מעבדה 05 — תיעוד התאוששות מאסון

BIA · RPO/RTO · Runbook · Tabletop Exercise — חצי כתיבה, חצי תרגול

מודול 5 — ניהול מערכות ושירותים | זמן משוער: 60-75 דקות | רמת קושי: ⭐⭐ בינוני (כתיבה)

→ הקודם: Linux Backup

הבא ← מעבדה 06: gMSA

מטרות הלמידה

- להבין את ההבדל בין Backup ל-Disaster Recovery (לא אותו דבר!)
- לבצע Business Impact Analysis (BIA) פשוט עבור 5 שירותים
- לחשב RPO ו-RTO לכל שירות
- לכתוב Runbook מפורט עבור תרחיש "DC נפל"
- לבצע Tabletop Exercise — סימולציה של אסון, מעבר על ה-Runbook
- לתעד פערים ב-Runbook אחרי הסימולציה

למה המעבדה הזו חשובה

Backup הוא **פעולה**. DR הוא **תכנית**. ההבדל קריטי:

- **Backup** = יש לי עותק של הנתונים. נקודה.
- **DR** = יש לי תהליך מלא של איך לחזור לעבוד אחרי אסון — מי עושה מה, באיזה סדר, כמה זמן זה לוקח, מה הפריוריטיות, מה אם המנהל לא זמין.

ארגונים שיש להם Backup אבל אין DR — נכשלים בשעת אסון. כי "יש גיבוי" זה רק 10% מהסיפור. ה-90% האחרים = תהליך, אנשים, החלטות.

במעבדה הזו תכתבו DR plan פשוט אבל אמיתי, ותתרגלו לפי ה-Runbook. בסוף תראו אילו צעדים פספסתם ותתקנו את התיעוד.

דרישות מקדימות

- ✓ מעבדה 00 — הקמת AD הושלמה
- ✓ מעבדה 03 — Backup הושלמה (יש גיבויים בפועל)
- עורך טקסט/מסמכים — Word, Notepad++, או VS Code
- קחו snapshot עכשיו: `Pre-Lab-05` — נשבור דברים בכוונה!

> ⚠️ **שימו לב:** המעבדה הזו **תהרוס** את ה-DC ב-Tabletop Exercise. snapshot עכשיו או צרות בהמשך.

חלק א' — Business Impact Analysis (15 דקות)

BIA = "כמה כואב אם השירות הזה נופל?". זה הצעד הראשון בכל DR plan. בלי BIA לא יודעים מה לתקן קודם.

1 שלב 1 — צרו קובץ BIA

פתחו Notepad או Word. שמרו בשם `BIA-CyberLab-2026.md`. הקלידו את הטמפלייט הבא:

```doc
# Business Impact Analysis – CyberLab Inc.
# Date: 2026-04-29
# Author: [שמך]

| Service | Description | Criticality | Max Downtime | Data Loss Tolera
|---------|-------------|-------------|--------------|----------------
| AD DS   | Domain Auth | CRITICAL    | 1 hour       | 15 min
| File Server | Business files | HIGH    | 4 hours      | 1 hour
```

```
| Email    | Communication | HIGH      | 2 hours      | 30 min
| Print Server | Printing | LOW       | 24 hours     | N/A
| Internal Wiki | Documentation | MEDIUM | 8 hours    | 4 hours
```

✅ **תוצאה צפויה:** 5 שירותים. כל אחד עם רמת קריטיות + max downtime + data loss + dependencies.

🤔 **עצרו וחשבו:** מה זה Criticality? ההשפעה על העסק אם השירות לא זמין:
CRITICAL — העסק לא יכול לעבוד בלעדיו (AD = הכל מחובר).
HIGH — חלק גדול מהעובדים נעצרים.
MEDIUM — הפרעה אבל יש workaround.
LOW — לא נעים אבל לא קריטי.

2

שלב 2 — חשבו עלות per hour

הוסיפו עמודה: **Cost per Hour Down**. להעריך פחות חשוב מלהבין את הסדר.

דוגמאות:

```doc
| Service     | Cost per Hour Down |
|-------------|--------------------|
| AD DS       | 50,000 NIS         |  (כל העובדים נעצרים)
| File Server | 30,000 NIS         |  (חלקית — חלקם עובדים מקומית)
| Email       | 20,000 NIS         |
| Print       | 500 NIS            |
| Wiki        | 2,000 NIS          |
```

🤔 **עצרו וחשבו:** מהיכן המספרים? בארגון אמיתי: # עובדים מושפעים × שכר ממוצע לשעה. במעבדה — הערכה. החשוב: הסדר היחסי.

חלק ב׳ — RPO + RTO (10 דקות)

שני המספרים החשובים בכל תכנית DR.

```
רגע האסון
      │
──────┼──────────────────────────────────► זמן
      │
      │
◄─────┤  RPO (Recovery Point Objective)
      │  כמה זמן של נתונים אני יכול לאבד
      │  = הזמן מאז הגיבוי האחרון
      │
      ├──►  RTO (Recovery Time Objective)
      │       כמה זמן עד שהשירות חוזר לפעולה
```

1 שלב 3 — קבעו RPO ו-RTO לכל שירות

הוסיפו לטבלת ה-BIA:

```
| Service     | RPO       | RTO       | Required Backup Frequency |
|-------------|-----------|-----------|---------------------------|
| AD DS       | 15 min    | 1 hour    | Every 15 min (incremental)|
| File Server | 1 hour    | 4 hours   | Hourly                    |
| Email       | 30 min    | 2 hours   | Every 30 min              |
| Print       | N/A       | 24 hours  | Daily (config only)       |
| Wiki        | 4 hours   | 8 hours   | Every 4 hours             |
```

DOC

🤔 **עצרו וחשבו:** RPO מכתיב את *תדירות הגיבוי*. RTO מכתיב את *סוג הגיבוי* + *תשתית שחזור*. 15 RPO דקות מצריך VSS תכוף או database log shipping. RTO של שעה מצריך מערכת standby מוכנה (לא רק tape archive).

2 שלב 4 — השוו RPO/RTO למה שיש בפועל

כעת השוו לגיבויים האמיתיים שעשיתם במעבדה 03:

```doc
| Service     | Required RPO | Actual RPO (today)      | Gap?     |
|-------------|--------------|-------------------------|----------|
| AD DS       | 15 min       | 12 hours (manual backup)| ✗ HUGE   |
| File Server | 1 hour       | 12 hours                | ✗ Yes    |
```

⚠️ **שימו לב:** בארגון אמיתי הטבלה הזו = מה שמציגים ל-CIO. כל "Gap" = השקעה שצריכה להיעשות.

חלק ג׳ — כתיבת Runbook עבור "DC Down" (15 דקות)

Runbook = רשימת הצעדים שאדם רגיל יכול לעקוב אחריהם בלי להבין הכל. דוקומנט של חירום — לא של למידה.

1 **שלב 5 — צרו קובץ Runbook**

שמרו בשם `Runbook-DC-Down.md` . השתמשו בטמפלייט הבא:

```doc
# RUNBOOK — Domain Controller Down

## Trigger
שגיאות login של משתמשים, gpresult נכשל, dcdiag מחזיר שגיאות.

## Severity: CRITICAL
RTO: 1 hour | RPO: 15 minutes

## On-Call
- Primary: [שם מנהל IT] — 050-1234567
- Backup: [שם מנהל IT 2] — 050-7654321

## Phase 1 — Diagnose (5 min)
1. Login to backup admin VM (`cyberlab-admin01`)
```

```
2. Run: `Test-NetConnection cyberlab-dc01 -Port 389`
   - If success → DC reachable, AD service issue
   - If fail → DC offline (network/host issue)
3. Run: `Get-Service ADWS,KDC,Netlogon,DNS -ComputerName cyberlab-dc01`
   - Note which services are NOT running

## Phase 2 — Triage (10 min)
**Decision tree:**
- Services running but slow? → Resource issue (RAM/CPU). Reboot DC. Skip
- Services not running, host responsive? → Try `Restart-Service ADWS -C
- Host not responsive? → Continue to Phase 3 (full restore).

## Phase 3 — Restore from Backup (30-45 min)
1. Open VirtualBox Manager
2. Select `cyberlab-dc01` → right-click → Snapshots
3. Restore latest known-good snapshot (`DC-Promoted-Clean` or `Post-Lab
4. Power on
5. Wait 3-5 min for AD services to start
6. Login as `CYBERLAB\Administrator`
7. Run validation:
   ```
   Get-ADDomain
   dcdiag /q
   Get-Service ADWS,KDC,Netlogon
   ```

## Phase 4 — Verify Service (5 min)
1. From cyberlab-ws01: `gpupdate /force`
2. Test domain login: logout → login as `CYBERLAB\student01`
3. Verify file access: `\\cyberlab-dc01\sysvol`
4. Notify users service restored

## Phase 5 — Post-Mortem (within 48h)
- Root cause analysis
- Update Runbook if gaps found
- Schedule infrastructure improvements

## Rollback Plan
If snapshot restore fails:
1. Boot DC from Windows Server ISO
```

```
2. Choose Repair → System Image Recovery
3. Point to backup target E:\WindowsImageBackup
4. Follow wizard

## Success Criteria
- All 5 services in BIA accessible
- Users can login
- File shares mount
- No errors in `dcdiag /q`
```

✅ **תוצאה צפויה:** קובץ Runbook מוכן. זה לא רק תיעוד — זה הוראות חירום.

2 **שלב 6 — בקרה: האם זה דמוי-טיפש?**

קראו את ה-Runbook בעיני מישהו שלא מכיר את הסביבה. שאלו את עצמכם:

- האם כל פקודה עם הפרמטרים בדיוק?
- האם יש דרך לדעת מתי להתקדם לשלב הבא? (success criteria)
- אם הצעד נכשל — מה עושים? (decision branches)
- האם נסמכתי על ידע סמוי שלא תועד?

💡 **טיפ:** הכלל: אם מישהו ב-3:00 בלילה יכול לעקוב אחרי ה-Runbook ולגרום לשירות לחזור — זה Runbook טוב. אם הוא צריך להתקשר אליך — לא טוב.

חלק ד' — Tabletop Exercise (15 דקות)

הזמן לבדוק את ה-Runbook. נחקה אסון אמיתי.

1 **שלב 7 — "תקלה": כבו את ה-DC בכוח**

cyberlab-dc01 → VirtualBox Manager → סגירת חלון → **Power off** (כן, הפעם בכוונה — מדמים crash).

✅ **תוצאה צפויה:** DC נכבה. ה-VM אפור.

2 **שלב 8 — בדקו אצל הקליינט**

עברו ל-cyberlab-ws01. תנעלו (Lock) את המסך → נסו להיכנס שוב כ-`CYBERLAB\student01`.

✅ **תוצאה צפויה:** הכניסה נכשלת או מציגה אזהרה. השירות באמת ירד.

3 **שלב 9 — עקבו אחר ה-Runbook**

פתחו את ה-Runbook שכתבתם. עקבו אחריו צעד אחר צעד. **אל תסטו ממנו** — גם אם אתם יודעים פתרון מהיר יותר. המטרה: לבדוק שהמסמך עובד.
זמנו את עצמכם. רשמו זמן בכל שלב.

⚠️ **שימו לב:** אם נתקעתם ב-Runbook — סמנו את הצעד שבו נתקעתם. **אל תתקנו עכשיו!** — נדע שיש שם פער.

4 **שלב 10 — שחזרו**

VirtualBox → Snapshots → restore `Pre-Lab-05` → Start.
חכו 2-3 דקות. בדקו ב-WS שהדומיין עובד שוב.

✅ **תוצאה צפויה:** DC חזר. הקליינט יכול להיכנס. סיימתם את ה-recovery.

חלק ה' — Post-Mortem ועדכון Runbook (10 דקות)

1 שלב 11 — תעדו את הפערים

צרו קובץ `PostMortem-2026-04-29.md`:

```doc
# Post-Mortem — DC Down Drill — 2026-04-29

## Total Downtime: __ minutes
## RTO Target: 60 min | Achieved: __ min — pass/fail?

## Timeline
- T+0:    DC powered off (simulated crash)
- T+__:   Detected by client login failure
- T+__:   Started Runbook Phase 1
- T+__:   Restored from snapshot
- T+__:   Service validated working

## Gaps Found
1. [צעד שלא היה ברור]
2. [פקודה שחסרה]
3. [קישור שלא היה]

## Action Items
- [ ] עדכן Runbook עם...
- [ ] הוסף ניטור על שירות X
- [ ] תרגול נוסף בעוד 30 יום
```

✅ **תוצאה צפויה:** post-mortem כתוב. זה הסוף הנכון של DR drill.

2 שלב 12 — עדכנו את ה-Runbook

חזרו לקובץ `Runbook-DC-Down.md`. תקנו את הפערים שמצאתם. שמרו עם תאריך עדכון בראש הקובץ.

🤔 **עצרו וחשבו:** זה ה-secret sauce של DR טוב — לא מסמך שכותבים פעם ואז שוכחים, אלא מסמך חי שמתעדכן אחרי כל drill ואחרי כל אירוע אמיתי.

אתגרי בונוס

🏆 **אתגר בונוס: בונוס 1 — Runbook נוסף.** כתבו Runbook לתרחיש "Ransomware על file server". מה שונה? (תשובה: Restore לא יספיק — צריך גם לחקור איך נכנס, לבודד את המכונות הפגועות, לוודא שה-backup לא מוצפן.)

🏆 **אתגר בונוס: בונוס 2 — DR Site שלם.** עצבו (לא תקימו) DR site מלא. איזו תשתית: cold/warm/hot? עלות יחסית? RTO? מה השיקולים?

🏆 **אתגר בונוס: בונוס 3 — Communication Plan.** בעת אסון — מי מודיע למי? באיזה סדר? באיזה ערוץ? כתבו plan: Internal staff, External customers, Executive team, Press.

🏆 **אתגר בונוס: בונוס 4 — תרגול עיוור.** תנו את ה-Runbook לחבר/תלמיד אחר. בקשו ממנו לבצע. אם הוא מצליח בלי לשאול שאלות — Runbook מצוין. אם הוא נתקע — תיעוד צריך עבודה.

צ׳ק-ליסט אימות

- ☐ קובץ BIA.md עם 5 שירותים
- ☐ עמודות RPO + RTO + Required Backup Frequency
- ☐ Cost per Hour Down (מוערך)
- ☐ קובץ Runbook-DC-Down.md מלא
- ☐ Tabletop Exercise בוצע (DC כבוי + שחזור)

- ☐ Post-Mortem עם timeline + gaps + action items
- ☐ Runbook עודכן אחרי הניסוי

עיקרי הדברים

- Backup ≠ DR. Backup הוא נתונים. DR הוא תהליך + אנשים + תקשורת + מועדים.
- BIA = מה כואב אם נופל. בלי BIA לא יודעים על מה לשים מאמצים.
- RPO = כמה אני יכול לאבד. RTO = כמה זמן יקח להחזיר. שניהם חייבים לכל שירות.
- Runbook = הוראות חירום שאדם רגיל יכול לעקוב אחריהן. דמוי-טיפש בכוונה.
- Tabletop Exercise = drill פיזי. בלי זה לא יודעים אם ה-Runbook עובד.
- Post-Mortem אחרי כל אירוע — חזרה תמיד מסתיימת בעדכון התיעוד.
- תוכנית שלא נבדקה = לא תוכנית. נבדקה = רלוונטית רק אם נבדקה ***שוב לאחרונה***. תרגלו DR פעם בחצי שנה לפחות.

בסוף המעבדה

1. שמרו את כל המסמכים בתיקייה `~/dr-docs/` (או דומה)
2. קחו snapshot: `Post-Lab-05-DR`
3. כיבוי תקין של ה-VMs

→ הקודם: Linux Backup

הבא ← מעבדה 06: gMSA