Laboration Felsökning - Windows Avancerade Verktyg

Översiktliga labbinstruktioner för felsökning av Windows Avancerade Verktyg.

Material: Man behöver tillgång till en Windows 10/11 dator (eller VM) samt ha lokal administratörsbehörighet till operativsystemet.

Windows Performance Toolkit

1. Logga in på datorn med ett konto som är lokal administratör.
2. Starta webbläsaren och sök efter ”Windows ADK download”. Ladda hem installationsfilen till ADK och starta installationen.
3. Välj enbart **Windows Perfromance Toolkit** av alla verktyg och slutför installationen.
4. Tryck på Windows-logotypen, navigera till Windows Kits och starta Windows Performance Recorder.
5. Klicka på Mer alternativ.
6. Klicka på rullgardinsmenyn Prestandascenario till höger och välj Start (boot). Ställ in Antal iterationer till 1. Observera: I verkligheten krävs minst 3 iterationer för att få tillförlitliga resultat.
7. Klicka på Start, följt av Spara och sedan OK för att starta om datorn.
8. Vänta på att datorn startar om. Logga in igen och vänta på att spårningen ska slutföras. Datorn startar om igen.
9. Tryck på Öppna i WPA när allt är klart. Windows Performance Analyzer öppnas nu.
10. Expandera Systemaktivitet och dubbelklicka på Processer.
11. I listan med processer, scrolla upp till toppen och titta på vilka processer som startas och i vilken ordning.
12. När du undersökt Windows Performance Analyzer och den data som visas, stäng ner programmet.
13. Starta Windows Performance Recorder igen
14. Klicka på rullgardinsmenyn Prestandascenario till höger och välj Allmänt.
15. Expandera Resursanalys och markera CPU-användning, Disk-I/O-aktivitet och Fil-I/O aktivitet.
16. Öppna nu Windows Security och klicka på Virus- och hotskydd och välj sedan Snabbsökning nu.
17. Gå sedan tillbaka till Windows Performance Recorder och klicka på Start.
18. Låt det köra i cirka 30 sekunder, klicka sedan på Spara, följt av Spara. När det är klart, välj Öppna i WPA.
19. Expandera Beräkning och högerklicka på CPU-användning (Precise) och välj Lägg till graf i analysvyn.
20. Hovra nu över den översta grafen för att se vilken process som tar mest CPU-kraft.
21. Expandera sedan Lagring och sedan Diskanvändning, och högerklicka på Aktivitet efter IO-typ, process och klicka på Lägg till graf i ny analysvy.
22. Expandera Läs för att se vilka processer som använder mest diskaktivitet.
23. När du är klar. Stäng ner programmen.

WinDbg

1. Följ instruktionerna här https://learn.microsoft.com/en-us/troubleshoot/windows-client/performance/generate-a-kernel-or-complete-crash-dump för att ändra inställningar vid systemkrascher så att datorn ej startar om direkt (System – Avancerade Systeminställningar – Start och återställning)
2. Ladda hem NotMyFault verktyget från SysInternals https://download.sysinternals.com/files/NotMyFault.zip
3. Starta NotMyFault och generera en krasch av datorn, Notera blåskärmen
4. Starta om datorn
5. Installera WinDbg via Microsoft Store appen
6. Starta WinDbg och öppna dump-filen som skapats (c:\Windows\Minidump)
7. Analysera resultatet