AD review

January 9, 2023 12:11 PM

AD:

- database that contains info about all users computers and accounts in the domain
- domain represents a single company
- controls authorization and authentication, policy, and control
- multiple servers can share a single database (replication)

AD installation:

IP MUST BE UNIQUE AND STATIC
NAMES MUST BE UNIQUE
install AD DS
promote to DC
create a new domain or join existing domain
DNS zone is created

DNS: actually required
ties names to IP addresses
reverse - IP to names

DHCP: basically required
assigns IP addresses and (can be setup for) other info to devices on the network automatically

Best Practices:

- Default Administrator is **NEVER** used. Copy it so you have a template user, then **disable** it.
- Domain Admins are **not used for normal operations.**
- Techs will have 2 accounts: a **normal user**, and an **admin user**.
- Add users to groups based on their role.
- Permissions are assigned to Groups, **not users.**
- Documentation is **VERY** important.
- Firewalls should stay on. Configure rules to allow traffic if needed.
- A GPO can set basic firewall rules for the domain. (default for ICMP traffic for example | hint)
- ADP can be managed remotely
    - Remote Desktop (RDP) - individual endpoints
    - Remote System Administration Toolkit (RSAT) - Domain Users, GPOs, DNS
    - Windows Access Center (WAC) - server and domain management
- Most admins set up a dedication workstation with those tools installed and set up (hint)

Expectations:

- use admin workstation
- login with normal user, elevate if needed
- firewalls stay on

if not: penalties can occur (if thing that is submitted does not follow those)

File Servers - Access, Permissions, and GPOs

January 16, 2023 12:06 PM

File server - main job is to host files, can do other but usually doesn't
- centralizes important data (makes it easier to backup/restore)
- multiple servers can work together using DFS (distributed file services)

File Server set up:
- Folders are shared to the company
- usually one per department, and a public share for everyone.
- possibly other shares for utils/apps

Best Practices:
- dedicated hard drive on the server for shares (not on C:\ drive)
- top level folders for each use case (E:\Shares\whatever)
- keep names short (256 character limit for share path)

Don't do:
- if putting shares on C:\ drive - could lose OS, would lose all data on it (shares)
- make specific top level folders on the drive (E:\Data\whatever is better than just E:\whatever, scalability and what not.)
- DON'T SHARE E:\ - this is a root directory, and bad to share

Permissions:
- limit data using share and NTFS permissions
- permissions are inherited
- more restrictive >>>

Drive Mapping:
- use a drive map to make a drive that is of \\Accounting\FolderName\Number1 for example
- it can be done manually, but is annoying
- use GPOs as best practice - auto maps drives (can do it based on membership)
- location of GPO will determine who gets affected
- affects user accounts

Drive Map Options:
- action: sets behaviour
- Location - share path of share
- Label
- Specific drive letter - N:\, P:\ (network, public) are common
- Could also set every department drive to be set to E:\ for example, (this is kinda messy, don't do it) - called item level targeting

Roaming Profiles:
- for users logging into many PCs (gives settings and files and preferences)
- roaming profile basically follows user between PCs
- usually used today for configuration and settings rather than data
- "Roaming Profiles" are the old way of doing it.

new way:

Folder Redirection:
- auto copies files/folder from local PC to File Server
- saves data in case of drive failure
- copies of their data are made available at any workstation for a user
- if you redirect %appdata% you can mimic roaming folders (settings and configs)

Folder Redirection setup:

- use different top level share on root, which is hidden (E:\Users$ or E:\Folder Redirection$ as example)
- new security group to have permissions for redirection
- GPO to apply redirection for those users
- Setup folder under Folder Redirection Share (E:\UserData$\qparent1 as ex.)
- permissions for the hidden shares are automatically setup for privacy

File permissions are on the File Server
GPOs are on the DC

Sites and Domains

January 23, 2023 12:04 PM

Sites:
Control Replication:
- interval of replication
    - instant or 15 seconds wait for update (intra site replications)
- replication routing

Client Affinity:
- which DC a client logs into

Intra site - within same site
inter site - in multiple sites

Site - AD objects that represent **one or more TCP/IP subnets - highly reliable, fast network connections** (definitions of this may vary)
- we use 192.168.10**X**.x for example in different "sites" or vmnets
- makes replication easier (intra site DCs replicate nearly immediately, without it delay and chaos would ensue)
- allows clients to log into a closer DC rather than having to go across the world every time (client affinity)

Inter Site Connectivity:
- sites are connected by site link objects - we can assign a cost (lower = better) for priority
- replication interval by default is 180 (minutes or 3 hours)
- the site link is made by the KCC (knowledge consistency checker)
- you can also set a schedule for when inter site replication happens if you need to conserve bandwidth

INTRA site replication - Immediately or 15 second delay
INTER site replication - 3 hours by default (can force replication)

Bridgehead Server - responsible for replicating changes for its whole site to other bridgehead servers
Client Affinity - prevents logon authentication traffic from leaving site, this preserves WAN bandwidth

Why are sites important?
- replication traffic control
- login authentication traffic control

lab 3 demo notes

January 23, 2023 12:37 PM

active directory sites and services

dc1:

- rename site to calgary or whatever
- make a new custom link with first and new site in

new site

- use custom link to make a new site

subnets folder:

- new subnet
- site subnet ip - select which site its for
- do for old and new site (2 subnets)

dc2:

- set to static ip, set dns server as DC1 (need router powered on)
- install AD DS
- make it a standalone server, *then* join it to your domain
- add domain to existing domain
- looking for site name to automatically select **NEW site**
- replicate from any domain controller - fine for now, however now that we are doing more with it, use the closest DC

can now use admin workstation to manage both DCs

users and computers:
wont show up on dc2 yet

FORCE REPLICATION:
DC1 -> SITES AND SERVICES -> NTDS SETTINGS -> REPLICATE

- this can either pull updates from another DC, or push updates from that DC

command prompt:
'nltest /dsgetsite' - tells you what site you're connected to

for joining client:
new client either needs DHCP or static IP with correct subnet
DNS - closest DC server

make sure DNS works or you're idiot

multi domain setup and FSMOs

January 30, 2023 12:05 PM

- AD DS is a hierarchy that stores info about objects on a network

Multiple domains:
domains are triangles - they all have their own:
- domain admins
- domain root servers
- security groups
- trust relationships between domains

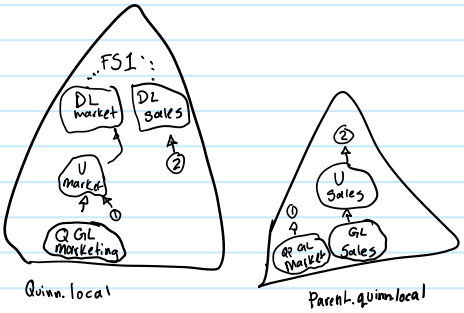
- domain admins - the administrator for that domain
- enterprise admins - they are the admin of the whole forest > **be careful who is in this**

adding a child domain:
- in AD DS configuration > add a new domain to an existing forest
- domain type > child domain
- parent domain name > 'acme.ca'
- credentials need to be of the DOMAIN not of local admin

verifying child domain:
- active directory domains and trusts > should be under the main domain now
- dns manager > should be under the main domain name as a name server (this is to check for file servers or whatever on the child domain from the parent one, and vice versa)

to remove child domain:

- remove AD DS feature/roll



AGUDLP -
- global - only come from local, can access any domain
- domain local - can come from any domain, only access local domain
- universal - can come from any domain, can access any domain

Flexible Single Master Operations (FSMO)
- to prevent conflicts, only one DC in the entire directory is allowed to process updates
- standard replications use Multiple Master Model (multi replications)

five operations master roles:
- schema master
- domain naming master
- RID master
- PDC emulator
- Infrastructure master

- Forest root server - first DC installed in top level domain
- Domain root server - first dc installed in any domain

FSMO: Schema Master
- schema master is the DC responsible for performing updates to the directory
- schema = blueprint/framework for AD database - objects and properties where they get stored in NTDS.dit

- this DC is the **ONLY** one that can process updates to the directory schema
- one per forest - is the forest root server

FSMO: Domain Naming Master
- the domain naming master is the DC responsible for making changes to forest-wide domain name space of directory (like quinn.local)
- This DC is the only one that can add or remove a domain from the directory
- one per forest - is the forest root server

FSMO: RID (relative ID) master
- RID master is the single DC responsible for processing RID Pool requests from **ALL DCs** within a given domain
- when a DC creates an object it gets an SID #. It gets them from the RID Master - max of 500 SIDs at a time
- one per domain - domain root server

FSMO: PDC Emulator
Primary Domain Controller was a role from Windows NT (1993-1999)
was the "boss" server and held the only editable copy of the NTDS
- responsible for windows time service for kerberos authentication
- all DCs sync their clocks to the PDC emulator - does it every 60 minutes
- used for account lockouts are also managed by this role
- one per domain - domain root

FSMO: Infrastructure Master
- infrastructure FSMO is the DC responsible for updating object SIDs and distinguished name to other domains
- this Infrastructure master in one domain will update the changes for its objects with an infrastructure master from another domain
- one per domain - domain root

Transferring Roles to Another Server:
- Active Directory Users and Computers > delegate control
- or ntdsutil.exe
- if a DC dies suddenly, seize the role and transfer
- **DO NOT BRING IT BACK ONLINE**

lab 4 demo - partner guy

January 30, 2023 12:46 PM

plug Vmnet 1 into Vmnet 1 for both side of partner guy

hosted server:
- open server manager
- change IP address to a static IP
- they can now do everything they need

on your DC - active directory sites and services
- make links for all your guys
- setup subnets of your guys

when you're promoting DC3 to AD DS
- add a new domain to an existing forest
- child domain
- parent domain > quinn.local
- child domain > parent
- create DNS delegation > check that box yo

you can use the same account you already have (firstnameAdmin)

AGUDLP

accounts
global groups
universal groups
domain local
permissions

users > global group "G_<name>" on all domains that it must exist

global group > universal group "U_<name>" on the parent domain usually (only needed once)

universal group > domain local "DL_<name>" on the same domain as the resource you are trying to access

Imaging and Deployment

February 6, 2023 12:10 PM

goal of imaging and deployment -> if the time it takes to setup a new device is minimal, the device is basically disposable

What is it?

- process of installing a pre-configured OS (all drivers, apps, settings,)
- reduce workload on the it staff
- allows faster turnaround of new systems
- allows quick refreshes of faulty systems

Image - file that contains the OS (.iso, .img, .wim)

Multiple Images can exist next to each other

- depending on drivers (AMD, Intel, etc.)
- different software (accounting, engineering, etc.)
- different OS (server, desktop)

Gold Image - common "factory default" image from a company

Deployment - the process of installing an image onto a piece of hardware, or VM

- can be done from a USB, CD, or most commonly **network**
    - ****need DHCP**, DNS needs to work too, physical infrastructure**
- requires extra infrastructure to enable

2 main deployment methods: Image based and orchestration based

- **Image based:** capture a specific state and save it, then deploy - quicker, easier
- **Orchestration based:** applies a series of steps to modify an existing OS - more customizable, more setup

Why?

for IT team:

- minimizes mistakes (we're human)
- save time vs manual installs
- allow quick turn around of re-installing OSes

for End Users:

- standard environments, less learning curve
- minimize interruption of users

Deployment Strategies:

High-Touch:

- manual deployment, you run installer yourself

Lite-Touch, High-Volume Deployment:

- limited interaction during deployment, basically you need to click start

Zero-Touch, High-Volume Deployment:

- requires no interaction, fully automated process (through system center configuration manager)

Deploying an Enterprise Workstation: (image)

1. Build a deployment share

- location on the network that holds your images, accessible to the workstation

2. perform a reference computer installation
   - setup a pc or VM to be the gold image
3. capture an image of reference computer
   - software will create an **image** of that reference computer
4. boot the target computers
   - turn the PCs that are getting deployed to on
5. apply the windows 10 reference computer image

Image types:

Thick Image
- everything is on reference PC, and included in capture

Thin image
- minimum installed on the reference PC, other items are installed after deployment (orchestration)

Hybrid:
- install a baseline, but some people need some more software - this is how you do it

Deployment Tools (1st party):
- Windows Deployment Services (WDS) - server role, network and file sharing, Lite-Touch deployments
- Microsoft Deployment Toolkit - extends WDS and allows some orchestration

Windows Deployment Services (WDS)
- server role in server 2016+
- used to deploy images over network rather than in person
- DHCP is required
- Pre-Boot Execution Environment (PXE) must be supported across infrastructure - both server & end device

Microsoft Deployment Toolkit (MDT)
- requires Win10 ADK to function for deployments
- creates **Task Sequences** for automation
- Tasks can be before or after installation (partition drives, inject drivers, install apps, etc.)

MDT Ex.
- gather info (hardware, type of CPU)
- partition and format drive
- inject drivers
- apply OS
- windows update
- install apps

Windows 10 ADK
- customize existing Windows Images
  - WinPE, sysprep, etc to do that
- WinPE is a mini OS used to install, deploy and repair windows Oses
- also can be used to capture windows images
- can help testing performance

- has a bunch of pre installation, and management stuff on it (comes with windows)

Capturing Images
- manual or automatic

- simple or complex
- one single image
- one image per department

Capturing using WDS
- automates capture process
- wizard-based
- create capture image and upload to WDS server
- can be deployed immediately

Deployment Image Servicing and Management (DISM.exe)
used to modify image files while offline
- add drivers
- languages
- packaged updates
- enable or disable OS features
- append a volume image to a workstation image
- combine multiple images in a single Windows Imaging File

Deploying Images Using WDS
- any image can be uploaded to WDS (regardless to deployment method) and deployed (needs boot image, WinPE)
- Multicast with WDS (aka deploying to many things at once)

Deployment Images Using MDT
- some overhead is required
- add images to deployment share
- create **task sequences** to apply images to target computers
- multiple sequences can be created as needed
- sequences can be simple or complex
- more complex = more work

Performing a Lite-Touch Deployment
with WDS
- boot computer, specifying a network boot
- select the correct image to be installed
- more interaction may be required depending on the OS

with MDT
- Boot the computer
- run deployment wizard
- select task sequence
- more interaction may be required depending on sequence

Less interaction = more preparation for deployment

System Center Configuration Manager (SCCM)
- required for Zero-Touch installation
- complex
- can be used to capture and deploy image files in the same basic sequence as LTI (?)
- SCCM tools instead of Deployment Workbench

- only use this product for deployment if you are already using it
- huge pain in the ass and very complex
- stores data in SQL database

- requires client agent on each computer it manages
- very expensive but powerful

Common Issues

- networking - need **DNS, DHCP,** and support for **PXE booting**

drivers - not a problem for VMs but for stuff with different hardware :/

- need to keep images up to date (windows updates, driver updates, etc.)

WSUS (windows server update services)

February 13, 2023 12:56 PM

downloads updates from windows > then acts as the server that updates client PCs

different types of microsoft updates:
- critical update - fix critical, non-security related bugs
- definition updates - additions to definition database
- feature packs - adds new product functionality (ex. 21h2)
- security updates - updates for security vulnerability
- service packs - dont really exist anymore - used to be hotfixes, security updates, and regular updates
- update rollups - basically new service packs, hotfixes, security updates, critical updates, and regular updates, packaged all nice
- monthly rollups - multiple updates packaged - every second tuesday

WSUS: can act as the windows update server
- control the timings of updates
- bandwidth of updates
- types of updates
- allows testing

Timing:
- if something goes down it can be annoying to catastrophic (surgery, or in the middle of the work day)
- Does all updates when everyone is at home

Bandwidth:
- WSUS server acts as a relay
- this means you don't flood your network with downloading and installing windows updates on every single PC in your environment (do it from one location already on your network)

Types of Updates:
- can prioritize different update types
- can categorize server updates, client updates, azure updates
- can pick and choose updates we want on hand

Testing:
- can test an update to make sure nothing gets broken with the new update

Windows Server Update Services:
- role in windows server
- centrally manages updates
- synchronizes with microsoft update servers to see what is out there available for updates (goes back forever) (THIS DOES NOT DOWNLOAD, IT JUST INDEXES)
- can distribute updates to all, or groups of clients (separate from AD)
- allows uninstalling updates from clients

WSUS deployment strategies:
single WSUS deployment
- microsoft update server > through cloud > firewall > WSUS > clients

★ Hierarchical WSUS deployment
- microsoft update server > (a downstream from updates) > server a > (b downstream from a) > server b > clients
- server b can search only server A

(Hierarchical) Autonomous Mode (default)
- upstream WSUS server shares its updates with downstream servers
- downloaded updates are approved from each downstream servers

(Hierarchical) Replica Mode
- upstream WSUS server shares its updates with downstream servers
- downloaded updates a re not approved from each downstream server, but from upstream WSUS server

note:
- WSUS isn't always necessary, especially more recently - bandwidth is available, and updates are stable.
- 3rd party management platforms are being used more and more (RMM, Intune, SCCM)
- probably need **something** to centralize / control updates

Active Directory in the Cloud (exchange)

February 27, 2023 12:02 PM

exchange relies on AD to exist for it to work, in the cloud this is true as well.

on-prem: your hardware
hosted: some else is running the hardware
hybrid: combo of on-prem & hosted

hosting the AD in the cloud:
- would work in theory
- cost a shiiit load of money (super resource intensive = super money intensive)
- plus now you need to know about cloud stuff too which is :/

Microsoft cloud structure:
- create a 'tenant' - container for all the Azure subscriptions
- tenants are hosted on MS hardware, in MS datacenters
- they are also independent from each other, no tenants can interact
- many products/services can exist in the tenant, it can also be bundled (ex. M365)

everything is in your tenant - big ol container

Microsoft 365
- used to be called office 365
- SaaS, ADDS functions and services in the cloud
- includes a whole ton of shit
- fully cloud

Traditional AD is **fully On-Prem**
- can connect our local AD to our tenant using Azure Active Directory (AAD)
    - passwords, users, GPOs, policies - on prem
    - licensing, data storage, email - in cloud
- hierarchy, DCs contain OUs, contain Objects and groups

Azure AD can be **fully online**
- good for new, small businesses (don't need a ton up front for servers)
- need more functionality ? click button and pay :)
- flat structure, access controlled by assigning roles
- requires a service running in AD to sync at regular intervals

Azure AD Sync
- utility that runs on one of our DCs
    - ★ run with service account
- takes AD hierarchy and convers it to a flat format, then pushes to Tenant
- default - only writes one way (AD to Tenant) but can be configured to by synchronous

Azure Tenant Accounts
- users in local AD will be given an account in Azure AD
- on-prem, username format is DOMAIN\qparent or qparent@domain.local
- default Tenant accounts will be qparent@domain.onmicrosoft.com
  (same account, just has a different UPN because cloud v on-prem)

users in the tenant need to pay for things via licensing

- this is expensive as balls

Exchange Online

- Azure AD - allows us to do exchange online
- exchange 2025 probably the last on-prem exchange thing ever ???
- running in the cloud - waaaay easier

Shit will change, Microsoft sucks.

- screenshots are dumb as hell fuck this shit bro i wanna go home :(

Exchange - Intro and Install

February 27, 2023 12:54 PM

MS Exchange - messaging and collaboration server, (also has calendar resources)

how email works:
- sender mail client (MUA) | gmail or outlook for example
- sender mail server (MTA) > looks for the recipients mail server (MTA)
- Recipient's Mail Server (MTA) does spam & virus checkers
- recipient mail client (MTU)

Mail User Agent (MUA) - user interacts
- how a user interacts with stuff, also known as a mailbox or email client

Mail Transfer Agent (MTA) - sends email out
- user writes and sends email to mail server using MUA
- software used by email server to forward the mail from the MUA

Mail Delivery Agent (MDA) - gets the email to the recipient
- if external to org, MTA sends the message via internet to destination mail server
- recipient mail server uses its MDA to deliver the email to recipient's mailbox
- then they access it through their MUA

Mail Server DNS
mail requires quite a few DNS records to function
need:
- MX record
- A Record

technically optional (do it anyways):
- PTR Record
- SPF Record

MX (mail exchange) record
- specifies a mail server that handles a domain's email
- used by mail servers to find other email servers on the internet

MX records have an additional attribute called preference/priority
- mail attempt to deliver to the lowest preference value first if they get a response for that server
- if you have round robin configured on DNS server, easy load balancing

A (host) record
- all servers and clients require at least a single A record
- these DNS records need to be externally published for other mail servers to determine your server (DMZ)
- Time to live (TTL) can be important especially during mail migrations/DNS changes

PTR Record
- basically checks to see if the email is actually coming from where it says its coming (this counters spoofed emails)

SPF Records
- special text record that proves domain ownership
- may be generated for you by a provider, or reference an external IP of your on-prem server
- you may be marked as spam and have your traffic rejected if this is missing

Exchange on Prem Server Architecture
- Exchange On-Prem will require that your AD Schema is modified - if your environment is not healthy, it will break your shit, dog.
- Data related to Exchange is stored in a special Database on the Server
- Multiple databases are supported and common. (locations, archiving, backups, executive, etc.)

on-prem servers have 2 roles:
- exchange will function with just a mailbox server, the edge roll increases security

- **mailbox server role** - handles all activity for the mailboxes and client access (hosts databases, etc)
- **Edge transport role** (optional) - deployed in the perimeter network, handles all internet-facing mail flow (applies anti-spam and anti-virus)

Exchange online architectures
- all in the background
- cant see anything easily
- magic :)

Mail Access Protocols

POP3/POP3S - ports 110 and 995 (STAY AWAY AND SUCKS ASS DONT USE)
- Post Office Protocol
- retrieves and REMOVES email from the server when the client accesses an email
- defunct (DO NOT USE) in favour of IMAP

IMAP4/IMAP4S - port 143 and 993
- Internet Message Access Protocol
- retrieves email from the server without removing it
- mailbox contents are synced between server and client - mailbox is persistent across devices :)

HTTP/HTTPS - ports 80 and 443
- used by browser for OWA (outlook, gmail, whatever website)

Autodiscover service
- allows quick exchange account setup without MUA entry/configuration
- leverages DNS to achieve this typically using CNAME and SRV records
- points to a server that contains all the default exchange configuration information for your mail client

ActiveSync or Exchange ActiveSync (EAS)
- used by mail clients (MUAs) to sync with exchange mailbox
- intended for high-latency/low bandwidth scenarios (roaming mobile devices)
- these days its autodiscover

Availability service
- allows clients to use calendar and meeting/booking scheduling

Mail Transport Protocols

SMTP or ESMPT
- Simple Mail Transfer Protocol (E = Extended)
- ESMTP is newer and is the mainly used one because it supports graphics, audio, video, and multiple languages
- port 25 or 587

server to server, not client to server

EAC (exchange admin center that is accessible via a webUI)
EMS (exchange management shell) - basically just powershell with extra shit for exchange

Exchange Online Setup
- running server in "the cloud"
- mail-flow is the same theory
- DNS is still required
- management is the same - Web GUI or shell
- requires active directory - can be on-prem or cloud
- with on-prem AD we make the sync process so data in the cloud and on-prem is the same

what we are doing:
- create a new tenant and sign up for a 60 day free M365 trial
- need credit card, can immediately cancel
- install the AD sync tool on the network and complete a sync
- assign licenses to users

conclusion
- exchange server is a huge application
- it is basically the only mail server than anyone ever uses (amazon uses this dog)
- will give you a good basic working knowledge of exchange

- complex but there is tons of info out there (GOOGLE!)

Exchange - Recipients and Mailboxes config

March 6, 2023 12:05 PM

Recipient Object - anything that can send or receive an email.

types of recipients:

- mailboxes
- mail contacts
- distribution groups
- shared folders

User Mailbox:

- syncs to the user account **and** their mailbox

External Contact: (doesn't really exist in cloud exchange)

- a contact email (aka forwarder)
- they can't login to the domain

Mail Contact: (this is what we use instead of external contact in exchange online)

- just a contact, no forwarding (they use their own email, not your local domain)

Mail User:

- holds user account and local email address **(NO MAILBOX)** in the AD forest/exchange
- (they get an AD account but not a mailbox)
- would be used for a temp employee or external contractor
- forwards to their email that already exists (gmail or something)

Resource Mailbox:

- object that you can assign when scheduling a meeting
- used for booking rooms, equipment, cars etc.
- can setup options with automation, or manually (max # of people, max length of meeting, etc.)

Mail-enabled Groups:

- can create a group in AD
- allow you to email the group (will get responses individually)
- **security group** - assign permissions to resources and emails
- **distribution group** - only emails
- **dynamic group** - auto updates membership (based on conditions and attributes) emails send to a group send to all with that condition or filter. ex. send email to all 'Managers'

Shared Mailboxes:

- basically a shared email client that users and groups can be shared into
- can be setup to send/receive email

Public folders - stay away

- public directories are a mess, don't do them

Administration Groups - not fully translated over to exchange online

- Recipient Management Role group
- Organization Management Role group - this one is god mode

Admin Roles

- Global Admin - controls everything in the tenant

- Exchange Admin - controls only exchange

Microsoft Exchange Recipient (role thing?)
- object that sends system-generated messages internally

Postmaster (account)
- the object that sends system-generated messages externally

Mailbox Configurations:
- assigning license to an AAD - the mailbox is created automatically
- user's alias will become the user's SMTP address (by default) - (alias@domain.onmicrosoft.com)

  SMTP Addresses
  - SMTP - protocol that passes mail between servers
  - primary SMTP address is someone's "sending" address
  - secondary SMTP address (AKA alias) is configured as an additional email (think like quinn-facebook@gmail.com > quinn@gmail.com)
  - you will still send as your primary SMTP address
  - (used for changed names)

Delegations:
- often needed for different levels of permissions to another user's mailbox
- contains 3 perm types:
- **Send As**
- **Send on Behalf**
- **Full Access**

Send as:
- you send a message that appears on the recipient side as coming from the mailbox owner
- (grant "Send As" on the 'vacant' mailbox)

Send on behalf of:
- allows user to send a message that appears on the recipient side as being sent from the user on BEHALF of the mailbox owner
- used for assistants sending messages for their bosses

Full access:
- allows user to log into that mailbox and access its contents fully
- **does not allow you to send as that mailbox**

Import-Module ADSync
Start-ADSyncSyncCycle - PolicyType Delta

^ sync local to online

Exchange - Managing Email address lists and policies, backups

March 13, 2023 12:09 PM

Address List:

- contains any type of exchange recipients:
- mail groups
- mailbox users
- mail contacts
- mail users
- room and equipment resources

the one main list that microsoft exchange comes with is the **Global Address List (GAL)**

- need to use powershell to manage it

5 sub-lists that are built in

- all contacts
- all distribution list
- all rooms
- all users
- public folders

Custom Address Lists

- smaller custom address lists (can be based off of tags on the user's account or groups)
- must be done in powershell

Best Practices for creating additional address lists

- don't make too many lists - you might have people confused about which to use
- proper naming convention and hierarchy - lets people know who are in it
- Exchange Online uses Object Attributes - like role, group, etc.

Managing Resource Booking:

- resource policies determine how a resource mailbox can be booked

- how early you can book a meeting
- max time
- repeated meetings allowed or not
  - you can set a booking delegate - this is the person who can allow or disallow the use of the room
  - resource mailboxes have a **booking attendant** service turned on by default
- used to auto respond to scheduling requests, and to forward scheduling requests to those who are delegates

can do most of it through EAC
Set-CalendarProcessing

Managing Email Address Policies:

- SMTP (small mail transfer protocol)
- there can be multiple SMTP addresses assigned to recipients
- email address policies define the rules that create email addresses for recipients in the exchange organization

Email Address policy:

- you can change the email address format, priority (lower number better), and what recipients it applies to
- default email address policy can be changed (probably dont) but not deleted, default has the **lowest priority (highest number)**

- can set 2 SMTP address, can send from whichever you want (only one tho)

Microsoft Exchange Backups
- backups and restore are **VERY** important
- used for:

- disaster recovery
- recovery of accidentally deleted items
- long-term retention of data

Microsoft will make sure your infrastructure is good, but your data is on you.

Microsoft Exchange Backups
- a restored mailbox should not be older than 1 day
- a deleted mailbox should be restored within an hour and containing data should not be older than 30 days
- a deleted email should be restored within 1 day and you should be able to restore emails up to 60 days

Exchange has some built in protections for individual users:
- delete an email > trash bin (30 days <?>) > delete again > exchange recycle bin (14 days <?>)
- point-in-time backups are **not supported** inside exchange online (i want to see my mailbox from 3 days ago)

Exchange Native Data Protection
an alternate backup:
- NDP relies on multiple technologies (replication, item retention) to ensure that **multiple copies of every database exist for redundancy**
- if a copy of a DB becomes unavailable, another one is activated automatically - (the mailbox databases are part of a **Database Availability Group**)
- single item recovery - get single items back that have been deleted or purged
- in place and litigation holds - freeze the state of a mailbox for legal reasons
- deleted item retention and soft-deleted mailboxes - how to handle the removal of entire mailboxes

Database Availability Group - just bigger RAID + off site (2) that has backups of everything that is in site1

Email Retention settings - by default 14 days - can be changed
single-item recovery - ability to recover individual messages after retention period expires (enabled by default online)
mailbox retention settings - by default 30 days - can be changed

Exchange Commands:

March 13, 2023 1:04 PM

Import-Module ADSync
Start-ADSyncSyncCycle -PolicyType Delta

Import-Module ExchangeOnlineManagement - imports exchange online module for powershell
Connect-ExchangeOnline - connects exchange online to AD DS

Get-AcceptedDomain - this is to see what domain you are connected to for exchange

Get-MailboxFolderPermission -Identity fred@qparent.onmicrosoft.com:\Calendar | this gets the calendar permission for fred on exchange

Add-MailboxFolderPermission -Identity fred@qparent.onmicrosoft.com:\Calendar -user wilma@qparent.onmicrosoft.com -AccessRights Reviewer
- this is the command to add wilma to see fred's calendar

Set-MailboxFolderPermission -Identity fred@qparent.onmicrosoft.com:\Calendar -user wilma@qparent.onmicrosoft.com -AccessRights editor
- this command allows wilma to edit fred's calendar

proprac -

Add-MailboxPermission -Identity mark@qparent.onmicrosoft.com -user bo@qparent.onmicrosoft.com -AccessRights full | gives bo full access to mark's mailbox

Add-RecipientPermission -Identity mark@qparent.onmicrosoft.com -Trustee wayne@qparent.onmicrosoft.com -AccessRights SendAs | grants wayne send as permission on mark's mailbox

Set-Mailbox -Identity mark@qparent.onmicrosoft.com -GrantSendOnBehalfTo @{Remove="wayne@qparent.onmicrosoft.com"} | removes the send on behalf to permission from wayne to mark

Set-Mailbox -Identity wayne@qparent.onmicrosoft.com -MaxReceiveSize 1MB -MaxSendSize 1MB | this changes the max send and receive size to 1MB for wayne

Add-MailboxFolderPermission -Identity mark@qparent.onmicrosoft.com:\Calendar -user wayne@qparent.onmicrosoft.com -AccessRights PublishingAuthor | sets publishing author for wayne on mark
Add-MailboxFolderPermission -Identity mark@qparent.onmicrosoft.com:\Calendar -user bo@qparent.onmicrosoft.com -AccessRights PublishingAuthor | sets publishing author for bo on mark

New-Mailbox -Shared -Name prospects -DisplayName prospects -Alias prospects -PrimarySmtpAddress prospects@qparent.onmicrosoft.com | creating the shared folder

Add-MailboxPermission -User wayne -Identity prospects -AccessRights fullaccess -InheritanceType all | full access to wayne for shared folder
Add-MailboxPermission -User bo -Identity prospects -AccessRights fullaccess -InheritanceType all | full access to bo for shared folder

Add-RecipientPermission -Identity prospects -AccessRights SendAs -Trustee bo | send as permissions to bo for shared folder
Add-RecipientPermission -Identity prospects -AccessRights SendAs -Trustee wayne | send as permissions to wayne for shared folder

Get-RecipientPermission -Identity prospects | to see who has access and what level they have

New-AddressList -Name CenterDepartment -RecipientFilter "(Department -like 'Center')" | to create address list

March 20, 2023 12:10 PM

Exchange Public Folders
Public Folders - special type of mailbox called a public folder mailbox
- the public folder hierarchy
- public folder content

to create a public folder, the admin **MUST** create a public folder mailbox called the primary hierarchy mailbox

public folder permissions
- a user must have permissions to post/send to the public folder
- public folder permissions can be managed via EAC, EMS, or outlook
- whole hierarchy has permissions

Defining Public Folders administrators:
- Public Folder Management - this is the role to manage
- max mailbox size 100GB (the whole thing)
- max individual public folder size - 10GB (personal)
- max number of public folders - 1 million (this is a bad thing)

Shared Mailboxes
- a mailbox that multiple users can share
  - send, recieve, use a common mailbox
  - generic email (help@..., info@...,)
  - centralize calendar functions (vacations, shifts)
  - allows multiple people to interact with a mailbox

RecipeientTypeDetails: SharedMailbox
interactable through the EAC
- 3 levels of access
    Full Access
    Send As
    Send on Behalf

literally just better public folder

a distribution group just forwards something to all the members (sends them their own copy, rather than everyone gets the same one)

Exchange Compliance Management
- email is the most common way to communicate within a business
- sensitive data leaking - can have serious legal consequences - **data loss prevention, transport rules**
- some organizations have legal obligations to keep data for a certain amount of time - **retention policies, archiving**
- preserving email records for investigation/litigation - **eDiscovery, in-place hold (can also be used as snapshots)**

- **in-place eDiscovery** - search specific data in mailboxes across the exchange org > view, export, and store it
- **in-place hold** - freezes a mailbox indefinitely

- **data loss prevention** - allows for identifying and preventing critical information

- **transport rules** - server side rules that apply to incoming and outgoing emails > ex. every email that goes to a shared mailbox, send a copy to ____.
very strong, be careful, test before rolling them out
    conditions - when do we apply the rule
    actions - what happens when the rule is applied
    exceptions - DONT apply the rule when ...
- there are some pre-set rules :)

Deleting Mailboxes
- (ONLINE) if you remove a license, the user is disconnected and their mail is marked for deletion (default time is 30 days)
its common to convert to a shared mailbox so someone can review their stuff
- (ON PREM) delete = disconnect - SMTP address is deleted, but mailbox object still exists
disable - delete - mailbox is marked for deletion

SharePoint online

March 27, 2023 1:05 PM

Can run SharePoint
- on prem
- online (comes with the license)

Microsoft SharePoint - **content collaboration**
- one place where everyone can go to collaborate and access documents or files

SharePoint is web-based - it is a website
- you can make team sites
  -allows you to collaborate on teams (we have this in project)

- the other type of site is a communication site
  - this is for like blogs
  - just ready out of the box

- you can create a **Knowledge Base Wiki**
  - another SharePoint website that you can put guides, plans, instructional info, etc.

- SharePoint is integrated with all other M365 things

SharePoint **Workflows**
- automation for document handling, and other things

Fully web based, browser things :)
- it works on everything basically

the problem:
all your eggs are in one basket. what happens if someone gets in?

also controls one drive - hmmmmm

sharepoint site design - we are web designer :o
(only kind of :( )

Backups (enterprise edition)

April 3, 2023 12:05 PM

Why backup?
- Data integrity - corruption, deletion etc.
- Data archival - legal requirements
- Disaster recovery - in case things go south

How?
- windows backup feature
- virtual RAID on the server (not backups, just redundant)
- data backup when requested

Backup Types:
- Full backups - slow and take a lot of space, easier to recover
- Incremental - fast and not as much space, harder to recover

Media Types:
- tapes
- usb drives
- NAS - small, has its own IP, can directly connect
- SAN - block level storage, can't connect to it directly (would be the iSCSI target)
- cloud - free to put into cloud, costs to get it back (quicker = more expensive)

Enterprise Backups - Terminology
- on-site, local, on-prem
  > storage is physically in the same place/network as the items being backed up
  > you **own this hardware**

- off-site, remote, off-prem
  > storage is physically **separated** from items being backed up
  > **may** own the hardware (cloud you don't, but you could have a different site that has your "off-site" backups_

Considerations:
- price, reliability, speed to restore (pick 2)
- businesses will be using VMs - take a backup of the whole hypervisor or each individual VM?
- machine based or drive based is usually faster than file based.

Enterprise Backups
The 'default' nowadays is combining on-site and remote backups.
- on-site - running often, restore quickly, lower costs.
- remote - copies off-site in case of disaster, scale with long-term storage needs, synced from the on-site copies
  > on-site is more often than off-site.

Enterprise Media Types
- NAS is the most common
- Tape is rare, but can be used in medical for really long archiving
- USB can be used as a physical "link" for off-site backup (drive to the off-site with the drive)

Enterprise NAS or SAN
- Manageable over the network.
- variable storage (can be a little or a lot)
- RAID for redundancy (not backup)
- network connection allows versatile operations

How often do we need to run backups?
- it depends.
- money talks, they make the decisions.
- for mission critical things, more often (maybe hourly), for something less important maybe like every 6 hours.
- **Frequency depends on need.**
- possibly every 15 mins, possibly every day.
- this means we use incremental backups, not full (that is just super overkill).

Enterprise Backups - The Chain
- **Incremental Backups**
- looks at the previous backup file, then captures the **CHANGES**.
- it only looks back to the **BACKUP BEFORE**

- **Incremental Backups**
- recovery process considers the whole chain back to the first backup.
- allows for point-in-time recovery - meaning you can start at any part of the chain
- smaller individual files are easier to upload and to recover.

- **if one of the incremental backups gets broken, everything after is gone.**

- **The "chain" of backups requires management.**
- common option is "consolidation"
- whole chain can be compressed down to a single file. (hourly becomes daily, daily becomes weekly, etc.)

Consolidation:
- more files = more points of failure, this minimizes it.
- helps preserve space on storage destination
- increase speed of recovery - doesn't have to go through 30 daily files, could be just 4 weekly files.

What we have so far
- backing up each server individually
- multiple files per day per server
- storing data on local NAS
- data is a chain of files
- the whole chain is referenced as a single unit for recovery
- complexity increases exponentially as our environment grows
- we use software to handle it!

Enterprise Backup Solutions
- software helps with overhead:
  > timing for when backups run
  > location backups are saved
  > location backups are uploaded
  > consolidation
  > error checking

> recovery options

Software can be:
- Agent based, agentless, or both
- centrally controlled
- sold with an appliance, or use your own NAS
(nomenclature changes between vendors)

Generally,
- each server has their own backup settings, schedule, etc.
(this is called a **backup job**)
- the jobs create a chain of backup files
- each chain is then managed separately from each other
- each job can be set up independently as needed

We will use ShadowProtect SPX
3 main portions:
- the agent
- the controller
- image manager
- we are using a virtual NAS to store backups

Agent - endpoint
- installed to every server you want to back up
- controls processing jobs according to job settings,
- runs a handful of services

Console - centralized
- used to configure and check jobs
- set target disks backup destination, type and frequency
- check health of job
- see status of job
- only one of these needs to be installed

Image Manager
- service used to protect your chains
- **Required** for incremental backups
- one per environment
- automates verifying and consolidating your chains
- helps synchronize offsite backups
- recommend a dedicated VM to run this service.

a note on other tools:
- shadowprotect breaks out into 3 tools,
- other vendors could have it all in one, or less tools.

a note on performance
Network Traffic
- don't backup things all at the same time maybe (it could just murder your network every hour or whatever)

A note on automation
CHECK EVERYTHING MANUALLY

- regardless of software choice, most of the process is automated
- automation is not perfect
- backups could be failing and you wouldn't know.

ALWAYS CHECK BY HAND.

A note on security

- a copy of your entire environment is on your NAS. don't lose it.
- physical security is important.
- backups should be encrypted. (password protected)

a note on encryption

- **backups should be immutable**
  > cannot be changed after they are written
  > use separate credentials for everything
  > NAS should not be Domain Based, should be unique
  > if possible, separate VLAN

BACKUPS 2 (do this)

April 17, 2023 12:09 PM

Connor last test review

April 17, 2023 12:09 PM

different types of backups:
- incremental and full

full - a backup of the whole thing
incremental - the changes since the last backups

several incremental backups - this creates a chain,
if you lose a link in the chain, you lose the chan.
- the whole chain is considered a backup (?)

backup media
- tapes
- usb drives
- NAS
- SAN

NAS VS SAN
- SAN - set storage array network - usually larger, takes more space and has more storage (server rack) - direct storage, running VMs and stuff

- NAS - network attached storage - smaller, space and storage

SAN - block level storage - raw data (no file system) | centralized storage

NAS - file level storage - own operating system, has its own file system | navigate through \\NAS\Backup\blah (controlled entirely by what is on the NAS)

RAID is not a backup RAID is redundancy. It protects against drives failing NOT as a backup.

- on site backup - part of your local network
- off site backup - a remote location, physically separate (usually geographically diverse)

how often should you run backups? and why?

- 15 minutes - SQL server with a ton of data traffic

- every day -

security of backups: physical and virtual
- encrypt everything,
- backups should have its own account

3, 2, 1
3 copies of your backups
2 media types - nas, or just not online
1 offsite backup

the offsite chain is the same as the onsite chain - but they are physically independent

sharepoint
- owner, can change everything including permissions
- visitor - read only
- author - can create and modify

sharepoint and onedrive
- sharepoint is usually more permissive than onedrive
-

considerations for backups:
- network usage - stagger them and/or run them after hours

test info:

backup heavy
16 questions
multiple choice, true and false,