Overview of AD DS replication

Active Directory Domain Services (AD DS) replication is the process by which changes made to domain controllers (DCs) are synchronized across all DCs within a domain or forest. This ensures consistency and availability of directory information like user accounts, groups, computers, and security policies.

Key Concepts of AD DS Replication:

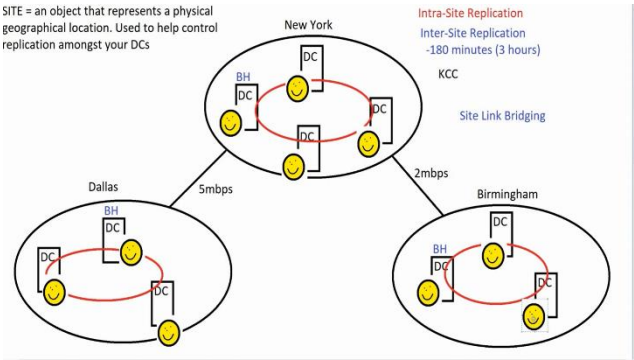
- **Multi-Master Replication** - All writable DCs can accept changes and replicate them to others (except RODCs).
- **Replication Topology** - Defines how domain controllers connect and replicate with each other.
- **Sites and Site Links** - Used to control replication over WAN/slow links by grouping DCs based on physical location.

Types of AD DS Replication:

- **Intra-site Replication** – Occurs between DCs in the same site. Fast and frequent. Uses RPC over IP.
- **Inter-site Replication** – Occurs between DCs in different sites.

Replication Process

- Change made on one DC (e.g., new user created).
- The change is assigned a unique USN (Update Sequence Number).
- Changes are replicated to other DCs.
- Receiving DC checks up-to-dateness vector to ensure no duplicate or outdated changes are applied.



KCC

- Knowledge Consistency Checker
- Responsible for checking and synchronizing between all the DCs within same site (approx. in 30seconds). This is called “intra-site replication”.
- This KCC syncs all the DCs in a single direction (least time).
- Every site has a Bridge Head (BH), that connects with another site for synchronization (called inter-site replication).
- Bridge Head (BH) syncs with every other site in every 180Minutes (3Hrs).
- Link that connects 2 sites is called “Link sites” (ex: 5mbps, 2mbps).

Pre-requisites

- At least two Domain Controllers (DCs) installed and configured.
- Both DCs should belong to the same forest.
- Proper DNS configuration and network connectivity between DCs.

Step 1: Open Active Directory Sites and Services

- On a DC, click Start → Administrative Tools → Active Directory Sites and Services
- Or run: dssite.msc

Step 2: Create New Sites

- In the left pane, right-click Sites → New Site
- Enter a name for the new site (e.g., Site-Branch01)
- Choose a site link object (e.g., DEFAULTIPSITELINK)
- Click OK → New site will appear under "Sites"

Step 3: Create Subnets and Associate with Sites

- Expand Subnets, right-click → New Subnet

- Enter subnet in CIDR format (e.g., 192.168.10.0/24)
- Choose the corresponding site you created (Site-Branch01)
- Click OK

Step 4: Move Domain Controller to the New Site

- Expand Sites → Default-First-Site-Name → Servers
- Right-click the server (DC) you want to move → Move
- Select the new site (Site-Branch01) → Click OK

Step 5: Configure Site Links (Optional/Advanced)

- Expand Inter-Site Transports → IP
- Right-click DEFAULTIPSITELINK → Properties
- Add/remove sites as needed
- Set:
    - Cost (lower = higher priority)
    - Replication Interval (in minutes)
    - Schedule for replication

Step 6: Force Replication (Optional)

- To immediately replicate changes between DCs:
- Open Command Prompt as Administrator
- Run: repadmin /syncall /AeD

Step 7: Verify Replication

- Use the following tools:
- Repadmin
    - repadmin /replsummary
    - repadmin /showrepl
- dcdiag
    - dcdiag /test:replications

Step 8: Monitor and Maintain

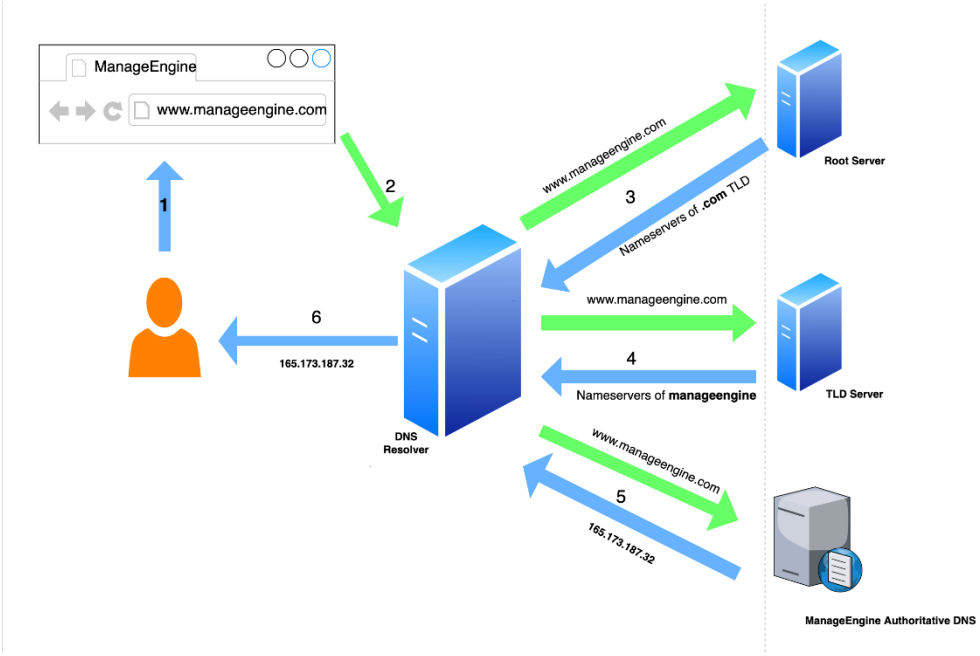
- Ensure that the site topology matches the network topology.
- Regularly check repadmin output.
- Adjust site link costs/schedules as needed for WAN optimization.

DNS

- DNS (Domain Name System) is a hierarchical and decentralized naming system for computers, services, or resources connected to the Internet or a private network.
- It translates human-readable domain names (like www.example.com) into IP addresses (like 93.184.216.34).
- It's often called the "phonebook of the Internet."

Hierarchy of DNS

- Root Domain (.): The top-level of the DNS hierarchy (invisible when browsing).
- TLD (Top-Level Domain): Last part of a domain name (e.g., .com, .org, .net, .in).
- Second-Level Domain: Directly before the TLD (e.g., google in google.com).
- Subdomain: A prefix to a domain (e.g., mail.google.com, where mail is a subdomain).
- Fully Qualified Domain Name (FQDN): A complete domain name ending with a dot (e.g., www.example.com.)



DNS Components

- DNS Resolver: A client-side service (usually your ISP or local device) that queries DNS servers.
- Recursive Resolver: Resolves the full DNS query by contacting various DNS servers.
- Root Name Server: Knows where the TLD name servers are.
- TLD Name Server: Knows where the authoritative name servers for specific domains are.
- Authoritative Name Server: Has the actual DNS records for a domain (final answer source).

Types of DNS Records

- *A Record* (Address Record): Maps a domain to an IPv4 address.
- *AAAA Record*: Maps a domain to an IPv6 address.
- *CNAME* (Canonical Name): An alias that maps one domain to another.
- *MX* (Mail Exchange): Directs emails to the appropriate mail servers.
- *NS* (Name Server): Specifies which servers are authoritative for a domain.
- *PTR* (Pointer Record): Maps an IP address to a domain name (used in reverse DNS).
- *SOA* (Start of Authority): Contains administrative information about the zone.
- *TXT* (Text Record): Stores arbitrary text, often used for SPF, DKIM, etc.
- *SRV* Record: Defines location of specific services (used in Microsoft AD, SIP, etc).

- Domain user can access redirected folder data from any machine within domain.
- Folder Redirection is a feature that allows administrators to redirect the path of user folders, like Documents, Desktop, and Downloads, to a network location instead of their default local storage.
- Folder Redirection allows you to redirect the path of a known user folder (such as Documents, Desktop, Pictures, etc.) from the local system to a network location (usually a file server).

Benefits

- Centralized storage of user data for backup and security
- Seamless access to files from any domain-joined computer
- Saves local disk space on client machines
- Works well with Roaming Profiles and Offline Files

Common Folders You Can Redirect

- Desktop
- Documents
- Pictures
- Downloads
- Start Menu
- Favorites
- Application Data

Link: https://newhelptech.wordpress.com/2017/07/06/step-by-step-configure-folder-redirection-in-window-server-2016/

Active Directory Certificate Service (ADCS)

- It's a role in window server that provides **Public Key Infrastructure (PKI)**.
- It is used to issue, manage, validate, and revoke digital certificates.
- It allows admins to manage and generate digital certificates.
- With certificate we can:
    - Authenticate users
    - Authenticate devices
    - Encrypt communication
    - Validate signature
- ADCS can be configured in 2 ways:
    1. Enterprise Certificate Authority (CA) – within domain
    2. Stand-Alone Certificate Authority – within workgroup

Core Features of AD CS

- Enables Certificate Authorities (CAs) to issue and manage digital certificates.
- Supports automated certificate enrollment and renewal (via Group Policy).
- Integrates tightly with Active Directory Domain Services (AD DS).
- Enables certificate-based authentication (smart cards, 802.1X, etc.).
- Supports certificate templates for standardizing issuance.
- Allows revocation management via Certificate Revocation Lists (CRLs) and Online Responders.

AD CS Role Services (Components)

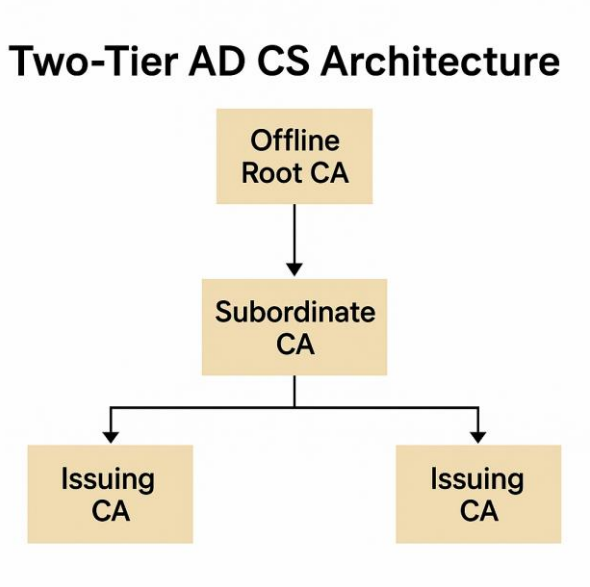
- *Certification Authority (CA)*
    - The server role that actually issues and revokes certificates.
    - Types:
        - Enterprise CA (AD-integrated) and
        - Standalone CA (not AD-integrated).
- *CA Web Enrollment*
    - Provides a web interface for users to request certificates and retrieve CRLs.
- *Online Responder*
    - Implements Online Certificate Status Protocol (OCSP) for real-time certificate status checking.
- *Certificate Enrollment Web Services*
    - Allows certificate enrollment across firewalls and to non-domain joined machines via HTTPS.
- *Network Device Enrollment Service* (NDES)
    - Supports Simple Certificate Enrollment Protocol (SCEP) for routers, switches, and mobile devices.
- *Certificate Templates*
    - Define the format, purpose, and issuance policies for certificates.

Common Deployment Models

- *Single-Tier PKI*
    - One CA (Root CA)
    - Easy to deploy, not recommended for production due to security risks
- *Two-Tier PKI* (Recommended)
    - Offline Root CA (high security, rarely used)
    - Online Subordinate CA(s) (issue and manage certs)
- *Three-Tier PKI*
    - Offline Root CA → Policy CAs → Issuing CAs
    - Used in very large or highly regulated environments

Typical Use Cases of AD CS

- Issuing SSL/TLS certificates for websites
- Smart card logon and multi-factor authentication
- Wi-Fi and VPN authentication (e.g., 802.1X)
- Email encryption and signing (S/MIME)
- Code signing for developers
- Encrypting File System (EFS) support
- IPsec authentication



Advantages of AD CS

- Enables automated certificate lifecycle management
- Ensures secure communications in enterprise environments
- Integrated with AD for scalability and ease of use
- Provides strong identity assurance
- Supports customizable certificate policies and templates

Disadvantages / Challenges

- Complex to deploy and maintain properly in large environments
- Mismanagement can lead to trust issues across the network
- Requires regular maintenance (CRL publication, backup, key renewal)
- High-value target – needs strong security hardening
- Backups of CA database and private keys are critical
- Offline Root CA must be carefully managed

Lifecycle Management

- Certificates have expiration dates – plan renewal ahead of time
- Revoked certificates are published in CRLs
- Use OCSP for faster and real-time certificate status checking

Tools and Utilities

- certsrv.msc – Certificate Authority console
- certtmpl.msc – Certificate Templates console
- certreq / certutil – Command-line tools for certificate management
- MMC Snap-ins – For managing certificates for users/computers
- Group Policy – For auto-enrollment and deployment

Step-by-step guide to creating an Enterprise Certification Authority (CA):

Pre-requisites

- A Windows Server machine (domain-joined).
- You must be logged in with a domain administrator account.
- Ensure the Active Directory Domain Services (AD DS) role is already installed.

Link: https://www.firewall.cx/operating-systems/microsoft/windows-servers/windows-server-2016-certification-authority-installation-configuration.html