|  |
| --- |
| Rapport |

Containrar och virtuella datorer

*En jämförelse om användar område*

|  |
| --- |
| *Författare:* Samuel Berg  *Termin:* Ht 23  *Kursnamn:* Teknisk kommunikation  *Kurskod:* 1ZT010 |



Sammandrag

Syftet med denna litteraturstudie är att få en bättre förståelse för vad olika virtuella tekniker har att ge och undersöka eventuella säkerhetsrisker samt eventuella för- och nackdelar med respektive teknologi. Detta ger de följande frågeställningarna att försöka besvaras i rapporten.

FS1: Vilka för- och nackdelar finns vid användning av containrar respektive VMs inom mjukvaruutveckling?

FS2: Vilka säkerhetsrisker har tillkommit med containrar jämfört med VMs?

Alla källorna som använts i denna litteraturstudie är vetenskapligt granskade. En fördel för containrar är att de är portabla. En fördel för VMs är att de är mer isolerade från värd-OS:et. I rapporten redovisas att det finns ingen självklart situation som kräver containrar eller VMs. Det som avgör är ändamålet som användaren strävar efter. När det kommer till tillkomna säkerhetsrisker så har containrar en större yta som kan bli attackerad i jämförelse med VMs. Det är viktigt att notera att i denna litteraturstudie tas inte alla för- och nackdelar upp. Inte heller samtliga tillkomna säkerhetsrisker med containrar jämfört med VMs diskuteras utan endast det som de redovisade källorna har handlat om.

The purpose of this literature study is to gain a better understanding of what different virtual technologies have to offer and to investigate security risks as well as pros and cons of each technology. This gives the following questions to try to answer in the report.

RQ1: What are the pros and cons of using containers and VMs in software development?

RQ2: What security risks have appeared with containers compared to VMs?

All the sources used in this literature study are scientifically reviewed. One advantage of containers is that they are portable. One advantage of VMs is that they are more isolated from the host OS. The report states that there is no obvious situation that requires containers or VMs. What determines is the purpose that the user strives for. When it comes to added security risks, containers have a larger surface that could be attacked compared to VMs. It is important to note that not all pros and cons are covered in this literature review. Nor are all added security risks with containers compared to VMs discussed, but only what the reported sources have dealt with.

Nyckelord

Docker, Containrar, VMs, Virtuella datorer, Virtuella maskiner

Innehåll

1 Inledning I

1.1 Syfte och frågeställningar I

1.2 Metod och material I

2 Resultat II

2.1 Vilka för- och nackdelar finns vid användning av containrar respektive VMs? II

2.2 Vilka säkerhetsrisker har tillkommit med containrar jämfört med VMs? III

3 Diskussion och slutsatser IV

3.1 Diskussion IV

3.2 Slutsatser IV

Referenser VI

# Inledning

Mjukvaruutvecklare är intresserade av att förbättra och utveckla både befintliga och nya verktyg, för att öka produktiviteten samt förenkla arbetssituationen hos de olika procedurerna vid programmering.

Denna litteraturstudie kommer att undersöka påverkan av *containers* (containrar) inom mjukvaruutvecklings branschen jämfört med virtuella datorer (VMs). Då man arbetar vid en lokal enhet, exempelvis en dator, använder enheten generellt endast ett operativsystem vilket i många fall kan vara begränsande vid programmering. Därför har virtuell teknik utvecklats som ger användaren möjlighet att samtidigt köra flera olika operativsystem och applikationer på en enda fysisk enhet. Arbetet kan då köras på det så kallade gäst-operativsystemet (gäst-OS) i stället för värd-operativsystemet (värd-OS). Värd-OS är det operativsystem (OS) som den fysiska enheten använder. I rapporten nämns även *image*:s vilket i detta sammanhang syftar på en avbild av allt från en applikation till ett OS.

Inom mjukvaruteknik finns det flera olika virtualiseringsmetoder och dessa som delas in flera olika klasser. I denna litteraturstudie studeras två olika klasser. Den första klassen är traditionell virtualisering där en komplett virtuell maskin används. Det innebär att traditionell virtualisering använder en komplett hårdvaruemulering och ovanpå detta ligger ett komplett operativsystem installerat. Den andra klassen kallas *containerization* (containerisera) eller ofta *Lightweight-Virtualization* [1]*.*

## Syfte och frågeställningar

I denna litteraturstudie kommer två olika typer av virtuell teknik att jämföras, containrar och VMs. Dessa två system har valts på grund av att de i nuläget är de mest välkända och mest använda av allmänheten. Syftet med studien är att få en bättre förståelse för vad olika virtuella tekniker har att ge och undersöka eventuella säkerhetsrisker. Det är även önskvärt att kunna undersöka de skillnaderna mellan de två systemen eftersom containrar och VMs är något som blir mer och mer populärt. Det blir då relevant att upptäcka för- och nackdelar med respektive system. Denna litteraturstudie kommer att fokusera på följande frågeställningar:

FS1: Vilka för- och nackdelar finns vid användning av containrar respektive VMs inom mjukvaruutveckling?

FS2: Vilka säkerhetsrisker har tillkommit med containrar jämfört med VMs?

## Metod och material

Denna rapport är en litteraturstudie. Materialet utgörs av följande akademiska artiklar [1–8].

# Resultat

I den första delen av resultatet redovisas de svar som hittats angående den första frågeställning, det vill säga de för- och nackdelar som finns vid användning av containrar och VMs. I den första delen redovisas exempel på fördelar för containers, exempelvis portabiliteten, skalbarheten samt resurseffektiviteten.

En fördel med VMs är att systemet som körs på VM:et är mer isolerat. Några andra fördelar är möjligheten till att kunna köra flera olika OS samt mognaden av att det är en äldre teknologi än containrar. I den andra resultatdelen presenteras de säkerhetsrisker som tillkommit med containrar.

## Vilka för- och nackdelar finns vid användning av containrar respektive VMs?

Mjukvaror som *Docker* gör det möjligt för ett enstaka värd-OS att isolera flera applikationer eller gäst-OS, liknande virtuella datorer. Detta genomförs inom en abstrakt abstraktion som kallas containrar. Det är en statistisk ökning av energiförbrukningen när man körde tester i Docker, mestadels på grund av prestanda för *input/output* (I/O) systemanrop. Mjukvaruutvecklare som är oroliga för höga I/O kostnader skulle kunna överväga *baremetal*-distributioner framför Docker-containerdistributioner. Baremetal-distributioner innefattar distributioner som är precis tillräckligt för att vara ett OS. I dessa sammanhang är det viktigt med egenskaper kopplade till driftsättning som portabilitet, skalbarhet och balans mellan mjukvarukrav och hårdvarukapacitet. Applikationer eller gäst-OS:en som används existerar dock inte på egen hand utan lagras på VMs eller containrar. Den mest populära container hanterings applikationen som används idag är Docker [2], [6], [7], [8].

Docker byggs vanligtvis med Linux-baserade OS. Den modell som används är vanligtvis paketeringsmodellen och den utgår ifrån respektive Linux-distribution. Detta innebär att det mesta av programvaran installeras som ett paket. När image:en har byggts upp så förblir paketen låsta för den versionen av paketen som image:en byggdes upp med. Majoriteten av paketen som ingår i image:en är inte heltids underhållna utan att de kan vara kvar i en version i flera månader innan en nyare version släpps. Först när en ny version av paketet har släppts så kan en ny imageversion byggas upp. Den gamla versionen av image:en kan fortfarande vara i bruk eftersom den är utplacerad som en container i produktion. De containrar som motsvarar gamla image:s kan innehålla föråldrade paket med kända säkerhetsbrister och buggar. Eftersom containrarna kan köras i produktion kan de utsättas för personer med skadligt uppsåt. Varje ny version av image:s är alltså ofta en förbättrad version där dessa buggar och säkerhetsrisker är borttagna [2], [3], [4], [8].

Då VMs eller/och containrar implementeras så används beräkningsresurser på ett resurseffektivt sätt. Processen att containerisera en applikation har ökat i popularitet på grund av att det lämnar ett mindre fotavtryck på hårdvaran av den fysiska enheten jämfört med VMs. En nyckelfunktion av containers är möjligheten att i produktion kunna migrera containrar tillsammans med deras applikationer som stöds till en distinkt server eller enhet utan att orsaka tjänstavbrott [1], [2], [3], [4], [8].

Containerisering är ett tillvägagångssätt för mjukvaruutveckling som syftar till att paketera en applikation tillsammans med alla dess beroenden. Samtidigt byggs en exekveringsmiljö som behövs för att köra applikationen i en lätt, fristående enhet. I denna fråga har Docker blivit den ledande industristandarden. Genom att definiera den specifika Docker image-arkitekturen och ordningen i byggandet spelar *dockerfile* (dockerfil) en viktig roll i den Docker-baserade processen av uppbyggandet av containers. Att förstå utvecklingen av *dockerfiles* (dockerfiler) och vilka byggnadstyper av dockerfiler som förbättrar dockerfilens kvalitet och minskar imagebyggandets tidsåtgång kan gynna den effektiva bearbetningen av containerisering [5].

När det kommer till VMs så är applikationerna och funktionaliteterna mer isolerande men hårdvarukrävande då det skapas ett nytt gäst-OS på din fysiska enhet. För det gäst-OS som skapats måste det tilldelas resurser från din enhet manuellt. Detta leder till att applikationen som du annars hade kört via containrar i stället körs på ett gäst-OS. Detta gäst-OS gör miljön mer isolerad vilket kort förklarat betyder att om något problem uppstår med applikationen så påverkar det inte ditt värd-OS utan endast det gäst-OS:et som applikationen körs på. Om man jämför det med vad som hade hänt om samma applikation hade körts med en container så hade även ditt värd-OS påverkats i stället för att det skulle ha varit helt isolerat till gäst-OS:et. Ett exempel på hur ditt värd-OS hade kunnat bli påverkat är exempelvis om containern skulle bli skadad. En sådan skada hade kunnat ge en permanent skada till ditt värd-OS [1-3].

## Vilka säkerhetsrisker har tillkommit med containrar jämfört med VMs?

Docker är en teknologi som dominerar inom mjukvaruutveckling när det gäller hantering av containrar. Med dess ökande popularitet uppstår nya metoder som gör det möjligt att implementera nya säkerhetsmekanismer. Det dyker upp många olika lösningar som hanterar säkerhet på nivån för containerns imageskapande parallellt med teknologier som hanterar mjukvara och Docker-miljön [2], [4], [8].

Trots eventuella säkerhetsbrister och buggar i äldre versioner så finns det möjlighet att de som använder containrar föredrar att hålla sig till äldre versioner av paket. Detta beror på paketen är kända för att fungera bra och de har testats i produktion under längre tid. Faktum är att reproducerbarhet är en av de viktigaste egenskaperna hos Docker-containrar och även för utvecklare. Orsak till detta är att användning av *containerimages* ger isolering från utvecklande beroenden och förändringar i paket som kan bryta fungerande system. Det betyder kort sagt att en nyare version kan innebära att vissa funktionaliteter slutar fungera. Detta är ett starkt incitament för att hålla sig till en föråldrad image eftersom den "bara fungerar" för den applicering den används i. En uppgradering till nya versioner av containerimage innebär alltid en viss risk. Sålunda balanserar användaren alltid mellan sitt behov av uppdatering till nya images och den möjliga sårbarheten och buggar. Även risken för att ett fungerande system går sönder på grund av oväntade ändringar i de uppgraderade paketen är en aspekt som användaren måste ta hänsyn till [2], [3], [4], [8].

Som nämndes under föregående underrubrik så finns det för- och nackdelar med containrar när det kommer till säkerhetsbrister och buggar. Dessa säkerhetsbrister och buggar finns i versioner av paket som inte underhålls på heltid. Detta är ett mer vanligt problem jämfört med underhållningen av hur den typen av applikationer körs i VMs där versionerna ofta är mer underhållna [2], [3], [4], [8].

# Diskussion och slutsatser

I den första av de kommande underrubrikerna hålls en kort diskussion om vad som undersökts i litteraturstudien, en sammanfattning samt en tolkning av resultaten. I den andra delen dras slutsatser och tolkningar utifrån alla de resultat som nämnts i rapporten. I den andra delen nämns även ett annat alternativ för mjukvaruutveckling. Alternativet ingår inte i denna studie men är en möjlig fortsättning av denna rapport.

## Diskussion

I denna litteraturstudie har jag undersökt för- och nackdelar med VMs och containrar samt tittat på tillkomna säkerhetsrisker för containrar då det är en nyare typ av teknologi jämfört med VMs. De för- och nackdelar som framkommit i undersökning innebär att det finns tillfällen då det är mer lämpligt att använda den ena teknologin över den andra. Även de säkerhetsrisker som framkommit i undersökningen pekar mot att VMS och containrar lämpar sig olika bra för olika tillfällen. Exempel på då VMs är den lämpligare teknologin att använda är när det är en prioritet att hålla mjukvaran isolerad från värd-OS:et. Ett annat exempel är att det finns fler resurser som kan hjälpa användare då man stöter på problem. Det finns också en annan anledning vilket leder till att man väljer VMs över containrar. Det handlar om att VMs inte är beroende av användarens fysiska enhets värd-OS. Med detta syftar jag på att en container alltid körs på samma OS som de värd-OS:et det ligger på vilket kan leda till nackdelar då man vill köra mjukvaran på ett specifikt OS som inte är det samma som värd-OS:et. Det finns situationer då man inte bör använda ett VM, exempelvis då mjukvaran är väldigt resurseffektiv samt då det önskas en snabb uppstartstid. Att ha en snabb uppstartstid är något som börjar bli ett mer vanligt förekommande krav för applikationer och system i dagens värld.

De situationer då containrar är mer lämpligt att använda är då det är viktigt för användaren att ha någon mjukvara som portabel, alltså att den är enkel att köra vart som helst utan några större krav. Containrar föredras även då man har en fysisk enhet med en mindre mängd resurser som kan tilldelas till användning för virtualiseringen. Detta leder till att man kan köra flertal containrar på samma mängd resurser som man kan köra endast en VM instans på. I jämförelse med VMs så har containrar en väldigt bra skalbarhet då det är enkelt att bygga upp en ny container med de senaste applikationsversionerna. Däremot krävs det en total ominstallering för ett VM. Både VM:et samt all mjukvara som är installerat på VM:et måste då ominstalleras. Det finns också situationer när det inte är lämpligt att använda containrar, exempelvis då det finns ett högre krav på säkerhet för mjukvaran man hanterar inom virtualiseringen samt om användaren behöver ett enklare sätt att koppla upp instansen till internet då detta är mycket svårare med en container jämfört med ett VM.

Det finns också en del kända för- och nackdelar som inte har tagit upp i denna litteraturstudie. Orsak till att de inte tagits upp är att det inte funnits någon relevant studie som har pekar just på dessa för- och nackdelar. Bra att vet är att det finns också möjligheter till att kombinera dessa två virtualiserings metoder, detta har inte redovisats i denna studie då det inte klassades som relevant.

## Slutsatser

Denna litteraturstudie har visat att det finns flertal för- och nackdelar med VMs respektive containrar vilket ger oss som ger användaren en tydligare bild av när och i vilken situation den ena respektive den andra teknologin ska användas. Självklart så finns det inget som säger att man inte kan använda en av teknologierna i en speciell situation men det kan vara att fördra den ena över den andra beroende på ändamålet. VMs är att föredra då det önskas en mer isolerad miljö för mjukvaran som körs samt om man vill ha färre säkerhetsrisker. Containrar är att föredra då användaren önskar något som är portabelt samt är resurseffektivt. Då containrar är en nyare teknologi än VMs så finns det vissa tillkomna säkerhetsrisker. Två exempel på tillkomna säkerhetsrisker är att vid användning av containrar ger en ökad attackyta samt att det finns större risker med äldre versioner av paket och ramverk.

# Referenser

[1] A. Abuabdo and Z. A. Al-Sharif, "Virtualization vs. Containerization: Towards a Multithreaded Performance Evaluation Approach," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-6, doi: [10.1109/AICCSA47632.2019.9035233](https://doi.org/10.1109/AICCSA47632.2019.9035233).

[2] D. Ukene, H. Wimmer and J. Kim, "Evaluating the Performance of Containerized Webservers against web servers on Virtual Machines using Bombardment and Siege," 2023 IEEE/ACIS 21st International Conference on Software Engineering Research, Management and Applications (SERA), Orlando, FL, USA, 2023, pp. 144-152, doi: [10.1109/SERA57763.2023.10197818](https://doi.org/10.1109/SERA57763.2023.10197818).

[3] S. Ramanathan, K. Kondepu, M. Tacca, L. Valcarenghi, M. Razo and A. Fumagalli, "Container Migration of Core Network Component in Cloud-Native Radio Access Network," 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 2020, pp. 1-5, doi: [10.1109/ICTON51198.2020.9328898](https://doi.org/10.1109/ICTON51198.2020.9328898).

[4] A. Maruszczak, M. Walkowski and S. Sujecki, "Base Systems for Docker Containers - Security Analysis," 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2022, pp. 1-5, doi: [10.23919/SoftCOM55329.2022.9911523](https://doi.org/10.23919/SoftCOM55329.2022.9911523).

[5] Y. Zhang, G. Yin, T. Wang, Y. Yu and H. Wang, "An Insight Into the Impact of Dockerfile Evolutionary Trajectories on Quality and Latency," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, pp. 138-143, doi: [10.1109/COMPSAC.2018.00026](https://doi.org/10.1109/COMPSAC.2018.00026).

[6] E. A. Santos, C. McLean, C. Solinas, and A. Hindle, "How does Docker affect energy consumption? Evaluating workloads in and out of Docker containers," The Journal of Systems and Software, vol. 146, pp. 14–25, 2018. doi: [10.1016/j.jss.2018.07.077](https://doi.org/10.1016/j.jss.2018.07.077).

[7] R. Kałaska and P. Czarnul, "Investigation of Performance and Configuration of a Selected IoT System—Middleware Deployment Benchmarking and Recommendations," Applied Sciences, vol. 12, no. 10, p. 5212, 2022, doi: [10.3390/app12105212](https://doi.org/10.3390/app12105212).

[8] A. Zerouali, T. Mens, G. Robles and J. M. Gonzalez-Barahona, "On the Relation between Outdated Docker Containers, Severity Vulnerabilities, and Bugs," 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), Hangzhou, China, 2019, pp. 491-501, doi: [10.1109/SANER.2019.8668013](https://doi.org/10.1109/SANER.2019.8668013).