**20️⃣ Security Hardening Best Practices**

**🔐 Domain Controller Security**

* Ensure DCs are physically and logically secure.
* Disable unnecessary services on DCs.
* Apply least privilege model to admins.
* Enforce secure channel traffic (LDAP signing, SMB signing).

**📜 Group Policies**

* Enforce strong password and lockout policies.
* Configure audit policies to log key activities.
* Disable Guest account and remove unused default accounts.

**🚫 Block Lateral Movement**

* Deploy tiered administration (Tier 0/1/2 model).
* Use separate privileged accounts.
* Limit interactive logon rights on DCs.

**🔒 Hardening LDAP and RDP**

* Require LDAPS or secure RDP (via certificate).
* Block untrusted networks from accessing DCs directly.

**🌍 21️⃣ Multi-Site AD Deployment**

**🗺️ Design Overview**

* Site A (Primary): 172.16.1.0/24
* Site B (DR): 172.16.2.0/24
* Each site has at least 1 DC.
* Sites are linked with AD Site Links (default cost 100).

**🔧 Configure AD Sites and Services**

1. Open **Active Directory Sites and Services**.
2. Create two new Sites: HQ-Site, DR-Site.
3. Associate each subnet to the correct site:
   * 172.16.1.0/24 → HQ-Site
   * 172.16.2.0/24 → DR-Site
4. Move Domain Controllers to the appropriate site.
5. Configure replication schedule and Site Link Bridge if needed.

🧠 Tip: Keep FSMO roles centralized unless intentional redundancy is needed.

**💥 22️⃣ Disaster Recovery Planning**

**🧰 Backup Essentials**

* Use **Windows Server Backup**, **Veeam**, or similar to back up:
  + System State
  + Active Directory (NTDS.DIT, SYSVOL)
  + DNS Zones (if integrated)

**🔁 Recovery Process**

1. Restore **System State** from backup.
2. Perform **Authoritative Restore** if needed:

ntdsutil

activate instance ntds

authoritative restore

1. Restore DNS or other dependencies as needed.

**📑 DR Runbook Suggestions**

* Regular backup validation/testing.
* Isolate DR replication traffic.
* Document failover plan:
  + Promote DR DC
  + Seize FSMO if needed
  + Adjust DNS priorities (SRV records, client configs)

**⛑️ Tools**

* wbadmin for backup/restore
* ntdsutil for authoritative restore
* repadmin & dcdiag for post-recovery verification