

מסמך בדיקות

הגנת סייבר

**מגיש: עומר כפיר (330869017) תיכון הרצוג יב'3**

**שם מנחה: אופיר שביט**

**נושא הפרויקט: פלטפורמת תצפית שקטה על פעילות עובדים בחברה**

**תיאור קונפיגורציית הפרויקט**

הגדרת שרת מדומה  
אגדיר שרת מדומה שישמש כשרת מרכזי לקבלת הנתונים. השרת יופעל במחשב אחר מהרשת המקומית, עם חיבור יציב ומאובטח.

סביבת מחשבים מגוונת  
אבצע בדיקות על מספר מחשבים שונים עם מפרטים ומערכות הפעלה מגוונות (Windows 10 ו-Windows 11), כדי לוודא תאימות.

כלי ניטור ובדיקת ביצועים  
אשתמש בכלים לניטור רשת, כמו Wireshark, וכלים למדידת ביצועים כמו Task Manager .

שמירת נתונים והצגת  
אבצע בדיקות של רמת התאימות בין הנתונים שנשלחו לבין הנתונים שהתקבלו בשרת.

**תיאור הבדיקות (קלט, פלט, מטרה ואופן ביצוע הבדיקה)**

1. בדיקת התקנה והפעלה ראשונית  
   מטרה: לוודא שהמערכת מותקנת ופועלת ללא שגיאות על מחשבים חדשים.  
   קלט: התקנת המערכת על מחשב חדש.  
   פלט: המערכת מותקנת ופועלת כמצופה, כולל הצגת מסך התחלתי תקין.  
   איך תתבצע הבדיקה: אנסה להתקין את המערכת על מספר מחשבים עם מפרטים שונים, אתחיל את התוכנה ואוודא שהיא עולה ללא שגיאות.
2. בדיקת העברת נתונים לשרת  
   מטרה: לוודא שהמערכת שולחת נתונים מהמחשב לשרת באופן תקין.  
   קלט: פתיחת קבצים במחשב המשתמש ושליחת נתונים לשרת.  
   פלט: הנתונים מתקבלים בשרת המרכזי במלואם ובזמן אמת.  
   איך תתבצע הבדיקה: אגדיר שרת מדומה, אבצע פעולות מוגדרות מראש במחשב המשתמש, ואעקוב אחרי הנתונים המתקבלים בשרת באמצעות כלי ניטור רשת כמו Wireshark.
3. בדיקת תאימות על מחשבים שונים  
   מטרה: לוודא שהמערכת פועלת תקין על סוגי מחשבים שונים.  
   קלט: התקנת המערכת ובדיקתה על מחשבים עם מפרטים ומערכות הפעלה מגוונים.  
   פלט: המערכת פועלת בצורה תקינה ללא שגיאות או תקלות.  
   איך תתבצע הבדיקה: אבצע את הבדיקה על לפחות 3 מחשבים שונים, עם מפרטים ומערכות הפעלה שונות (לדוגמה, Windows 10 ו-Windows 11).
4. בדיקת עומס נתונים  
   מטרה: לבדוק כיצד המערכת מתפקדת בעת שליחת כמות נתונים גדולה.  
   קלט: שליחת כמות גדולה של נתונים בו-זמנית.  
   פלט: המערכת מעבדת את כל הנתונים ללא קריסה או אובדן מידע.  
   איך תתבצע הבדיקה: אכתוב סקריפט שמדמה שליחת נתונים רציפה ומוגברת לשרת, ואעקוב אחרי השפעת העומס על השרת והמערכת.
5. בדיקת שמירת נתונים מקומית במקרה של ניתוק רשת  
   מטרה: לוודא שהנתונים נשמרים מקומית בעת ניתוק רשת.  
   קלט: ניתוק רשת בזמן שליחת נתונים.  
   פלט: הנתונים נשמרים במערכת המקומית ונשלחים לשרת לאחר שחוזרת הרשת.  
   איך תתבצע הבדיקה: אגדיר מחשב לקוח, אבצע שליחת נתונים, ולאחר מכן אנתק את חיבור הרשת ואעקוב אחרי שמירת הנתונים המקומית.
6. בדיקת ביצועי המערכת  
   מטרה: לבדוק שהמערכת אינה משפיעה בצורה משמעותית על ביצועי המחשב.  
   קלט: מדידת שימוש במשאבים (CPU, זיכרון) לפני ואחרי התקנת המערכת.  
   פלט: הבדלים מינימליים בצריכת המשאבים של המחשב.  
   איך תתבצע הבדיקה: אשתמש בכלים כמו Task Manager לפני התקנה ואחריה, ואשווה את הנתונים.
7. בדיקת עקביות נתונים  
   מטרה: לוודא שהנתונים שנשלחים לשרת תואמים לפעולות שבוצעו בפועל.  
   קלט: ביצוע פעולות מוגדרות מראש והשוואת הנתונים בשרת.  
   פלט: הנתונים בשרת משקפים בדיוק את הפעולות שנעשו.  
   איך תתבצע הבדיקה: אפתח תוכנות, אערוך מסמכים ואשווה בין התוצאות שהתקבלו בשרת לפעולות שבוצעו בפועל.
8. בדיקת מהירות תגובה  
   מטרה: לבדוק שהמערכת מגיבה במהירות לפעולות המשתמש.  
   קלט: עריכת קובץ ושמירתו.  
   פלט: הנתונים נשלחים לשרת באופן מיידי ללא עיכובים.  
   איך תתבצע הבדיקה: אשתמש בכלי מדידה לבדיקת זמני שליחה ואוודא שהתגובה מהירה.
9. בדיקת ריבוי משתמשים  
   מטרה: לבדוק שהמערכת יכולה לתפקד עם מספר משתמשים בו-זמנית.  
   קלט: שליחת נתונים ממספר מחשבים במקביל.  
   פלט: המערכת פועלת יציב וכל הנתונים מתקבלים בשרת.  
   איך תתבצע הבדיקה: אצור סביבה עם מספר מחשבים המדמים משתמשים שונים ואוודא שכל הנתונים מגיעים לשרת בצורה תקינה.
10. בדיקת ניהול תקלות בשרת  
    מטרה: לוודא שהמערכת מתמודדת עם קריסות לקוחות בצורה חכמה.  
    קלט: הפסקת פעילות לקוח באמצע פעילות.  
    פלט: הלקוח נמחק מן הלקוחות שכרגע מחוברים אל השרת והרשומות שלו נמחקות.  
    איך תתבצע הבדיקה: אגרום להפסקת פעילות הלקוח המדומה ואבדוק שהמערכת מחוקות את נתוניו מהמערכת.

**תאור תרחישים (קלט ופלט) למקרי קצה**

1. בדיקה במחשב בעל מפרט נמוך

* **מטרה**: לבדוק את יכולת המערכת לפעול בסביבה מוגבלת במשאבים.
* **איך אבדוק**:
  + אתקין את המערכת במחשב עם מעבד ישן ו-RAM נמוך.
  + אבצע פעולות בסיסיות כמו פתיחת מסמכים ושליחת נתונים לשרת.
  + אפעיל גם את המחשב עם ביצועים נימוכים גם כשרת.
* **תוצאה צפויה**: המערכת תפעל בצורה תקינה עם השפעה מינימלית על המחשב.

2. בדיקת עומס נתונים

* **מטרה**: לבדוק כיצד המערכת מתפקדת כאשר מועבר אליה מידע רב בבת אחת.
* **איך אבדוק**:
  + אבצע העברת כמויות גדולות של נתונים מהעובד לשרת בזמן קצר.
  + אבדוק אם השרת מצליח לקבל ולעבד את כל המידע.
* **תוצאה צפויה**: הנתונים יעובדו במלואם ללא קריסות או עיכובים.

3. התנתקות והתחברות של מחשב אחר

* **מטרה**: לבדוק כיצד המערכת מתפקדת כאשר לקוח בעל כתובת מסוימת מתנתק ולקוח אחר מתחבר עם אותה כתובת ip (כתובת שקיבל בצורה לגיטימית בעזרת פרוטוקול DHCP).
* **איך אבדוק**:
  + אנתק לקוח שמחובר למערכת באמצעות לכבות את המחשב.
  + אחבר לקוח חדש עם אותה כתובת ip.
  + אסתכל במערכת במחשב השרת לראות את הנתונים על אותה כתובת ip.
* **תוצאה צפויה**: הנתונים ימחקו לגמרי (לצורך בטיחות למניעת מתקפות – התחזות).

**תאור תרחישים המייצרים שגיאות וכיצד המערכת אמורה להגיב ומדווחת עליהם**

בפרויקט שלחי, כשמדובר בתקשורת בין לקוח לשרת, יש צורך להגדיר תרחישים שיכולים להוביל לשגיאות ולתכנן כיצד המערכת צריכה להגיב לכל אחת מהן. הנה כמה תרחישים עיקריים:

1. **לקוח סוגר תקשורת או מתרסק (Crash):**
   * **תרחיש:** הלקוח סוגר את החיבור או מתרסק תוך כדי תקשורת עם השרת.
   * **תגובה:** השרת ייתקל בשגיאה במהלך הקריאה או כתיבה ללקוח. חשוב לוודא שהשרת מזהה ניתוק כזה בצורה מהירה. ברוב המקרים השרת יזרוק שגיאה (לדוגמה Connection reset או Connection closed) וימשיך לפעול עם לקוחות אחרים.
   * **מידע שנשמר/אובד:** המידע על אותו לקוח ימחק, אשר אותו לקוח כבר אינו מחובר למערכת. המערכת שומרת מידע אך ורק על לקוחות מחוברים על מנת למנוע תקיפות של התחזות למחשבים שונים.
2. **שרת מנתק לקוח שלא על פי פרוטוקול :**
   * **תרחיש:** שרת נתקל בכשל כלשהו בתהליך (כמו קריסת thread) ומפסיק לתפקד כראוי.
   * **תגובה:** השרת יצטרך להיות מסוגל לזהות את הקריסה ולטפל בה, לדוגמה על ידי סגירת ה - thread וניתוק הלקוח.
   * **מידע שנשמר/אובד:** אם הלקוח שולח באופן רציף מידע שאינו עובד לפי הפרוטוקול/מידע שלא ניתן לפיצוח לפי ההצפנות, הלקוח ינותק וה thread יסגר, וכל המידע שקיים על הלקוח בשרת יימחק.
3. **שרת סוגר חיבור כללי:**
   * **תרחיש:** השרת סוגר את כל החיבורים הקיימים מכל סיבה שהיא.
   * **תגובה:** השרת ייסגר בצורה פתאומית, הלקוחות אינם מקבלים מידע מן השרת ועל כך אין להם דרך לדעת שהוא נסגר.
   * **מידע שנשמר/אובד:** כל הנתונים נמחקים, דבר שאינו קריטי אשר הנתונים שנמצאים בשרת הינם נתונים זמניים שאין חשיבות רבה אם יימחקו.
4. **שרת כולו מתרסק:**
   * **תרחיש:** השרת לא זמין לחלוטין.
   * **תגובה:** הלקוח צריך להיות מסוגל לנהל את המקרה הזה ולנסות להתחבר לשרת כל פעם לפני שהוא שולח הודעה, אם הוא לא מצליח להתחבר הוא לא שולח את המידע, אם הצליח להתחבר ישלח את המידע.
   * **מידע שנשמר/אובד:** הנתונים שנשלחו לאחרונה עשויים ללכת לאיבוד, כמו שהוזכר דבר זה אינו קריטי במיוחד.