Intro

January 10, 2023 8:04 AM

Service desk - single point of contact between a company and customer incidents / service requests

Help desk - single point of contact within a company for tech-related questions / incidents

Technical support - help people using they technology

Service desk:

1. mad skillz (business, technical, soft, time/self management)
2. good at customer service / tech skillz
3. know that you are the voice of the company for that person now

Technical support services:

- installing or upgrading hardware/**software**/network/app components
- keeping systems/devices in good shape - printers :(
- customer support

Incident report - an unplanned interruption to IT service (or works worse now)

- single user / application, ex. forgotten password

Problem - the cause of one or more incidents

- hardware defects, software errors, ex. phone line got messed up

Service request - a formal request from a user for something

- may include info, advice, or standard change (pre-approved change).

Multi-level / tier support model - if the service desk can't resolve the issue, they will refer to the group who can (internal, external or subject matter expert)

Subject matter expert (SME) - a person who has a high level of experience / knowledge with a subject

Customer Service components:

- Greeting and validation
    - intro to service desk
    - validate customer information - ID, SIN, manager name?
    - impression and attitude
- Investigation and diagnosis
    - questioning
        - closed ended questions - specific answer questions (are you logged in?)
        - open ended questions - questions as statement that needs response (describe to me ...)
        - probing questions -
        - confirming questions - to make sure we know what the issue was, and to see if its resolved
- Resolution
    - use your resources (knowledge base, standard procedures, best practices, peers, documentation, etc.)
    - update any outdated resources
    - estimate time and apply fix if possible

    - ensure the issue is resolved
- Closure
    - verify and update (description of issue, verify solution, symptoms, knowledge resources, update tickets)
    - ticket closure

Customer service tasks:

- hold
    - Describe - reason why, and time frame
    - Acknowledge and confirm they know why
    - Take timely actions and watch time
    - Express gratitude and personalize
- mute
    - brief pause - cough or sneeze, co-worker question
    - inform customer for long mutes
    - ensure your mute is working (dont immediately shit talk)
    - use hold instead if you can
- transfer and escalate
    - send an issue to another resource (customer asks, time, expertise, brain empty)
    - tell the customer about the escalation
        - tell customer next steps, group, time frame and ticket number
        - confirm understanding
    - make sure contact information is correct
    - screenshots/error message
    - steps already taken
    - any articles used
- Following up
    - used to schedule later contact
    - make sure they are happy with fix/workaround
    - confirm changes did not revert after reboot

Intro part 2

January 17, 2023 8:51 AM

- Treat customers with respect
- not everyone is tech savvy
- they call when upset
- they want help asap

Main Reasons for Customer Issues

- customer not trained with tech
- push/upgrade/process didn't work properly
- product isn't working
- system is slow
- customer using outdated equipment or software

Goal:

- provide quality customer service

service desk analysts need to be:

- understanding
- listening
- friendly - they can hear you smile
- patient - have to be patient

Rapport Benefits:

- handle contacts efficiently
- build brand loyalty
- make a foundation of quality customer service - learn who to go to for help, and your tools

Building Trust:

- set clear expectations
- follow up on commitments
- listen to the customer's needs
- give proper and clear information - don't just wing it

Phone Communication:

- Positive tone
- Listening and following
- Positive word choices
- empathy
    - diffuse a negative situation
    - calm an upset customer
    - shows you're listening

- **don't take it personally** - they are already upset, that ain't at you
- follow customer's lead - match
- don't use elite gamer nerd speak
- listen to customer's perspective

Writing Communication:

Style

- greeting
- formatting of paragraphs
- closure statement
- signature line

Tone

- purpose - what you're talking about
- audience - info about the customer
- words - use positive words

Recovering Unsatisfied or Angry Customers:

LEAD

Listen
Empathize
Apologize
Discover the source

Reasons to say no to a customer:

- product isn't covered
- customer doesn't pay for that level of service
- not a service you provide

How to say no:

- confirm the problem is something you **can't** help with
- use positive language to inform customer that you **can't** help
- give options/ideas/info that will help
- offer as much assistance as you can

Common Service Desk Situations:

- impassioned
  - don't let their emotions derail the help
- combative
  - let them vent, don't make excuses
- chatty
  - ask to the point questions
  - to the point answers
  - let them know the time frame
- timid
  - ask to the point questions

What if they use profanity?

- every service desk has a process for handling customers who have threatened, used profanity or become out of control

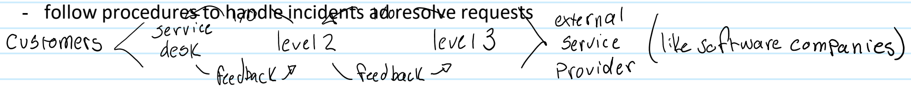
Service Desk Careers and Certificates

January 24, 2023 8:20 AM

ITIL: Information Technology Infrastructure Library - basically IEEE for service desk stuff

Service Desk Analyst:

- referred to as tier 1 or level 1 support
- entry point for the single point of contact (SPOC) model
- follow procedures to handle incidents and resolve requests



Responsibilities of a Service Desk Analyst:

- resolving break/fix issues
- doing requests
- following processes and procedures
- communicating and troubleshooting

Service Desk Analyst vs Technician:

- technicians are essentially a step up - generally more technical and experienced
- service operations, processes, including problem management
- change management - changing infrastructure
- release and deployment
- network monitoring, project management, knowledge management

CIO - chief information officer: top of org with ownership of service desk operations & other functional areas of IT
Director: reports to CIO or VP, oversees the operation of service desk
Manager: oversees the people of the service desk
Project Manager: may or may not be reporting to service desk manager, responsible for delivering updates and working directly with service desk manager
Supervisor/Team lead: supervising the day to day operations, identify/research/resolve complex tech problems

Incident - unplanned interruption to a service or reduction in the quality of service
problem - a multitude of incidents happening to more than just one user

problem management: goal is to reduce likelihood and impact of incidents by finding actual and potential causes. find workarounds and known errors

request fulfillment: do things that people ask - user creation, disabling users, password changes, etc.

- management > initiation > approval > fulfilment

demand management: goal is to understand, anticipate, and influence customer demand for services

release and deployment management: ensures releases are deployed into production efficiently and effectively

- request > plan/design > build > review > test > deploy > support > issue reporting (cycle)

change management: understand and minimize risks while making IT changes

- services should be stable, reliable, and predictable
- services should be able to change rapidly to meet evolving business requirements

service level management: service level agreements that are an agreement between customer and the service provider

knowledge management: gathering and organizing the information on your client(s) - uses Service Knowledge Management System (SKMS)

quality management: ensure that team members are following procedures/processes/policies, set standards, review and monitor processes, (managers, auditors and coaches)

Troubleshooting:

- ability to effectively diagnose issues and resolve them
- requires knowledge of supported hardware, software, tools, networks, infrastructures, and applications

accepting > logging > categorizing > prioritizing > diagnosing > escalating > restoring > resolving > documentation > closing >
follow up > follow knowledge based procedures > customer satisfaction

essential troubleshooting questions:

- have you had this problem before?
- has anything changed since this issue started - what changed before is a better question
- do you experience this issue on another computer, device or network - can the person sitting next to you do it?
- how is this impacting your work - goes with prioritization
- are you seeing a specific error message?
- are you the only one experiencing this issue?

troubleshooting skills:

- tech knowledge
- patience
- empathy
- listening skills
- positive attitude
- thinking skills
- ability to ask question
- incident process definition
- growth mindset (grindset)
- methodologies defined / strategy good

Topic 3: Careers and Certs

January 31, 2023 8:12 AM

Knowledge Worker Skills:

- create - knowledge
- analyze - only have good knowledge in your knowledge base
- filter - same as ^
- edit - change if wrong
- update - update new thing
- utilize - use it
- apply - use it

Technical Skills:

desktop skills: hardware

- installation
- testing
- connectivity
- upgrades
- pc deployment and repair skills (dont really repair pcs anymore, but definitely use deployment)
- basic remote admin skills (gotta be able to remote in and configure stuff, it wont always be close by)
- experience with centralized administration of pc servers

desktop skills: software

- configuration
- maintenance
- setup
- deployment
- troubleshooting
- antivirus
- software installation
- basic concepts on the administration of AD
- domain GPOs
- ticketing software experience

basic networking troubleshooting / knowledge

- Firewalls - gotta know how to configure and fix em (useful)
- Gateways
- Switching
- Routing
- Wireless
- VPNs
- Physical cabling
- Proxy
- Protocols

Security Skills:

- installing security patches and service packs
- knowledge of phishing scams, ransomware, and how data theft happens - delete phishing emails from exchange
- how to identify and define security attacks and breaches - is the outside source safe or not, why ?
- how to mitigate security attacks

Security breaches and Incidents:

- passwords hacked - from phishing links or whatever
- missing patches or updates - people not updating their computers

- virus and malware
- improperly configured software - why most people aren't allowed to download software
- loading unauthorized software
- insecure disposal of equipment - physical damage doesn't necessarily mean hard drives are wiped
- insecure storage of information - don't put your off site backup just on your desk or something
- theft or loss of equipment - it shouldn't be able to have everything stolen

Security Policies:

- a security policy governs employee activities

  Acceptable use policies: how use of network, email, social media, and personal is allowed

  BYOD and mobile device policies: the policy related to phones, devices, and laptops

goal of security policies:

- protect the property of the business implementing the policy
- in the case of IT, this includes protecting all of the company's Information Technology assets from security breaches

Values:

- ethical
- respectful
- integrity
- honest

Vision:

- what you want to do
- where you want to be in x years

Mission:

- how you're going to get to your vision

Business skills:

- Time Management - get it done on time but also have a life, don't JUST work
- ownership - take ownership of something, do it good
- accountability - if you take ownership, you are accountable, do it good
- defines tasks - know what you need to do to get to the end,
- proactive - update things before they break if you know they're going to break
- identify trends - huge for company growth if you can see them before they happen
- delivers on time - time management, do WBS, know what you need to do, deliver outcomes on time

Project Management Teams:

- **Root cause analysis team** - figure out what the issue is so you can fix it
- **Pilot and testing team** - tests the fix before you roll it out
- **knowledge team** - makes the manuals and stuff
- **education and training team** - shows people how to use the new solution
- **release and deployment** - people who install it, and roll it out

# of people doing these roles entirely depends on how large the project is

Project Tasks and Functions:

- provide knowledge and expertise
- work with end users to develop project needs
- document project tasks - show what you've done, and what you need to do
- conduct training and education - make sure people know what they're doing and how to do it
- provide input of current and future needs - solutions need to be flexible and expandable to match what needs to be done
- report on progress of tasks - really need stuff to be done on time
- development of processes and procedure
- assist with testing - make sure its working and doesn't break anything else

Essential Additional Skills:

- change management
- organizational skills
- resilient attitude -

- creative thinking
- collaborative spirit
- multitasking ability
- continuous improvement

Service Desk Certifications: ez money glitch (NOT PATCHED)

- establish knowledge and credibility
- validate commitment to learning
- *increases earning power*
- prepares and qualifies for promotions

Certificate Categories:

- Technical
- Customer Service
- Service Management
- Project Management

Microsoft Certification Levels:

- Fundamentals
- Associate
- Specialty
- Expert

different exams for different microsoft softwares

CompTIA

- A+ - kinda dated, hardware certification
- Network+
- Security+
- Project+

and probably

- Linux+
- Cloud+ (look at Azure first)

A+Essential

- IT Fundamentals
- A+
- Network+
- Security+

CompTIA is industry recognized

Project Management Professional Cert - good but super stressful. one place where crap flows uphill
Certified Associate in Project Management Cert

ITIL Levels - currently on version 4

- Foundation
- Practitioner
- Intermediate
- Expert
- Master

IT Infrastructure Library:

can get certs in:

- service strategy
- service design
- service transition
- service operation

- continual service improvement

HDI - don't really know what this is

- leadership
- strategy and policy
- people management
- resources
- process and procedure

Future of Service Desks:

technology

- Self-service - for password resets
- AI / Chat bots
- Automation
- Voice recognition
- Mobile

people

- white glove or concierge service - will pay to talk to a person rather than a robocall
- personalized service
- remote or global workforce - covid has showed a huge spike in this, here right now
- new IT skills required - things change, have to learn new stuff

process

- security - always and forever
- business relationship management - you are the first contact of your company when you answer the phone
- configuration management - managing configuration of the servers / software
- knowledge experience - need to know more about knowledge management, where to go for the info

BEST CERTS LIST BY BILL:

******AZURE*** OP

udemy.com

gotta take the tests through microsoft tho

Ticketing Systems

February 7, 2023 8:39 AM

Helps keep things organized, has notes on issues & attempted solutions

- tracks events and failures, service requests and issue reports
- past resolutions can be stored so you can see old solutions

Organization:

- better than sending emails and them getting lost
- handle and maintain increased load
- assign tickets appropriately to IT groups
- find commonality - bang out a couple at a time
- incidents and requests classification (?)

Efficiency:

- respond to requests with much less effort
- fewer hours to take care of all customers
- fewer mistakes
- grateful customers - don't have to ask your name and email or whatever every time

Speed:

- usually expect their requests to be answered quickly
- with organization and efficiency > things move more quickly and smoothly
- less support staff needed

Routing Options:

- allow customer to select topic
- route ticket to a specific support staff who may be more knowledgeable about that topic
- staff can re-route tickets to another support staff

Professionalism:

- shows you are more professional, keep customers
- outdated support systems are old and seen as unprofessional
- a ticket management system is seen as new and forward thinking - expected now dog
- customers will definitely appreciate the trustworthy feeling of your support system - at least they know you will get to it and wont forget about it

Automated Updates to Customers:

- when you give updates to customers it makes them worry less and less likely to reach out or start a new ticket

Records of Previous Communications:

- lets you see what has happened in the past

Statistics and Analytics Possibilities:

- lets you know what your average response time is
- how many tickets you used
- gives you proof of people working, also can show business clients that things are going smoothly
- customer satisfaction is also here

Queueing and Prioritization:

- gets set as a queue in order
- prioritization is set as how much of your stuff isn't working - less stuff working = more prioritization (probably)

Disadvantages of Ticketing Systems:

- need infrastructure
- maintenance
- requires licensing/support (hella expensive)
- staff training - if they don't know how to use it, it isn't worth it

Ticket Life:

- new
- in progress
- on hold
- resolved
- closed

or

- canceled

Network Troubleshooting

February 14, 2023 8:19 AM

Definition:

- experience and science
- to the uninitiated it may look like an artform

Methodologies:

- process to go through
- helpdesk > enterprise support
- hardware, software, network, storage and security problems

1. identify the problem and determine scope
   - see what the problem is, how many users is it affecting | single PC not working, probably not a server issue.

2. establish a theory of probable cause
   - what do you think caused the issue

3. test theory to determine a cause
   - try to figure out where the issue truly lies

4. establish a plan of action to resolve the problem
   - list options in order of probability

5. implement the solution or escalate as appropriate
   - try your solutions (1 at a time) because your fix might have broken something else

6. verify full system functionality & perform root cause analysis
   - make sure everything is working, if you can, figure out what caused the issues to occur

7. Document findings, actions and outcomes
   - what did you try, what worked, what didn't work

Common problems, causes and tools:
clients: hardware/software issues
storage & disks: storage
server: server stuff
firewalls routers and switches
security

Troubleshooting Methodologies (continued):
Identify the problem and determine scope:
what changed?

- change causes failures
- updates, configuration, movement, hardware/software
- questions users/stakeholders about changes made

collect additional documentation

- logs, performance counters
- expected configuration and operation - what do they expect it to do

if possible, make a backup before performing troubleshooting actions

- you could potentially mess things up a lot more while trying to fix the issue

can you replicate the problem?

- replicating the problem can lead to a cause, if you know when it happens that might help you find the issue

establish a theory of probable cause:

gather information - include diagnostic and log

- updates, configuration, movement, hardware/software
- questions users/stakeholders about changes

question the obvious

- is it plugged in
- is it on

propose a hypothesis

- educated guess of the problem

is there a common element causing multiple problems?

- single failure will appear as multiple problems (dns issue for example)
- do the observed symptoms point to a common cause?

establish a plan of action to resolve the problem:

- if confirmed, determine steps to resolve problem
- if NOT confirmed, establish new theory or escalate.

test the theory to determine cause:

- what steps will you take to resolve the problem?
- notify impacted users/stakeholders
- do i need to submit a change request?

implement the solution:

make one change at a time

- multiple changes are hard to track for success, and often add more problems
- document changes and results

test and confirm the change resolved the problem

- test one change at a time
- test often involve several use-cases

if the problem is not resolved - reverse course!

- reverse the change
- implement and test a new change

may need to escalate as appropriate

- the problem may be more complex and involve other teams
- this may impact more users/stakeholders

verify full system functionality

- confirm successful operation by testing and checking with users/stakeholders
- implement preventative measures if needed

perform root cause analysis

perform after problem is resolved

- root cause analysis takes time (up to company you work for)
- repair the outage first if possible

attempt to determine reason for failure

- changes, outside influence, hardware failure, malware

are there prevention measures or policies that can prevent future problems?

- enforcing strong password for ex.

documentation findings, actions and outcomes

documentation is most important! (i mean fixing the issue is probably more important)

- documents the troubleshooting process and resolution
- provides information for future similar problems
- often documented in a trouble-ticket system

document the symptoms of the problem
document the troubleshooting actions
document the cause of the problem
document the systems and users affected
document the solution to the problem

ABC-5 Steps program

A. Check the political layer - ask if its a good time to fix stuff right now - **ALWAYS** ask if you can remote in
B. Check the Physical Layer first
C. Do a quick ipconfig /all

1. Ping yourself. (ping 127.0.0.1)
2. Ping neighbor. Can I connect to the LAN
3. Ping gateway
4. Ping remote IP address (8.8.8.8/4.2.2.2)
5. Ping remote DNS name (www.google.ca)

Hardware Problems, Causes and Tools

- all hardware and network hardware can have issues.
- can be very complex

Environmental Causes

- can cause many of the problems discussed (shut down, slow down)
- can causes multiple simultaneous failures (if something breaks because it gets flooded for ex.)
- can be gradual failures over time (corrosion, or something)
- will reduce the life span of your hardware
- expensive to replace!

Failed Post

common causes

- hardware failure
- memory
- processor/bios
- temperature

tools/actions

- beep codes lookups
- displayed numeric codes lookups

Component Failure

common causes

- hardware failure

tools/actions

- hardware diagnostic
- remove and re-insert
- replace
- use ESD equipment

Incorrect Boot Sequence

common causes

- configuration error
- often after adding a new device

Tools/actions

- check BIOS config

Software Problems, causes and tools

- more than just computers, involves ALL software, drivers, etc.
- can get very complex

Logon Failure

common causes

- account locked
- unknown password
- password expiration

tools/actions

- account policies
- password policies
- password reset

Resource Access Problems

common causes

- permissions
- user account control
- network/connectivity problem

tools/actions

- verify permissions
- verify connectivity

BSOD

common causes

- failed driver software
- failed hardware - disk corruption

tools/actions

- check error codes
- replace/remove driver
- replace/remove hardware

Driver Issues

common causes

- mismatch driver for hardware
- damaged or corrupt
- unsigned 3rd party driver

tools/actions

- download new and correct driver
- use signed drivers

Slow OS Performance

common causes

- out of disk space - shit slooooooows down
- excessive paging - cant fit software into ram so it puts it in disk drive
- excessive processing - sometimes a program will eat your performance
- fragmentation - moving everything around on the drive which can cause cell degradation

tools/actions

- monitoring tools performance
- located bottleneck
- defragment disks

Server Problems, Causes and tools

- involves DHCP, DNS, FILE SERVERs

DHCP Review
D - discover
O - offer
R - request
A - acknowledgement

★ General terms

- unicast vs broadcast - you know the address you're sending to (MAC)
- multicast - talking to multiple end points at the same time
- Active directory
- LDAP
- Domain Controller
- TCP - connection oriented
- UDP - screams into the void
- IPv4 vs IPv6
- CIDR
- APIPA
- BOOTP/DHCP
- ICMP: Ping, Tracert & pathping
- ARP/RARP
- NSLookup
- FTP/HTTP
- ISP

Client Troubleshooting

February 28, 2023 8:10 AM

Important locations:

C:\

- main install drive for windows
- default subdivided into folders
- Admin shares created on all volumes
    - \\<systemname>\c$ - c drive
    - \\<systemname>\e$ - e drive

C:\Windows\System32

- critical windows utilities that are built in to windows
- ex. task manager, file explorer
- **drivers and registry files are stored here**
- **common for malware to try and install itself here**

Windows Registry

- database that stores low-level settings for windows OS (info, settings, options, values for both hardware and software)
- keys can be exported to back them up as a .REG file
- edited via Reg Edit or command line
- can also be modified by group policy
- corruptions usually mean gg to something

made up of keys, subkeys, and values

HKEY_LOCAL_MACHINE or HKLM
HKEY_CURRENT_USER or HKCU
^ those are the two main ones

values are stored inside a key

- usually a string or DWORD (1 or 0 usually)

cant really know all of reg edit > just google that shit bro :)

REG cmd prompts
reg delete
reg query
reg save

Windows 10 Reset

Refresh - refresh windows without deleting any personal files or apps - third party apps will be deleted

Reset - will remove everything and reinstall windows

Restore - can roll your PC back to an earlier point

- good if its a recent install that has broken something
- restore points are made automatically with software/update installs if the most recent restore point is more than 7 days
- also can be made manually

Settings > change PC settings > update recovery > recovery

Built in repair utility that provides a ton of functionality:

- automatic repair
- reset to factory
- system image recovery
- boot to safe mode - boots with minimal amount of drivers just to start the machine
- cmd and other command line tools

desktop and server

creates recovery partition on setup
fail boot 3 times > recovery mode

Safe Mode

- the most basic state of windows - limited files and drivers
- can optionally be launched with networking
- can reboot as safemode

DISM - Deployment Imaging Servicing and Management (run first)

- service and management for running windows files, images and VHDs
- connects to windows update source to reference and fix system files

SFC - System File Checker (run second)

- compares protected system files against local cache
- may run this if safe mode is required

App Installation

- C:\Program Files -
- C:\Program Files (x86) - both need admin rights
- C:\ProgramData
- C:\Users\<USERNAME>\Appdata - installs only for single user, doesn't need admin rights

Program Files - default install location for 64bit applications
Program Files (x86) - only created on 64bit systems, used for backwards compatibility for 32bit applications

- only admins can make changes to these folders

ProgramData - hidden by default

- less restrictive permissions than Program Files - can be edited by **any** user

Appdata - folders created for each user, contain user-specific settings or data

- user can see only their own appdata folders (%appdata%)
- 3 subfolders:
  roaming - holds settings for different computers
  local - wont follow user between pcs
  LocalLow - low level data - temp files, web cache etc.

Preventative Maintenance

- stopping issues before they happen, can apply to any system

- antivirus, patching, firewall settings
- password policy
- regular backups

Best Practices:

- keep OS up to date
- install anti-virus software
- install and configure personal firewall (windows firewall)
- install and configure anti-spyware programs (included with most anti-virus software)
- keep apps and software up to date
- dont open virus and shit
- follow secure password policies (complex good !)
- follow best practices for user account security (user, escalate if needed)
- configure system restore points
- perform regular backups
- turn off / restart pc regularly

Vendor Drivers

- most large vendors (Dell, Lenovo, HP, etc.) provide a utility that can automatically check for updates and drivers.
- allows auto bios and driver updates for system
- can and will restart your shit whenever because they can >:)

Troubleshooting: Desktop Utilities

March 7, 2023 8:10 AM

Windows tools

- computer management
- GPresult
- ipconfig
- nslookup
- traceroute
- systeminfo
- tasklist / taskkill

computer management

- compmgmt.msc
- gives you access to a bunch o utilities

ipconfig

- /all
- i know what this is

nslookup

- easy to figure out IPs (if you have dns)

traceroute

- shows you hops between source and target
- **we should use this more often**

systeminfo

- returns info about PC
- 'systeminfo'
- /s <computer> /u <domain>\<username> /p <password>
- /fo - formats the results as table, list, csv

tasklist

- displays running processes
- /s - goes to another PC | /fo - format | /fi - filter

taskkill

- /s - go to another computer, /fi - filter, /pid - the PID you want to kill, /im - to kill by name
- ex. taskkill /pid 2001

GPResult

- /r - displays the RSoP summary data
- /z - displays ALL info
- /v - verbose
- /scope:

IP/Port scanner

- can scan for open IP addresses
- can also scan for open ports (which is kinda dangerous)
- can generate a shit load of generate a ton of network traffic

disk health checks

- power-on hours, temp, SMART checks
- (read error rate, spin up time, start/stop count, power on hours, disk shift + more)

Email header analyzer

- check if an email is spam
- the header gives you all info you need > header analyzer gives you nice info

Storage Scanner

- shows file storage (what things are taking up space)
- break it down by location, size, and folder type
- WizTree or TreeSizeFree

MSRA (Microsoft Support and Recovery Assistant)

- can do advance diagnostic of office and windows 10 config problems
- detailed reports
- auto fix common issues

Remote connectivity analyzer

- web resources by MS to check connectivity to exchange or 365 servers
- for fixing mail problems
- IMAP or POP checker
- check SSO issues
- can check Exchange active sync

ForensIT

- tool that migrates user profiles
- capture profile as a zip file > extract it to a target PC

COMP1400 - Review (MASTER REVIEW GUY!)

March 14, 2023 8:11 AM

What is a ticketing system?

- keeps record of customer trouble and issue with technology

How does it work?

- ticket creation - either an automated system, or done manually
- notify user that ticket is created/queued
- is it an incident report or incident request?
- solve yourself
- or pass it on to someone else who can

Why Ticket?

- ticket number was the og queue method

applications of a ticketing system:

- user support
- security problem management
- issue tracking / incident management
- it requests

advantages and disadvantages

- disadvantages
- may require IT infrastructure (server, OS, bandwidth)
- maintenance (updates, security patches, application updates)
- requires support/licensing (can be real expensive)
- staff training
- compatibility issues with existing systems

- advantages
- keeps you organized
- tracks issues
- lets you keep track of your workers

Terms:

Service desk - single point of contact within a company for managing customer incidents and service requests (mostly incidents and service requests)

Help desk - a single point of contact within a company for technology-related questions and incidents

Technical Support - a wide range of services that enable people and companies to effectively use information technology

Service Level Agreement - a documented agreement between a service provider and a customer outlining the expectations for service delivery. (usually about service provider not messing up)

Root Cause Analysis - a procedure used to uncover the underlying cause of a problem

Incident / Incident Report:

- an **unplanned** interruption to an IT service or a reduction in the quality of an IT service
- ex. broken device, error message, a system outage

Problem:

- the cause of **one or more incidents**
- ex. hardware defects, corrupt files, software errors or bugs, and human error

Service Request:

- a formal request from a user for something to be provided
- ex. request for info, advice, or a standard change

Core Customer Service Components:

Greeting

- basic hello, good first impression

Validation

- get customer info

Investigation and diagnosis

- Questioning and Listening
- **close ended** questions - yes or no answers, "are you logged in?"
- **open ended** questions - requires a response, "can you show me the error?"
- **probing** questions - follow up / clarification, "you mentioned ... "
- **confirming** questions - usually used after probing questions, to understand the symptoms, error messages, relevant data

Resolution

- technical
- quick fix
- informational
- **use your resources**

- knowledge base
- standard procedures
- best practices
- solutions/hotfixes

- peers
- vendors
- documentations

Closure

Hold (DATE)

- **D**escribe: reasons, steps and time frame
- **A**cknowledge and confirm understanding
- **T**ake timely actions and watch time
- **E**xpress gratitude and personalize

what if customer puts YOU on hold ?
(ask if rn is a good time, call back later)

Mute

- like sneeze or cough or something, don't do it for long
- use hold for longer time

Transfer and Escalate (customer side)

- sending an issue to another resource
- reasons for escalation:

- customer asks for it
- VIP - special privileges
- High priority
- time
- expertise
- right or access
- exhausted knowledge options
- frustrated, tired or overwhelmed

- tell the customer about escalation (why you're doing it)
- give them the next steps (gonna send you to tier 2, this is your ticket number etc)
- confirm understanding

Transfer and Escalate (internal side)

- update contact info - make sure you can contact the customer
- error messages
- screenshots
- troubleshooting steps and results
- categorization and prioritization
- attached and knowledge articles utilized

Main reasons for customer issues

- skill diff (customer is not trained on tech)
- upgrade diff (didn't go through properly)
- product isnt working correctly
- system is genuinely slow
- customer is using outdated equipment or software

Communication

- most people prefer face to face over email because body language
- people can write in a different tone than they are feeling

Recovering Unsatisfied Customers LEAD

- **L**isten - carefully to understand source of conflict and how it makes them feel
- **E**mpathize - and acknowledge the conflict
- **A**pologize
- **D**iscover the source

How to deal with:

- impassioned customers - listen and empathize
- combative customers - listen and empathize
- chatty customers - ask "is this good now?"
- timid - ask directly yes or no questions

Service Desk Analyst:

- referred to as tier 1 or level 1 support
- serve the entry point for the single point of contact (SPOC) model

Customer Support Channels:

- phone
- remote
- email
- face to face
- chat
- text

Service Desk Analyst responsibility:

- resolving break/fix issues
- fulfilling requests
- following processes and procedures

- communication and troubleshooting via various channels

ITIL - service management life cycle

- strategy
- design
- transition
- operations
- CSI

★ **ITIL - service management processes** (don't need to know the definitions, but good to know of them)

- incident management
- problem management
- request fulfillment
- demand management
- release & deployment management
- change management
- service-level management
- knowledge management

Incident Management

- log > prioritize > investigate > communicate > resolve > review > closure > (circle)

Problem Management

- fix the problem bro idfk

Request Fulfillment

- initiation > approval > fulfillment > management > (CIRCLE)

Demand Management

- fuck you dont need to know

Release & deployment Management

- request for changes or new features > release planning and design > software build > review > test > deployment > support > issue reporting and collection > CIRCLE

Change Management

- services need to be: stable reliable, and predictable

1. understand and minimize risks while making IT changes
2. Make sure change consequences are planned for
3. make sure everyone that the change may impact is informed
4. make sure the IT services stay stable and reliable with minimum impact on production

Knowledge management

Server Troubleshooting

March 28, 2023 8:14 AM

GPO Review
- GPOs are applied at different places to have effects on users or computers.
- GPOs apply from the bottom up, so a domain GPO does not overwrite Local.
- GPOs only affect OUs, **not** containers
- Computer Policies - only affect user PCs
- User Policies - only affect User

GPO best practices:
- make OUs for computers and for users separately
- GPOs on these OUs for more granularity, and easier to see what's happening
- also keeps it cleaner

GPO Modeling
- doesn't act as the GPO, but lets you see if it would have worked or not
- good for testing changes before you apply them

GPOZaurr
- builds an HTML summary of existing GPOs
- great for when you take over an environment you are not familiar with
- use with caution, but it is cool and powerful

```
Install-Module -Name GPOZaurr
Import-Module GPOZaurr
Invoke-GPOZaurr
```

DNS - (it's always DNS)
- critical infrastructure
- needed for domain to work, as well as connection to internet
- systems have a HOSTS file (this overwrites any normal DNS resolution)
- installed on a server

DNS - Things to check:
- adapter settings (ipconfig /all)
- confirm servers are up
- check hosts file
- check DNS is running
- check records on server
- DNS forwarders

DHCP
- provides network connection info automatically
- "technically" not required but like. come on.
- will provide IP and DNS

DHCP - Common Problems
- network issues stopping initial DHCP lease
- server not on / DHCP not started
- IP exhaustion

Shadows Copies - VSS
- act like snapshots (point-in-time backups)
- good option on file server
- IS NOT A REPLACEMENT FOR A REAL BACKUP

right click volume > configure shadow copies
then settings - location of backups, schedule of backups, storage limits (configure these)

right click on a file - restore previous versions

iDRAC - out of band management
- a dedicated card that has a network connection and can be connected to via web.
- acts like you are in front of the server with a keyboard monitor and mouse.
- iDRAC is the dell brand name

Exam 2: Troubleshooting Review

April 18, 2023 8:04 AM

the one question:
- you will have to know some of the switches for searching he registry - RegQuery : have to interpret some of the switches on it (its common sense) - true false question

desktop troubleshooting:
server troubleshooting:
network troubleshooting:

Desktop Troubleshooting

Main windows system stuff:
- install locations (program files / program data / appdata)

admin shares
system 32
registry

utilites built in to windows
- regedit, tasklist, taskkill, DISM + SFC, etc.

third party tools
- disk checkers, MSRA, remote connectivity analyzer, etc.

Windows 10 reset

windows 10 has a refresh, reset or restore function

Refresh - refresh windows without deleting any personal files or apps
- third party apps will be deleted

Reset - will remove everything and reinstall windows

Restore - goes to a specific point in time as a restore - they are auto created if they are enabled (can create manually)

DISM + SFC
- deployment imaging servicing and management - compares your windows image to a known good windows repository (default looks at online)

System file checker - compare protected system files against a local cache

sfc /scannow - runs scan

when do we use them?
windows wont boot, or its acting weirdo
★ - run DISM command first, then SFC second
both commands take time

App installations

Program Files - 64 bit apps

Program Files (x86) - only created on 64 bit windows for backwards compatibility (it is 32 bit apps)

Program Files & Program Files (x86) need administrator rights

ProgramData - less restrictive because it is a hidden folder, can be edited by anyone. usually info for multiple users - shared cache, shared settings, shared databases (**used if a program needs to write something** - so it doesnt have to ask for admin privs)

users\<username>\appdata - only installs for a specific user - don't need admin privs. (discord for ex.)
  - roaming - follows you between pcs in a domain environment
  - local - doesn't follow you between pcs
  - LocalLow - for temp files and the like

Desktop troubleshooting 3rd party

IP/port scanner - can scan for IP addresses on the network, sometimes for open ports too (used for security sometimes)
  - angry IP scanner
  - Advanced IP scanner
  - nmap, zmap

Disk health checks - checks the health of hard drives - shows drive info like power-on hours, temperature, SMART checks

- tools written at the bit level
- seatools is one of the tools for this

Email Header Analyzer

- checks header info to see where the email came from (see if it is legitimate)
- allows you to read the header info in human words
- mx toolbox, appriver - these are tools to read them

Storage Scanner - used to assess free storage or find the large files taking up space

- breakdown by location, size, and file type
- with admin perms sometimes you can delete files
- WizTree, TreeSizeFree - tools for this

MSRA - microsoft support and recovery assistant - utility that can do diagnostic for office / windows 10 configs

- just for microsoft stuff

Remote Connectivity Analyzer - used to check if you can connect to exchange

- useful to check for new imap / pop3 servers

ForensIT - migrates profiles over

- keeps everything the same after transferring your profile (keeps all settings and personalization)

Shadow Copies - VSS - allows you to do system restores for specific files/folders

- comes built in with windows,
- act like snapshots - point-in-time backups of data and files
- can be used by third party applications

- system restore, windows server backup, shadow protect

★ **DOES NOT REPLACE A ROBUST BACKUP SOLUTION**

Shadow Copies ext.

- MS recommends a dedicated drive for shadow copies (it will run out of space)
- if it has been running - "restore to previous version"

Server Troubleshooting

event viewer
file permissions
gpo modeling and testing
ad health / replication
dns and dhcp issues

File sharing settings: by default they are inherited

- Share permissions
- NTFS permissions

Special NTFS Permissions

- traverse - pass through a folder to folders below
- list - list the contents of a folder
- read attributes - read the attributes of a file in the folder
- write attributes - change the attributes of a file in a folder
- change permissions - change permissions of the contents of a folder
- take ownership - take ownership of a folder

etc.

an administrative share is created by default on each volume (\\<PCname>\c$)

Windows Utilities

GPResult - shows the result of GPOs on the system for this user
ipconfig - shows network settings
nslookup - for dns query
traceroute - follows a ping
systeminfo - info about a system
tasklist/taskkill - find and kill tasks
event viewer - lets you view event logs - show errors and warnings

Troubleshooting Methodology

general approach:

- identify problem
- establish theory
- test theory to see if youre right

- establish plan of action to resolve
implement the solution or escalate
verify full system function
document

★ **ABC 5 steps progrm**
bottom up, top down, other one

A. **check the political layer**
B. **Check the physical layer first**
C. **do a quick ipconfig /all**
1. **ping yourself 127.0.0.1**
2. **ping neighbor > can you connect to lan**
3. **ping gateway**
4. **ping remote IP address (8.8.8.8)**
5. **ping google.ca - dns**

bottom up:
start at physical layer and work your way up

divide-and-conquer:
- you have an idea of where some issue may start - "i think it is network issue"

top down:
- from application layer down, (we usually don't use this. only if everything else is working except 1 app)

Network Troubleshooting Tools
- protocol analyzer
- cable analyzer/tester
- SNMP monitoring tools
- centralized log management
- WiFi analyzers

UNICAST - know the logical and physical address of the target
BROADCAST - communication message when you know nothing
MULTICAST - sends to multiple addresses (you know just the logical address)
DEFAULT GATEWAY - the source out to the greater inter/intranet
TCP - connection-based protocol with more overhead - connects to a specific guy and talks to him
UDP - connectionless protocol with less overhead - screams into the void
IPV4 - a 32 bit address for a network interface
IPV6 - a 128 bit address for a network interface
CIDR - the name of the fully qualified guy with subnet (192.168.1.25/24 as ex.)
APIPA - 169.254.x.x - used when you don't have an IP address in ipv4 from DHCP
DHCP - dynamic host configuration protocol
DNS - domain name system, converts IP to name
ICMP: Ping, Tracert & Pathping - tool used for network troubleshooting
ARP/RARP - procedure for mapping a dynamic IP address to a permanent physical machine address in a lan
NSLOOKUP - a command used to send a dns query to the dns server for a specific hostname
FTP/HTTP/TFTP - file transfer protocol, hyper text transfer protocol, trivial file transfer protocol
ISP - internet service provider
AUTHENTICATION - checks to see if you are who you are
AUTHORIZATION - do you have the access you need for something?
PUBLIC IP - can only be 1 on the internet (private are not public)
SWITCH -
ROUTER