multiple servers with operating systems like VMware. Network traffic loads can also be configured for smaller environments across two servers in a physical active-active cluster. In active-active clusters, both servers actively handle network traffic simultaneously.

Supplemental Reading for Database Admin Jobs

For more information on Database Admin jobs click here and for Database types click here.

Supplemental Reading for Troubleshooting with Developer Tools

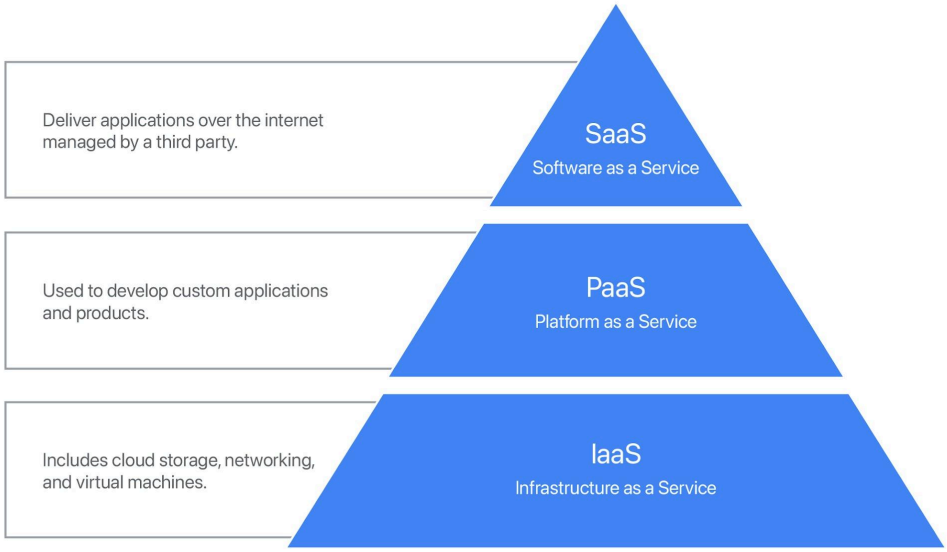
For more information on Chrome Developer Tools click here and for a list of HTTP status codes click here.

Common Cloud Models

The cloud is a part of everyday life in the modern internet world. It gives users a place to work, access, and store data from any system plugged into the cloud. Being able to work with the cloud is a vital skill in IT. This reading will cover common cloud services and four types of cloud computing.

Types of cloud services

Companies use cloud services to provide access to internal tools, develop software, store data, and more. The three primary cloud services are Software as a service, Platform as a service, and Infrastructure as a service. The Google Cloud Platform is a prime example of a system that employs all three types of cloud services.



Software as a Service (SaaS)

SaaS providers allow users to use their software with an internet browser or application instead of having to download software to a specific device. Users access information from any device through a login. The SaaS vendor stores all user data and files online instead of on the user's physical equipment. SaaS typically uses a subscription model for its services. Hacking is a concern when using this service since the full-service run in the cloud.

Platform as a Service (PaaS)

PaaS offers computer hardware and software in the cloud that allows users to develop and deploy applications or cloud based services. PaaS makes buying, developing, configuring, managing, and installing software and hardware unnecessary.

Infrastructure as a Service (IaaS)

IaaS provides an IT infrastructure to a company over the internet and on-demand. IaaS provide access to things like virtual machines, containers, networks, and storage. This service reduces the need to purchase expensive hardware. IaaS allows companies to centralize infrastructure for faster disaster recovery.

Additional cloud services

The following cloud services are more narrow in focus and are designed to solve unique problems.

VPN as a Service (VPNaaS)

VPNaaS secure networks through a cloud-based connection between the employee and the organization's network. Using this approach eliminates the need for a physical VPN endpoint.

Function as a Service (FaaS)

FaaS is an event-based service that lets developers do the building, running, and managing functions directly in the cloud without needing to maintain a server. Event-based systems use an event, such as a website click, to trigger communication within a system.

Data as a Service (DaaS)

DaaS provides data access as a service to a business. It manages the data companies generate and uses APIs to deliver data from various sources on demand. DaaS allows companies to organize and access the data they need. DaaS monetize by providing access to data. By increasing accessibility to data, DaaS can lower the cost of data-driven decision making, remove personal bias in data collection, and innovation.

Blockchain as a Service (BaaS)

BaaS is a newer and increasingly mainstream cloud model that uses a non-centralized system. This model uses encrypted, connected blocks of information for higher security than standard cloud services. BaaS is used to store smart contracts and high-security documents. This model authenticates users without needing additional applications. SaaS services may adapt BaaS as a standard feature to address the risk of hacking.

– – Continued – –

Four types of cloud computing

Cloud computing is the delivery of computing services like the cloud services mentioned above. There are four main types of cloud computing:

1. Public clouds: cloud environments created from IT infrastructure owned by a provider such as Google Cloud or Amazon Web Services. Public clouds host the data of multiple companies. Be aware that public clouds do not provide absolute security for the information it stores.
2. Private clouds: serve a single business or organization. The cloud runs behind an internal firewall. Private clouds can be deployed and managed by a third-party vendor.
3. Multiclouds: involve using more than one cloud service from more than one vendor. These can be private or public.
4. Hybrid clouds: blend at least two public or private cloud services and connects them with internal networks, such as local area networks or VPNs.

Cloud services and cloud computing work together to meet the needs of companies and organizations.

Key Takeaways

Companies use the cloud for many tasks and services.

- The three primary cloud services are SaaS, PaaS, and IaaS.
- Additional cloud services include VPNaaS, FaaS, DaaS, and BaaS.
- Four main types of cloud computing are public clouds, private clouds, multiclouds, and hybrid clouds that deliver cloud services.

Resource for more information

For more information on the Google Cloud Platform and the services it offers, visit this website.

Managing Cloud Resources

If you are considering hosting some services in the Cloud, you'll need to learn what the different terms used to configure the services mean.

When deploying a service to the cloud, you will typically create a number of virtual machines that will be the servers in charge of hosting your service. In the usual case, you would start by creating a single machine that will run the service, creating the configuration associated with the machine, verifying that it works, and then turning this into a template that can be used for the creation of many machines as needed.
In order to do this, you'll make use of both Autoscaling and Load Balancing. Autoscaling means being able to automatically create new instances when the load increases and automatically turn them down when the load decreases. In order for this to be possible, you need to ensure that your instances can be completely configured automatically, and that there's no data being kept in the instances themselves (data can be stored in a database, or in separate drives).

Load Balancing means distributing the load among many servers. There's different approaches to doing load balancing, but the main concept is that there's a load balancing service that will route traffic to the servers in a way that they each get to serve a portion of users, without the users realizing that they are connecting to different machines. In other words, the users will access a single address (e.g. http://www.example.com), which can be served by different servers, in different parts of the world, without the users having to care about that.

Once you have your service set up to scale automatically and balance the load, you'll want to also setup Monitoring and Alerting for it. Monitoring means checking that the service is healthy, that it's responding to queries as expected and not generating unusual errors. Alerting means sending alerts when things don't happen as expected.

For a simple service, you might go with the monitoring that is already built in by the cloud provider, which will allow you to check that your instance is healthy, but is likely not going to go into much detail as to whether the content is being served correctly. If your service is more complex, you might want to invest more time into making it possible to monitor additional parameters of your service.

Depending on the specific service you are deploying, there might be more concepts that you need to understand before you can actually do it. We recommend reading the documentation offered by the cloud provider you have chosen to figure out what you need to do.
Here are some links with more information from some of the biggest cloud providers:

- https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/
- https://aws.amazon.com/getting-started/
- https://cloud.google.com/docs/overview/

Module 4: Directory Services

Centralized Management
A central service that provides instructions to all of the different parts of an IT infrastructure.

Supplemental Reading for Kerberos
For more information on Kerberos reading check out the link here.

Supplemental Reading for Active Directory
For more information about Active Directory, check out the link here.

Supplemental Reading for Group Security Principles
For more information on Group Scope check out the link here and for Security Principles click here.

Supplemental Reading for EFS Features
For more information on Features of EFS click here.

Supplemental Reading for DFL & FFL
For more information on Forest and Domain Functional Levels click here.

Supplemental Reading for Group Policy Troubleshooting

This reading expands upon a previous topic on various approaches to troubleshooting common Group Policy problems.

Terminology

Important terminology used with Microsoft Windows Server Group Policies:

- **Group Policy Object (GPO)**: A set of Active Directory (AD) Group Policy configurations that controls the appearance and behaviors for groups of computer systems and/or groups of end users.
- **Group Policy Management Console (GPMC)**: A console that is used to create, manage, edit, and link GPOs. The GPMC provides thousands of options for computer and user settings such as Control Panel items, Registry settings, and environmental variables. Policy settings are refreshed every 90 minutes, so changes are not applied immediately. The GPMC can be used to create GPOs that control registry-based policies and software installations, as well as options for:
    - security
    - maintenance
    - scripts
    - folder redirection

- **Active Directory (AD) containers**: AD containers can be linked to GPOs. AD containers include:
    - Sites: Physical sites or aspects of a network, which are linked to AD Domains. Can be used to group and connect geographically dispersed locations into the same domain.
    - Domain: A collection of objects in an AD network, such as computers, users, and groups. Can contain multiple AD Sites and be linked to multiple GPOs.
    - Organizational Unit (OU): Collectively groups end users, computers, groups, and/or other OUs. OUs can reflect an organization's hierarchy and business divisions. For example, an organization might have separate OUs for executives, administration, accounting, IT, sales, marketing, vendors, etc.

GPOs process order: Windows will apply GPOs in the following order:

1) The Local GPO
2) GPOs linked to Sites
3) GPOs linked to Domains
4) GPOs linked to OUs

- Resultant Set of Policies (RSoPs): A report of AD Group Policy settings that indicates how all GPO settings are hierarchically inherited by end users and computers. RSoP reports can be collected for evaluation using RSoPs logging.
- Windows Management Infrastructure (MI) and Windows Management Instrumentation (WMI): MI is the next generation of WMI. However, both MI and WMI are fully supported by Microsoft and MI is backwards-compatible with WMI. MI/WMI provide the operations infrastructure and management data in Windows. They also are used for scripting administrative tasks to run on remote systems.

Group Policy troubleshooting tools

The following command line tools can be used for troubleshooting Group Policy issues:

- **gpresult**: Displays the RSoP report or values for a computer and user account. This information can help to ascertain which configuration settings have been applied and which settings were overridden. A few of the switches available to the gpresult command include:
    - **/s *host*** - Displays the RSoP values of a remote computer.
    - **/u *user***-*account* - Displays the RSoP values of an end-user.
    - **/p *password*** - Displays the RSoP values of an end-user password policy.
    - **/r** - Displays the RSoP summary of applied GPOs.
    - **/z** - Turns on verbose mode to display details of the RSoP applied settings.
- **gpedit**: The Group Policy Editor, which is a robust tool for changing Registry settings related to the Control Panel, Settings, user profiles, system configurations, third-party software, and more.
- **gpupdate**: Command that can be used to force a new or edited GPO to be applied immediately using the /force switch. If the policy setting requires the users to logoff or reboot, the switches /logoff or /boot can be added to the command.

Additionally, system event logs are important tools for most Windows troubleshooting issues:

- **Event Viewer and Windows Logs**: The Windows Event Viewer is an invaluable tool for viewing Windows Logs. These tools help IT Support specialists track system problems and events related to items like applications, user logins, security, and systems. To open the Windows Event Viewer, click on the Start menu and type “Event Viewer”. Any error messages or codes found in the logs can be investigated using the Microsoft Knowledge Base (support.microsoft.com), as well as through an internet search. The main Windows Logs include:
- **System log**: Records Windows OS events like hardware conflicts, driver load failures, service load failures, network issues, and more.
- **Application log**: Records application processes and utilities events/errors.
- **Security log**: Records system security audit information.
- **Setup log**: Records installation events and errors.

Resources for more information

- Group Policy troubleshooting documentation for Windows Server - Extensive troubleshooting guide for Group Policies. Topics can be accessed from the left side menu.
- Group Policy processing and precedence - Additional information about GPO processing order and exceptions.
- Active Directory documentation - Extensive troubleshooting guide for AD. Topics can be accessed from the left side menu.
- Use Resultant Set of Policy logging to gather computer policy information - Microsoft article that provides information on how to use the RSoPs utility (Rsop.msc) to gather computer-specific policy information.
- Suggested hotfixes for WMI related issue on Windows platforms - Provides information on symptoms and resolutions for WMI issues.
- How the Windows Time Service Works - (from the video on troubleshooting Group Policies) Microsoft article that includes information on how to manually force a domain computer to resync.
    - W32tm - Syntax for using the w32tm /resync command, which can be used to diagnose problems related to Windows Time.
- 6.3.2.3 SRV Records - (from the video on troubleshooting Group Policies) Information from Microsoft on the SRV DNS Resource Record.

Supplement Reading for Group Policy Troubleshooting Examples

As an IT Support professional, you may need to troubleshoot Group Policy issues in Windows. The following are a few examples of the most common problems encountered when working with Group Policies. Included are suggested tips on how to troubleshoot these issues using tools you've learned about previously.

Scenario 1: Group Policy settings are not being applied

Imagine that you are an IT Support Analyst for an organization. You recently made changes to several settings on a Group Policy Object (GPO). However, the group policy changes do not appear to be active for the target end users or computers. You must troubleshoot to uncover the root of the problem and to fix it.

1. **Check the GPO Scope**. In the Group Policy Management utility, select the GPO that you recently changed and go to the Scope tab. Check the Links section to see if the GPO that you changed is linked to the correct Organizational Units (OUs). The linked OUs should contain the target computers (for computer-side settings) or target users (for user-side settings) for the changed GPOs.
2. **Check Security Filtering**. Below the Links section on the Scope tab, check the Security Filtering section. Make sure the correct computers and/or users intended for the changed GPO settings are specified in the security filters.
3. **Check Read and Apply permissions**. If any items have been added to Security Filtering, check the Delegation > Advanced tab to ensure the Allow option is checked for the Read and Apply permissions.
4. **Check the Group Policy Delegation**. On the Delegation tab, check the Groups and users section for Allowed Permissions for the GPO. This list contains the groups and users that have the authority to edit, delete, and modify security for the GPO. Ensure that these settings are desired for your environment and no unauthorized users or groups can edit GPO settings.
5. **Enable/disable User or Computer configurations**. On the Details tab of the GPO, check the GPO Status to ensure the selection matches your intended setting. The options are:
    - **All settings disabled**: GPO will be inactive.
    - **Computer configuration settings disabled**: Any Computer configurations in the GPO will be inactive.
    - **User configuration settings disabled**: Any User configurations in the GPO will be inactive.
    - **Enabled**: All GPO configurations will be applied (default).
6. **Check the GPO Policy Process Order (LSDOU)**. The GPO process order from first applied to last is Local GPOs, Site GPOs, Domain GPOs, then OU GPOs. Each GPO policy overrides the previous GPO setting in this LSDOU process order. To change the default order, select the affected OU in the Group Policy Manager and go to the Linked Group Policy Objects tab. The Link Order enumeration for the GPOs is listed in reverse order, meaning the GPO with the highest Link Order number is applied first and the GPO with the lowest number (1) is applied last. The number 1 indicates the GPO has the top-ranking priority, as it will override the previous GPO settings where the settings overlap. You can change the order that the GPOs are applied using the up and down arrows to the left of the list.
7. **Ensure target GPO to OU links are enabled**. GPO to OU links are technically shortcuts, which can easily be enabled or disabled. Check to ensure that the Link Enabled setting has not inadvertently been turned off.
8. **Check if an upstream GPO is set to Enforced**. An upstream GPO is a GPO linked to an OU that has a higher LSDOU priority than a downstream GPO. If an upstream order of applying settings is enforced, a lock will appear on the link icon. Evaluate if enforcement is overriding the desired GPO settings.
9. **Check if the affected OU is set to Block Inheritance**. The default Group Policy inheritance for OUs, which is applied hierarchically to nested objects, can be blocked. Block Inheritance is indicated in the Group Policy Manager as a blue exclamation point icon on the affected OU. If you believe this setting might be the cause of the GPO changes not propagating, right-click on the OU and select Block Inheritance from the menu to toggle it off/on. Note that Block Inheritance will not affect Enforced GPOs.
10. **Check if loopback is enabled**. If loopback is enabled, the user-side settings that belong to the computer's OU will override any computer-side settings in the same OU. If the OU's computer-side settings need to have priority over the user-side, set the user Group Policy loopback processing mode to Disabled.
11. **Check MI or WMI filters**. Check to see if Windows Management Infrastructure (MI) or Windows Management Instrumentation (WMI) filters are set on the changed GPO. MI or WMI filters might be used to apply a policy to a subset of objects. The MI or WMI query may need to be edited to ensure the target objects for the changed GPO are not excluded by the filter.
12. **Ensure your expectations for the GPO setting match its actual purpose**. If the troubleshooting steps listed above do not solve the Group Policy problem, research the GPO settings you are using. It is possible that your expectation for a setting may not match what the setting actually does.

Scenario 2: GPO settings are not correct.

- Edit incorrect GPO settings. If there are any problems found with GPO settings, open the Group Policy Management interface and edit the GPO:
    - **Step 1**: Select the GPO with the incorrect settings.
    - **Step 2**: Right-click the GPO, and then click Edit.
    - **Step 3**: Edit the settings using the appropriate instructions listed in Scenario 1 of this article.

Scenario 3: The user can't authenticate into the Active Directory domain

- Check Active Directory (AD) infrastructure. Investigate if the user or computer cannot locate the domain controller. Domain controller and replication problems in AD can prevent GPOs from functioning correctly.

Key takeaways

Outline of troubleshooting steps for GPO settings that are not being applied:

1. Check the GPO Scope.
2. Check Security Filtering.
3. Check Read and Apply permissions.
4. Check the Group Policy Delegation.
5. Enable/disable User or Computer configurations.
6. Check the GPO Policy Process Order (LSDOU).
7. Ensure target GPO to OU links are enabled.
8. Check if an upstream GPO is set to Enforced.
9. Check if the affected OU is set to Block Inheritance.
10. Check if loopback is enabled
11. Check MI or WMI filters.
12. Ensure your expectations for the GPO setting match its actual purpose.

Resources for more information

For more information on Group Policy troubleshooting, please visit:

- Working with Group Policy Objects using GPMC - Microsoft's guide to the Group Policy Management Console and managing GPOs.
- Troubleshooting: Group Policy (GPO) Not Being Applied to Clients - Troubleshooting guide for GPOs. Includes screenshots of various settings in the Group Policy Management Console with descriptions of how each setting works.

Supplemental Readings for Mobile Device Management (MDM)

Check out the following links for more info:

- iOS - Apple Platform Deployment
- Android - Apply settings for Android mobile devices
- iOS - Intro to Profile Manager
- Android - Get started with Google Mobile Management, Apply settings for Android mobile devices

Supplemental Reading for OpenLDAP

For more information about installing and configuring OpenLDAP and phpLDAPAdmin on Ubuntu 16.04, click here or check out this article on openldap.org.

Supplemental Reading for Managing OpenLDAP

For information about how to use LDIF files to make changes to an OpenLDAP system, click here.

Module 5: Data Recovery & Backups

Rsync
A file transfer utility that's designed to efficiently transfer and synchronize files between locations or computers.
- Uses compression
- Can send file via ssh
- It can synchronize files between remote machines, useful as an automated backup.

Supplemental Reading for Backup Solutions
For options to backup data, check out Microsoft Backup and Restore, Apple Time Machine and Rsync as a backup utility.

Disaster Recovery Plan
A collection of documented procedures and plans on how to react and handle an emergency or disaster scenario, from the operational perspective.

Post-Mortem
Created after an incident, an outage, or some eve when something goes wrong, or at the end of a project to analyze how it went.

– fin –

Glossary

IT Support

Terms and definitions from Course 4

A

AAA (authentication, authorization, accounting): The services that the directory services provide to all the computers within a company or organization

Active directory (AD): The Microsoft alternative to directory services that offers customization and added features for the Windows platform

Active directory users and computers (ADUC): The client tools that are used for accessing and administering a directory server

Advanced group policy management (AGPM): A set of add-on tools from Microsoft that gives some added provision control abilities in GPMC

Autoscaling: A system that allows the service to increase or reduce capacity as needed, while the service owner only pays for the cost of the machines that are in use at any given time

B

Backup and restore: A Microsoft offer and first party solution that has modes of operation, as a file based version where files are backed up to a zip archive

Bind operation: The operation which authenticates clients to the directory server

C

Central management: A central service that provides instructions to all of the different parts of my IT infrastructure

Change management process: The process to notify others in the organization about the changes that you are about to make

Cloud computing: The concept and technological approach of accessing data, using applications, storing files, etc. from anywhere in the world as long as you have an internet connection

Computer configuration: Contained within a Group Policy Object (GPO)

Configuration management: The creation of rules about how things should work in your organization, such as printers, configure software, or mounting network file systems

D

Databases: Databases allow us to store query, filter, and manage large amounts of data

Data center: A facility that stores hundreds, if not thousands of servers

Data recovery: Is the process of trying to restore data after an unexpected event that results in data loss or corruption

Data tapes: The standard medium for archival backup data storage

Default domain control policy: One of the two GPOs that are created when a new Active Directory domain has been made

Delegation: The administrative tasks that you need to perform a lot as a part of your day to day job but you don't need to have broad access to make changes in AD

Deployment: Hardware is set up so that the employee can do their job

Detection measure: The measures to alert you and your team that a disaster has occurred that can impact operations

Differential backup: A backup of files that are changed, or has been created since the last full backup

Directory Access Protocol (DAP): A protocol that is included in the X.500 directory standard from 1988

Directory Information Shadow Protocol (DISP): A protocol that is included in the X.500 directory standard from 1988

Directory Operational Bindings Protocol (DOBMP): A protocol that is included in the X.500 directory standard from 1988

Directory server: The server that contains a lookup service that provides mapping between network resources and their network addresses

Directory services: A lookup service contained in a network server that provides mapping between network resources and their network addresses

Directory System Protocol (DSP): A protocol that is included in the X.500 directory standard from 1988

Disaster recovery plan: A collection of documented procedures and plans on how to react and handle an emergency or disaster scenario, from the operational perspective

Disaster recovery testing: A regular exercise that happens once a year or so, that has different teams, including IT support specialists, going through simulations of disaster events

Distribution group: A group that is only designed to group accounts and contacts for email communication

Domain Name System (DNS): A global and highly distributed network service that resolves strings of letters, such as a website name, into an IP address

DNS records: A DNS request for the SRV records matching the domain that it's been bound to

Domain admin: The administrators of the Active Directory domain
Domain computers: All the computers joined to the domain except domain controllers
Domain controllers (DC): The service that hosts copies of the Active Directory database
Domain local: The tool used used to assign permission to a resource
Domain users: A group that contains every user account in the domain
E
Enterprise admin: The administrators of the Active Directory domain that has permission to make changes to the domain that affect other domains in a multi-domain forest
Enterprise mobility management (EMM): A system that can create and distribute policies and MDMs
F
Fast logon optimization: The group policy engine that applies policy settings to a local machine may sacrifice the immediate application of some types of policies in order to make logon faster
File compression: The files and folder structures are copied and put into an archive
File storage service: Allows to centrally store files and manage access between files and groups

Flexible single-master operations (FSMO): The single domain controller that has been tasked with making changes to the AD database that can only be made by one DC at a time
Forest: The hierarchy above a domain that contains multiple domains, allowing accounts to share resources between domains that are in the same forest
Full backup: The full unmodified contents of all files to be backed up is are included in this backup mechanism whether the data was modified or not
Functional levels: The different versions of Active Directory, a functional level that describes the features that it supports
G
Global: The tool that is used to group accounts into a role
Group policy management console (GPMC): The tools used for creating and viewing a group policy object
Group policy objects (GPO): The ways to manage the configuration of Windows machines, referring to the objects that represent things in your network that you want to be able to reference or manage
Group policy settings reference: A spreadsheet that details the GPO policies and preferences that are available and where to find them
Group scope: The way that group definitions are replicated across domains
H
HTTPS: Hypertext Transfer Protocol Secure is a secure version of HTTP that ensures the communication your web browser has with the website is secured through encryption.
HTTP status code: The codes or numbers that indicate some sort of error or info messages that occurred when trying to access a web resource
Hybrid cloud: Used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud or on premise while entrusting their less sensitive servers to a public cloud
I
Import: Moving a backup of the test example policy to the production example policy
Intranet: An internal network inside a company, accessible if you are on a company's network

IT Infrastructure: The software, the hardware, network, and services required for an organization to operate in an enterprise IT environment
J
K
Kerberos: The authentication protocol that AD uses, that is sensitive to time differences
KVM Switch: Keyboard, video, & mouse switch that looks like a hub that you can connect multiple computers to and control using one keyboard, mouse, and monitor
L
LDAP data interchange format: The tool that allows you to authenticate, add, remove users, groups, computers and so on in a directory service
LDAP Entry: A collection of information that's used to describe something
LDIF files: A text file that lists attributes and values that describe something
Lightweight Directory Access Protocol (LDAP): The most popular open-source alternative to the DAP, which allows clients to access the X.500 directory
Linked: A GPO that all of the computers or users under a domain, site, or OU will have a policy applied
Load balancer: Ensures that each VM receives a balanced number of queries
M
Maintenance: Where software is updated and hardware issues are fixed if, and when, they occur
MDM policy: The profiles that contains settings for the device

MDM profile: The policies that contains settings for the device
N
NAS device: A network attached storage device that has hard drives to automatically create backups and store data
Network file system: A protocol that enables files to be shared over a network

NTP: Network Time Protocol, keeping clocks synchronized on machines connected to a network
O
One-way cryptographic hash: The method used by AD to store passwords
OpenLDAP (lightweight directory access protocol): An open source and free directory service
Organizational units (OU): A hierarchical model of objects and containers that can contain objects or more organizational units
P
Parent group: Groups that are principal groups and contain other groups
PHPLDAPadmin: A tool to manage OpenLDAP
Platform Services: A platform for developers to completely build and deploy software applications, without having to deal with OS maintenance, server hardware, networking or other services that are needed to use the platform tools
Policies: Settings that are reapplied every few minutes, and aren't meant to be changed even by the local administrators
Post mortem: A way for you to document any problems you discovered along the when recovering data, and the ways you fixed them so you can make sure they don't happen again
Precedence: When computers are processing the Group Policy Objects that apply to them, all of these policies will be applied in a specific order based on a set of precedents rules
Preventative measures: Any procedures or systems in place that will proactively minimize the impact of a disaster
Private cloud: When a company owns the services and the rest of the cloud infrastructure, whether on-site or in a remote data center
Procurement: Hardware is purchased or reused for an employee
Production: The parts of the infrastructure where certain services are executed and serve to its users production
Proxy Server: An intermediary between a company's network and the Internet, receiving network traffic and relaying that information to the company network
Public cloud: The cloud services provided by a third party

Q
R
RAID (redundant array of independent disks): A method of taking multiple physical disks and combining them into one large virtual disk
Read-write replicas: Domain controllers in the Active Directory network that each have a complete copy of the AD database and are able to make changes to it
Regions: A geographical location containing a number of data centers
Remote wipe: A factory reset that you can trigger from your central MDM rather than having to do it in person on the device
Replication: the store directory data is copied and distributed across a number of physically distributed servers but still appears as one unified data store for querying and administering
Replication failure: A reason that a GPO might fail to apply as expected
Reproduction case: Recreating an error to test a solution to make sure the problem is gone after a fix has been applied
Reset: When an SysAdmin restores or resets the password of a user
Restart: A command that will let the machine reboot to complete a domain join
Restoration procedures: A recovery process and process needs to be tested regularly that is documented and accessible so that anyone with the right access can restore operation when needed
Resultant set of policy (RSOP): The policy that forms when all of the group policies have been grouped together for a specific machine and apply precedence rules to them
Retirement: Hardware becomes unusable or no longer needed, and it needs to be properly removed from the fleet
Risk assessment: Allows you to prioritize certain aspects of the organization that are more at risk if there's an unforeseen event
Role-based access control (RBAC): The process of changing a persons group that they are a part of when they have changed roles within a company to limit or change their access to resources
Rollback: Reverting to the previous state before you made changes

RSOP report: The process of troubleshooting group policy and comparing what you expect to be applied to a computer and the resultant set of policy report
S

Secondary or stand-by machine: A machine that is the same as a production machine, but won't receive any traffic from actual users until enabled
Security account manager (SAM): A database in windows that stores user names and password
Security filtering: A tool to make group policies apply more selectively
Security group: One of the two categories that groups in Active Directories can be part of, they can contain user accounts, computer accounts or other security groups
Security principal: Any entity that can be authenticated by the system, such as a user account, a computer account, or a thread or process that runs in the security context of a user or computer account
Server: Software or a machine that provides services to other software or machines
Server Operating Systems: Regularly operating systems that are optimized for server functionality
Service discovery: One of the services that the domain controller provides to the clients
Simple authentication and security layer (SASL): The authentication method that can employ the help of security protocols like TLS, it requires the client and the directory server to authenticate using some method
Single point of failure: When one system in a redundant pair suffers a failure
Software Services: The services that employees use that allow them to do their daily job functions, such as word processors, Internet browsers, email clients, chat clients, and more
SRV records: A service record used to define the location of various specific services
System Administration: The field in IT that is responsible for maintaining reliable computer systems, in a Multi-user environment
Systems administrator (sysadmin): A person who works only in system administration, configuring servers, monitoring the network, provisioning, or setting up new users in computers and taking responsibility of systems
T

Test environment: A virtual machine running the same configuration as a production environment, but isn't actually serving any users of the service
U
Universal: The tool that is used to group global roles in a forest
User configuration: Contained within a Group Policy Object (GPO)
User Groups: The management of resources on a computer and on a network through organizing user accounts into various groups
V
W
Web Server: A web server stores and serves content to clients through the Internet.
Windows management instrumentation (WMI): The container that is used to define powerful targeting rules for your GPO
Windows registry: A hierarchical database of settings that Windows, and Windows applications, use for storing configuration data
WMI filter: A tool to make group policies apply more selectively on the configuration of the computer
Work group computer: A Windows computer that isn't joined to a domain
X
X.500 directory: The agreed upon directory standard that wa approved in 1988 that includes, DAP, DSP, DISP, DOP, DAP, and LDAP
Y
Z