**12️⃣ Certificate Authority Setup**

**📥 Install AD CS**

1. Open **Server Manager > Add Roles and Features**.
2. Select **Active Directory Certificate Services** → Add Features.
3. Proceed with default settings until **Role Services**, then select:
   * **Certification Authority**
   * (Optional: CA Web Enrollment, Online Responder)
4. Complete installation and click **Configure Active Directory Certificate Services**.

**⚙️ Configure CA**

1. Choose **Enterprise CA**.
2. Select **Root CA** or **Subordinate CA** (choose Root for lab).
3. Create a **new private key**.
4. Keep default cryptographic options or customize.
5. Name the CA (e.g., vlab-RootCA).
6. Define the validity period (default: 5 years).
7. Complete configuration.

**🧾 13️⃣ Certificate Template Publishing**

**📤 Publish a Template**

1. Open **Certification Authority > Certificate Templates**.
2. Right-click **Certificate Templates > Manage**.
3. Duplicate an existing template (e.g., **User**).
4. Under **General**, rename it (e.g., SmartCard-User).
5. Under **Security**, give **Enroll**/Autoenroll rights to specific groups.
6. Close the template editor.
7. Back in CA console, right-click **Certificate Templates > New > Certificate Template to Issue** → choose your template.

**♻️ 14️⃣ Backup & Recovery**

**🔒 Backup AD & CA**

# System State Backup (includes AD, CA, DNS, etc.)

wbadmin start systemstatebackup -backupTarget:D:

# Export CA Cert & Private Key

certutil -backup D:\CA-Backup

**🔄 Recovery**

* Use **wbadmin** to recover full system state.
* To restore CA:
  + Reinstall AD CS.
  + Run: certutil -restore D:\CA-Backup

**🔍 15️⃣ Auditing & Logging**

**🧾 Enable Auditing Policies**

Audit Directory Service Access

Audit Logon Events

Audit Object Access

Configure via: Group Policy > Security Settings > Advanced Audit Policy Configuration

**📁 Enable Audit on Objects**

1. Open **AD Users and Computers**.
2. Enable **Advanced Features**.
3. Right-click object (e.g., OU) → **Properties > Security > Advanced > Auditing**.
4. Add principal (e.g., Domain Admins) and define auditing rules.