**Phase 1: Vorbereitung – Eine Abhängigkeit schaffen**

**Ziel:** Server02 so konfigurieren, dass er für bestimmte Anmeldeinformationen auf den GC von Server01 angewiesen ist.

**Aufgabe 1: Server02 die GC-Rolle entziehen**

1. Öffnen Sie auf einem der Server das Verwaltungstool **"Active Directory-Standorte und -Dienste"**.
2. Navigieren Sie im linken Baum zu: Sites -> Default-First-Site-Name (oder Ihr Standortname) -> Servers -> **Server02**.
3. Klicken Sie mit der rechten Maustaste auf das Objekt **NTDS Settings** unter Server02 und wählen Sie Eigenschaften.
4. Entfernen Sie den Haken bei **Globaler Katalog (GC)**.
5. Klicken Sie auf OK. Es erscheint eine Meldung, dass die Änderung Zeit benötigt. Das ist normal.

**Aufgabe 2: Den "Beweis" erbringen – Eine universelle Gruppe verwenden**
Der GC ist der einzige, der die Mitgliedschaft in "Universellen Gruppen" auflösen kann. Das nutzen wir für unseren Test.

1. Öffnen Sie **"Active Directory-Benutzer und -Computer"**.
2. Erstellen Sie einen neuen Benutzer, falls Sie keinen Testbenutzer haben (z.B. Name: Test Anmeldung, Benutzername: testanmeldung).
3. Erstellen Sie eine neue Gruppe mit folgenden Eigenschaften:
    - Gruppenname: U_Test_Gruppe_GC
    - Gruppenbereich: **Universal** (Dies ist der entscheidende Punkt!)
    - Gruppentyp: Sicherheit
4. Fügen Sie Ihren Benutzer testanmeldung als Mitglied zu dieser neuen universellen Gruppe hinzu.

**Überprüfung:** Die Ausgangslage ist nun:

- Server01 ist ein DC und ein GC.
- Server02 ist ein DC, aber **kein** GC mehr.
- Der Benutzer testanmeldung ist Mitglied einer universellen Gruppe.

**Phase 2: Die Störung simulieren – Der GC-Ausfall**

**Ziel:** Server01 für Server02 unerreichbar machen und die katastrophalen Folgen für die Anmeldung testen.

**Aufgabe 3: Den primären GC (Server01) blockieren**
Wir simulieren einen Netzwerkausfall mit einer Firewall-Regel.

1. Gehen Sie zu **Server01**.
2. Öffnen Sie die "Windows Defender Firewall mit erweiterter Sicherheit".

3. Erstellen Sie eine neue **Ausgehende Regel**:
    - Regeltyp: Benutzerdefiniert
    - Protokolltyp: Jedes
    - Bereich: Unter "Remote-IP-Adressen" fügen Sie die **IP-Adresse von Server02** hinzu.
    - Aktion: **Verbindung blockieren**
    - Profil: Alle drei (Domäne, Privat, Öffentlich) anhaken.
    - Name: TEST - GC Ausfall simulieren
4. **Aktivieren Sie die Regel.** Server01 kann nun keine Anfragen mehr von Server02 beantworten.

**Aufgabe 4: Der Moment der Wahrheit – Der Anmeldeversuch**

1. Sie benötigen einen Client-PC, der Mitglied der Domäne ist.
2. **WICHTIGER SCHRITT:** Konfigurieren Sie die Netzwerkeinstellungen dieses Clients so, dass er **ausschließlich die IP-Adresse von Server02 als DNS-Server** verwendet. Damit zwingen wir den Client, sich bei Server02 zu authentifizieren.
3. Versuchen Sie nun, sich am Client mit dem Benutzer testanmeldung anzumelden.

**Beobachten Sie das Ergebnis:**

- Die Anmeldung wird **extrem lange dauern oder mit einer Fehlermeldung fehlschlagen**, z.B. "Es sind keine Anmeldeserver verfügbar...".
- **Warum?** Der Client kontaktiert Server02. Server02 muss für die Anmeldung die Mitgliedschaft in der universellen Gruppe U_Test_Gruppe_GC prüfen. Da Server02 selbst kein GC ist, versucht er, den GC (Server01) zu fragen. Aufgrund der Firewall-Regel erreicht er ihn nicht. Nach einem langen Timeout bricht die Anmeldung ab.
- **Hinweis:** Falls die Anmeldung doch klappt (sehr langsam), kann es am "Credential Caching" liegen. Der beste Effekt erzielt sich mit einem Benutzer, der sich noch nie an diesem PC angemeldet hat.

**Phase 3: Das Problem lösen – Redundanz herstellen**

**Ziel:** Das Problem beheben, indem wir Server02 wieder zu einem GC machen und damit den Standort autonom machen.

**Aufgabe 5: Server02 wieder zum Globalen Katalog machen**

1. Gehen Sie zurück zu **Server01** und **deaktivieren Sie die Firewall-Regel** "TEST - GC Ausfall simulieren". Die Replikation muss wieder funktionieren.
2. Gehen Sie zu Server02 (oder bleiben Sie auf Server01).
3. Öffnen Sie wieder "Active Directory-Standorte und -Dienste".
4. Gehen Sie zu den NTDS Settings von Server02.
5. Setzen Sie den Haken bei **Globaler Katalog (GC)** wieder.

6. **Warten Sie ca. 5-10 Minuten.** Der Server muss nun den gesamten Katalog-Index von Server01 replizieren. In der Ereignisanzeige von Server02 unter "Verzeichnisdienst" erscheint das Ereignis mit der **ID 1119**, sobald der Server bereit ist.

**Aufgabe 6: Der finale Test**

1. Die Firewall-Regel auf Server01 kann für diesen Test ruhig wieder **aktiviert** werden, um zu beweisen, dass Server02 jetzt autonom ist!
2. Gehen Sie zurück zum Client-PC (der immer noch nur Server02 als DNS nutzt).
3. Versuchen Sie erneut, sich mit testanmeldung anzumelden.