SRE home assignment

**General Guidelines**

Remember that the goal of this assignment is to assess your capabilities.

* Do not use any AI tool.
* Document the steps you are taking so we can discuss them later.
* Describe in comments any assumptions you’ve made.
* We are expecting a working code.

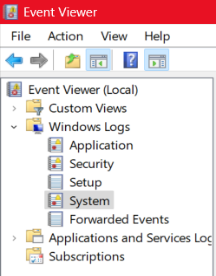
**You will be measured on the following aspects:**

* Completing the task as defined.
* Being able to describe your code.
* Organized and clean result.

**Please create the following:**

1. Write PowerShell/Batch scripts that can perform the following tasks on Windows:
   1. Check the disk space every 5 minutes and log the current date and time to a file if it's below 10%.
   2. Replace the suffix of every file in a folder from 'txt' to 'xml'.
2. A Windows server suddenly got restarted.  
   Describe the step you would take to understand when and why it happened.  
   List 3 possible reason and advice how to handle each one.
3. When you ping 'google.com' you get an IP address.
   1. Describe what this IP address represents, and which service is responsible for showing it.
   2. This IP address may change if you ping 'google.com' again, why is that?
   3. List two reasons the ping request may fail.
4. In your role you might need to instruct others on how to do some technical stuff like upgrading a software to its latest version.  
   Write a short document that describes how to access Nginx official image page in DockerHub (<https://hub.docker.com/>) and look for the latest tag for version 1.23 (e.g 1.21.4).

**Good luck!**

**Answer: question 2**

1. **בדיקת ה Event Viewer –** שם מוצגים כל הלוגים - כל אירועי השרת,   
   לדג': במידה ושירות נכשל/נפל נראה שם את השגיאה ודרכה נוכל להבין את הסיבה שבגללה זה קרה, במקרה של ריסוט השרת נסתכל באירועים שקרו סביב אותה שעה שהשרת אותחל ונחפש אירועים קריטיים שקרו או אירועים לא צפויים העלולים לגרום לנפילת השרת, ספציפית בלוגים System + Application . < מצורפת תמונה להמחשה >  
   **-** דרך כדי לזהות **מתי** התרחש הריסטרט האחרון היא לבדוק כמה זמן השרת דלוק וככה להבין את השעה המדויקת פחות או יותר שבה התרחש הריסוט ולחפש בלוגים סביבות אותה שעה.  
   **פקודת ps כדי לזהות ריסטרס אחרון :**   
   Get-CimInstance -ClassName win32\_operatingsystem | select csname, lastbootuptime

* **כמובן שמידה ויש לנו מערכת ניטור צד שלישי על השרתים ( לדג' Scom) נבדוק את ההתראות שקפצו בזמן הריסוט ונוכל להבין מתי ולמה השרת רוסט.**

1. **סיבות אפשריות לריסטרס ופתרונן :**

* **עדכוני תוכנה:** קיימים התקנות / עדכונים המצריכים ריסטרט לאחר ההתקנה, בעיקר אם מדובר בעדכונים הקשורים למערכת ההפעלה, לדג': עדכון אבטחתי במערכת ההפעלה **הדרך להימנע מריסוט מפתיע כזה –** לתזמן ריסוט מראש לאחר העדכון, נתזמן את הריסוט לזמן שבו **אין** פעילות שותפת או קריטית מול השרת כדי למנוע כישלונות באפליקציה שרצה על השרת.
* **זליגת זיכרון:** לכל שרת יש הקצאה של המשאבים הדרושים לו להרצת הפעולות על השרת (CPU, RAM ..) ברגע שהזיכרון המוקצה נגמר בעקבות תהליכים שדרשו יותר זיכרון השרת עלול לרסט את עצמו באופן אוטומטי כמנגנון בטיחות.  
  **הדרך להימנע מריסוט מפתיע כזה –** לנטר את צריכת המשאבים ולהקפיץ התראות במידה והמשאבים הפנויים יורדים מ 10% - 20% - לשקול הוספת משאבים במקרה הצורך ובדיקת הסיבה של השירותים והתהליכים הדורשים כמות משאבים גבוהה.
* **פריצת אבטחה:** סיבה נוספת לריסוט פיתאומי בשרת היא יכולה להיות פריצת סייבר לשרת והורדה של תוכנות זדוניות על השרת כדי לפרוץ לחברה ולדלות מידע קריטי על החברה.  
   **הדרך להימנע מריסוט מפתיע כזה –** שמירה על אבטחת הרשת בעזרת חברה חיצונית או צוות מיועד המנטר את אירועי ה SOC ובודק כניסות ויציאות חשודות לשרתים ומהשרתים + זהירות שיא בפתיחת פורטים ונתינת גישה לשרתים לשלוח מידע לשרתי החברה או חוסר אבטחה בסיסמאות החברה.

**Answer: question 3**

1. כשאנחנו שולחים ping ל google.com אנחנו מקבלים כתובת IP המייצגת את google.com –   
   מאחורי הקלעים השרתים מדברים בעזרת כתובות IP (או יותר נכון MAC אבל לא ניכנס לזה) , שמות השרתים נועדו בשביל האנשים המשתמשים בשרתים הללו לעזרה במקום לזכור את כל IP של האתרים שאנו פונים אליהם, יותר קל לזכור שמות ממספרים וגם בנוסף ניתן להפנות שם 1 לכמה IP שונים כדי לייצר איזון עומסים (מפורט בסעיף הבא).   
   שם השירות שאנו משתמשים בו הוא DNS – Domain Name System . שירות זה אחראי לתרגם בין שם שרת לIP והפוך.. בסביבות גדולות השירות יושב על שרת או על קבוצת שרתים הנותנים את המענה הנדרש בתרגום השמות – המחשב/שרת שרוצה לפנות לשם של שרת אחר יפנה קודם לשרת DNS המכיל רשימה של IP מול שמות של שרתים בדומיין ויקבל את הIP של השרת השני כדי שיוכל לפנות אליו.
2. אתרים גדולים ובניהם גם גוגל צריכים לספק מענה להרבה פניות ובקשות DNS לכן הם מקימים המון שרתי DNS המספקים מענה לבקשות – שיטה זו נקראת Round-robin, שיטה לאיזון העומסים וטיפול בנפח גבוה של בקשות, לכן בכל פעם שפונים לgoogle.com מקבלים שרת אחר כדי לאפשר חלוקה שווה של בקשות נכנסות ובכך לפזר את העומס בצורה שווה בין השרתים.
3. 1) חוק ב Firewall החוסם כניסה או יציאה של פרוטוקל ICMP (הפרוטוקול שבו משתמש הפקודה PING)  
   2) שרת יעד כבוי / בעיות בדרך אל היעד בנתבים או במתגים האחראים להעביר את הבקשה ליעד.

**Answer: question** 4

Document that describes how to access Nginx official image page in Docker Hub

1. Open your web browser and go to the DockerHub website (https://hub.docker.com/).
2. In the search bar at the top, type "nginx" and click on it.
3. On the Nginx image page, you will find various tabs providing information about the image. Click on the "Tags" tab.
4. Scroll through the list of available tags to find the desired version, such as 1.23. Look for the latest tag associated with version 1.23. For example, if the latest tag is 1.23.4, note down that tag.
5. For example, to pull the image run the command: "docker pull nginx:1.23.4"

For any question you can contact the author of the document by email: lidorrofehaim@gmail.com