T.C.
Radyo ve Televizyon Üst Kurulu

SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ VE KULLANIM ALANLARI

UZMANLIK TEZİ

Tuğçe ÇİÇEK

ANKARA
HAZİRAN/2021

T.C.
Radyo ve Televizyon Üst Kurulu

SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ VE KULLANIM ALANLARI

UZMANLIK TEZİ

Tuğçe ÇİÇEK

DANIŞMAN
Üst Kurul Uzmanı Fatih ÖZTÜRK

ANKARA
HAZİRAN/2021

Radyo ve Televizyon Üst Kurulu Başkanlığına,

Bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir.

	Adı Soyadı	İmza
Başkan :		
Üye :		
Üye :		
Üye :		
Üye :		

ONAY

…./…./2021

Üst Kurul Başkanı

Ebubekir ŞAHİN

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulunda görev yapan Üst Kurul Uzman Yardımcısı olarak, Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi'ne uygun şekilde hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplayıp sunduğumu; ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim.

Bilgilerinizi ve gereğini arz ederim.

Tarih

Adı-Soyadı-Unvanı-İmzası

Uzmanlık Tezinin Adı:
……
……
……
EK:
-Tez (6 adet)
-CD (1 adet)

Tezi Teslim Alan

Daire Başkanı

Tarih

Adı-Soyadı-İmzası

Bu tez çalışmasının hazırlanmasında desteklerini esirgemeyen başta Üst Kurul Başkanı Sayın Ebubekir ŞAHİN'e, Sayın Üst Kurul Üyelerine, Daire Başkanım Sayın Olcay ÇİÇEKLİTAŞ'a ve Daire Başkan Yardımcım Sayın İbrahim ESER'e ve tez danışmanım Sayın Fatih ÖZTÜRK'e teşekkürlerimi sunarım.

Hayatımın her safhasında bana olan desteklerini esirgemeyen canım aileme teşekkür ederim. Bu çalışmayı; çalışma sırasında ve tüm hayatım boyunca en büyük destekçilerim olan sevgili kardeşim Melike AÇLAN'a ve sevgili eşim Emre ÇİÇEK'e ithaf ediyorum.

İÇİNDEKİLER

İÇİNDEKİLER I
ŞEKİLLER V
TABLOLAR VI
TANIMLAR VE KISALTMALAR VII
GİRİŞ 1
Tezin Konusu 2
Tezin Amacı 3
Tezin Önemi 3
Tezin Yöntemi 4
Tezin Kapsamı ve Sınırlılıkları 4
BİRİNCİ BÖLÜM 5
SANALLAŞTIRMA TEKNOLOJİSİ 5
1.1. SANALLAŞTIRMA KAVRAMI 5
1.1.1. Sanallaştırma Tarihi 8
1.1.2. Sanallaştırmanın Çalışma Mantığı 11
1.1.3. Sanallaştırmanın Hedefleri 12
1.2. HİPER YÖNETİCİLER 13
1.2.1. Tip 1 Hiper Yönetici 14
1.2.2. Tip 2 Hiper Yönetici 16
1.3. SANAL MAKİNE 18
1.3.1. Sanal Makine Kavramı 18
1.3.2. Sanal Makine Çalışma Prensibi 20
1.3.3. Sanal Sunucunun Klonlanması 20
1.3.4. Sanal Makinede Şablon Oluşturmak 22
1.3.5. Sanal Makinelerde Anlık Görüntü Almak 22
1.3.6. Açık Sanallaştırma Formatı (OVF) 24
1.3.7. Sanal Makinelerin Taşınması 26
1.3.8. Sanal Makinenin Güvenliği 27
İKİNCİ BÖLÜM 30
SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ VE KULLANIM ALANLARI 30

2.1. SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ 30
2.1.1. Tam Sanallaştırma 30
2.1.2. Kısmi Sanallaştırma 30
2.1.3. İşletim Sistemi Düzeyinde Sanallaştırma 31
2.1.4. Sunucu Sanallaştırma 32
2.1.4.1. Fiziksel Sunucu ve Sanal Sunucu Tarafından İhtiyaç Duyulan Kaynakların Karşılaştırmalı Analizi 34
2.1.4.2. Sunucu Sanallaştırmasının Uygulama Etkisi Analizi 35
2.1.4.3. Sunucu Sanallaştırma Güvenlik Önlemleri 37
2.1.5. Depolama Sanallaştırma 38
2.1.5.1. Depolama Alan Ağı (SAN) 39
2.1.5.2. Ağa Bağlı Depolama (NAS) 41
2.1.6. Ağ Sanallaştırma 41
2.1.6.1. Ağ Sanallaştırmanın Faydaları 42
2.1.7. Ağ İşlevleri Sanallaştırma 42
2.1.8. Uygulama Sanallaştırma 43
2.1.9. Masaüstü Sanallaştırma 44
2.1.9.1. Sanal Masaüstü Altyapısı (VDI) 46
2.1.9.2. Hizmet Olarak Masaüstü (DaaS) 48
2.1.10. Servis Sanallaştırma 48
2.1.11. Konteyner Tabanlı Sanallaştırma 49
2.1.11.1. Konteyner Tabanlı Sanallaştırma Örnekleri 50
2.1.11.2. Kubernets 52
2.1.11.3. Konteyner Tabanlı Sanallaştırmanın Avantajları 53
2.1.11.4. Konteyner Tabanlı Sanallaştırmanın Dezavantajları 55
2.1.11.5. Sanal Makineler ile Konteynerler'ın Karşılaştırılması 56
2.2. SANALLAŞTIRMANIN KULLANIM ALANLARI 61
2.2.1. Sunucu Sanallaştırma Kullanım Alanları 61
2.2.2. Depolama Sanallaştırma Kullanım Alanları 62
2.2.3. Ağ Fonksiyonları Sanallaştırma Kullanım Alanları 62
2.2.4. VDI Kullanım Alanları 64
2.2.5. Servis Sanallaştırma Kullanım Alanları 65
2.2.6. Konteyner Sanallaştırmanın Kullanım Alanları 65
2.2.7. Sanallaştırmada Bulut Bilişim Kullanımı 66
ÜÇÜNCÜ BÖLÜM 68

SANALLAŞTIRMADA SÜREÇ VE YÖNTEMLER, KULLANILAN YAZILIMLAR 68
3.1. SANALLAŞTIRMADA SÜREÇ VE YÖNTEMLER 68
3.1.1. Sanallaştırmaya Geçiş Süreci 68
3.1.2. Sanallaştırmaya Hazırlık 68
3.1.3. Sanallaştırmanın Etkinleştirilmesi 70
3.1.4. Sanallaştırmanın Bakımı ve Sürdürülmesi 71
3.1.5. Süreç Konusunda Öneriler ve Uyarılar 73
3.2. SANALLAŞTIRMADA KULLANILAN YAZILIMLAR 74
3.2.1. Açık Kaynak Kodlu Sanallaştırma Yazılımları 74
3.2.2. Ticari Sanallaştırma Yazılımları 77
3.3.2.1. Ücretsiz Ticari Sanallaştırma Yazılımlarına Örnekler 77
3.3.2.2. Ücretli Ticari Sanallaştırma Yazılımlarına Örnekler 78
3.2.2.3. Ticari Sanallaştırma Yazılımlarının Sağladığı Özellikler 79
DÖRDÜNCÜ BÖLÜM 85
SANALLAŞTIRMADA BİLGİ GÜVENLİĞİ VE SANAL SİSTEMLERE YÖNELİK TEHDİTLER 85
4.1. SANALLAŞTIRMANIN BİLGİ GÜVENLİĞİ ÜZERİNDEKİ ETKİLERİ 85
4.1.1. Bilgi Güvenliği ve Bilgi Güvenliği Yönetimi 85
4.1.2. Bilgi Güvenliği Yönetim Sistemi 86
4.1.3. İlgili Standartlar 87
4.2. SANALLAŞTIRMADA BİLGİ GÜVENLİĞİ SORUNUNUN İNCELENMESİ 88
4.3. SANAL SİSTEMLERE YÖNELİK GÜVENLİK TEHDİTLERİ 93
4.3.1. Sanal Makine Yayılımı (VM Sprawl) 95
4.3.1.1. Sanal Makine Yayılımına Karşı Önlemler: 96
4.3.2. Sanal Makine Kaçışı (VM Escape) 99
4.3.2.1. Sanal Makine Kaçışına Karşı Önlemler 100
4.3.3. Çapraz Sanal Makine Yan Kanal Atakları 102
4.3.3.1. Çapraz Sanal Makine Yan Kanal Ataklarına Karşı Önlemler 103
4.3.4. Güvensiz Sanal Makine Göçü 103
4.3.4.1. Güvensiz Sanal Makine Göçüne Karşı Önlemler 104
4.3.5. Hyperjacking Saldırısı 106
4.3.5.1. Hyperjacking Saldırısına Karşı Önlemler 107
4.3.6. Sanal Makine Atlama Saldırısı (VM Hopping) 107

4.3.6.1. Sanal Makine Atlama Saldırısına Karşı Önlemler 108
4.3.7. Kötücül Sanal Makine Saldırısı (Malicious VM Attack) 109
4.3.7.1. Kötücül Sanal Makine Saldırılarına Karşı Önlemler 109
4.3.8. Sanal Makine Geri Alma Saldırısı (VM Rollback) 110
4.3.8.1. Sanal Makine Geri Alma Saldırılarına Karşı Önlemler 110
4.3.9. Sanal Makine DoS ve DDoS Saldırıları 111
4.3.9.1. Sanal Makine DoS ve DDoS Saldırılarına Karşı Önlemler 112
4.3.10. Zararlı Yazılımlar 112
4.3.10.1. Kötü amaçlı yazılıma bir örnek: Crisis 112
4.3.10.2. Zararlı Yazılımlara Karşı Önlemler 113
BEŞİNCİ BÖLÜM 116
SANALLAŞTIRMADA YENİ YAKLAŞIMLAR VE SANALLAŞTIRMA TEKNOLOJİSİNİN YARARLARI 116
5.1. SANALLAŞTIRMADA YENİ YAKLAŞIMLAR 116
5.1.1. Veri Merkezi Mimarisi Evrimi 116
5.1.2. Yazılım Tanımlı Depolama (SDS) 117
5.1.3. Yazılım Tanımlı Veri Merkezi (SDDC) 118
5.1.4. Eski Altyapı Yığını (Legacy Infrastructure Stack) 119
5.1.5. Yakınsak Altyapı Mimarisi (CI) 120
5.1.5.1. Yakınsak Altyapı Mimarisinin Avantajları ve Dezavantajları ... 120
5.1.5.2. Yakınsak Altyapı Mimarisinin Sınırlamaları ve Dikkat Edilmesi Gereken Hususlar 121
5.1.6. Hiper Yakınsak Altyapı Mimarisi (HCI) 122
5.1.6.1. Hiper Yakınsak Altyapı Mimarisinin Kullanım Durumları 124
5.1.6.2. Yakınsak ve Hiper Yakınsak Altyapı Mimarilerinin Karşılaştırması 125
5.2. SANALLAŞTIRMANIN YARARLARI 126
SONUÇ VE ÖNERİLER 132
KAYNAKÇA 139
ÖZET 148
ABSTRACT 150

ŞEKİLLER

Şekil 1.1 : Geleneksel sistem mimarisi 6
Şekil 1.2 : Sanallaştırma sonrası sistem mimarisi 8
Şekil 1.3 : NACA'da bulunan 1957 yılına ait IBM 704 ana bilgisayarı 9
Şekil 1.4 : Konuk I/O işleme 13
Şekil 1.5 : Tip 1 hiper yönetici 15
Şekil 1.6 : Hiper yöneticideki bir konuk hatası 16
Şekil 1.7 : Tip 2 hiper yönetici 17
Şekil 1.8 : Sanal makinenin basitleştirilmiş gösterimi 19
Şekil 1.9 : Sanal ortamda basitleştirilmiş bir veri talebi 19
Şekil 1.10 : Sanal makine klonlama ve özel sistem adı belirleme 21
Şekil 1.11 : Anlık görüntü disk zinciri 23
Şekil 1.12 : OVF dışa ve içeri aktarma 25
Şekil 1.13 : Sanal makinenin taşınması 27
Şekil 2.1 : İşletim sistemi düzeyinde sanallaştırma 31
Şekil 2.2 : 2019'da Kuzey Amerika ve Avrupa'daki işletmeler tarafından mevcut ve planlanan sanallaştırma teknolojilerinin türe göre benimsenmesi 34
Şekil 2.3 : Sanal sunucu ile fiziksel sunucu arasındaki ana performansın karşılaştırmalı analizi 36
Şekil 2.4 : Sanal sunucu ile fiziksel sunucu arasındaki ana performansın karşılaştırmalı analizi 37
Şekil 2.5 : Sanal masaüstü altyapısına uç nokta cihazlarla erişim 46
Şekil 2.6 : Kubernetes orkestratörünün mimarisi 53
Şekil 2.7 : Sanal makine ve konteyner kıyaslama 56
Şekil 2.8 : 600 saniyede işlenen talepler 58
Şekil 2.9 : İlk 400 saniye için talep süresi 59
Şekil 2.10 : Sanal makineler ve konteynerlar arasında ölçeklenebilirlik 60
Şekil 3.1 : KVM Mimarisi 76
Şekil 3.2 : İki ana makine arasında canlı geçiş 81
Şekil 4.1 : Sanal makine yüzeyine saldırı 93
Şekil 4.2 : Sanal makinelerde en çok görülen saldırı türleri 95
Şekil 4.3 : Sanal makine kaçışı 100
Şekil 4.4 : VM hyperjacking saldırısında kodun hiper yönetici hâline gelmesi 106
Şekil 5.1 : 2015'ten 2021'e kadar dünya genelindeki veri merkezlerinde gerçekte depolanan veri miktarı 116
Şekil 5.2 : Veri merkezinin evrimi 117
Şekil 5.3 : SDS ve yazılım katmanı 118
Şekil 5.4 : Hiper yakınsak altyapının fiziksel gösterimi 122
Şekil 5.5 : Hiper yakınsak altyapı, sanallaştırmanın geleneksel bileşenlerini tek bir birleşik platformda birleştirir. 124
Şekil 5.6 : Geleneksel, yakınsak ve hiper yakınsak altyapıları 126

TABLOLAR

Tablo 2.1 : Fiziksel sunucu ile sanal makine arasındaki kaynak karşılaştırmasını göstermektedir. 35
Tablo 4.1 : Bilgi güvenliği sorunu incelemesi 911

TANIMLAR VE KISALTMALAR

ACL Erişim Kontrol Listesi (Access Control List)

AES Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

API Uygulama Programlama Arayüzü (Application Programming Interface)

App-V Uygulama Sanallaştırma (Application Virtualization)

ARP Adres Çözümleme Protokolü (Address Resolution Protocol)

AWS Amazon Web Service

BT Bilgi Teknolojileri

Caas Hizmet Olarak Konteynerlar (Containers-as-a-Service)

CBV Konteyner Tabanlı Sanallaştırma (Container Based Virtualization)

CD Kompakt Disk (Compact Disc)

CI Yakınsak Altyapı (Converged Infrastructure)

COS Konsol İşletim Sistemi (Console Operating System)

CPU Merkezi İşlem Birimi (Central Processing Unit)

DaaS Hizmet Olarak Masaüstü (Desktop-as-a-Service)

DMZ Savunmasız Bölge (Demilitarized Zone)

DoS Disk İşletim Sistemi (Disk Operating System)

DVD Dijital Çok Yönlü Disk (Digital Versatile Disc)

FC Fiber Kanal (Fiber Chanel)

HCI Hiper Yakınsak Altyapı **(**Hyperconverged Infrastructure)

HDD Sabit Disk (Hard Disc)

IBM Uluslararası İş Makineleri (International Business Machines)

IaaS Hizmet Olarak Altyapı (Infrastructure as a Service)

IDS Intrusion Detection Systems

IEC Uluslararası Elektroteknik Komisyonu(International Electrotechnical Commission)

I/O Giriş/Çıkış (Input/Output)

IoT Nesnelerin İnterneti (Internet of Things)

IPC Süreçler Arası İletişim (InterProcess Communication)

IPS Saldırı Önleme Sistemi (Intrusion Prevention System)

ISO Uluslararası Standartlar Organizasyonu (International Organization for Standardization)

IT Bilgi Teknolojisi (Information Technology)

ITaaS Hizmet olarak Bilgi Teknolojileri **(**IT-as-a-Service)

ITIL Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technologies Infrastructure Library)

KVM Çekirdek Tabanlı Sanal Makine (Kernel based Virtual Machine)

LAN Yerel Alan Ağı (Local Area Network)

LUN Mantıksal Birim Numarası (Logical Unit Number)

LXC Linux Konteyneri (Linux Container)

LXD Linux Konteyner Arka Plan Programı (Linux Container Daemon)

MEC Çok Erişimli Kenar Bilgi İşlem (Multi-Access Edge Computing)

NAS Ağa Bağlı Depolama (Network Attached Storage)

NFS Ağ Dosya Sistemi (Network File System)

NFV Ağ Fonksiyonları Sanallaştırma (Network Function Virtualization)

NV Ağ Sanallaştırma (Network Virtualization)

OS İşletim Sistemi (Operating System)

OVA Açık Sanal Cihaz **(**Open Virtual Appliance)

OVF Açık Sanallaştırma Formatı (Open Virtualization Format)

PaaS Hizmet Olarak Platform (Platform as a Service)

PC Kişisel Bilgisayar (Personal Computer)

PID İşlem Kimliği (Process ID)

RAM Rastgele Erişim Belleği (Random Access Memory)

SaaS Hizmet Olarak Yazılım (Software as a Service)

SAN Depolama Alanı Ağı (Storage Area Network)

SCSI Küçük Bilgisayar Sistem Arayüzü (Small Computer System Interface)

SDS Yazılım Tanımlı Depolama (Software Defined Storage)

SDDC Yazılım Tanımlı Veri Merkezi Software (Defined Data Center)

SSD Katı Hal Sürücüsü (Solid State Driver)

TAR Teyp Arşivi (Tape Archive)

TB	Terabayt
TCB	Güvenilir Bilgi İşlem Tabanı (Trusted Computing Base)
UYG	Uygulama
V	Sanallaştırma (Virtualization)
VDI	Sanal Masaüstü Altyapısı (Virtual Desktop Insfracture)
VHD	Sanal Sabit Disk (Virtual Hard Disk)
VIS	Sanal Komut Seti (Virtual Instruction Set)
VLAN	Sanal Yerel Alan Ağı (Virtual Local Area Network)
VM	Sanal Makinesi (Virtual Machine)
VMDK	Sanal Makine Diski (Virtual Machine Disk)
VMFS	Sanal Makine Dosya Sistemi (Virtual Machine File System)
VMM	Sanal Makine Monitörü (Virtual Machine Monitor)
VMS	Sanal Bellek Sistemi (Virtual Memory Sistem)
VNF	Sanallaştırılmış Ağ İşlevleri (Virtualized Network Functions)
VPN	Sanal Özel Ağ (Virtual Private Network)
WAN	Geniş Alan Ağı (Wide Area Network)
ZB	Zettabyte

GİRİŞ

Sanallaştırma, bilgisayar kaynaklarının soyutlanması anlamına gelen bir terimdir. Sanal bilgi işlem ortamının amacı, heterojen ve özerk kaynakların bir araya getirilmesine dayalı olarak kullanıcılar ve uygulamalar için birleşik bir entegre işletim platformu sağlayarak kaynak kullanımını iyileştirmektir.

Sanallaştırmanın popülaritesi son yıllarda önemli ölçüde artmış olsa da sanallaştırma kavramının kökeninin, IBM'in çözümleri geliştirmeye çok fazla zaman ayırdığı 1960'ların sonlarındaki ana bilgisayar günlerine kadar gittiği bilinmektedir. IBM, sanallaştırmayı büyük ana bilgisayarları birkaç mantıksal birime bölmek ve donanımları tek fiziksel ana bilgisayar üzerinde çalıştırmak için geliştirmiştir. Bölümleme özelliği, birden fazla işlemin ve uygulamanın aynı anda çalışmasına izin vermektedir. Böylece ortamın verimliliği artmakta ve bakım yükü azalmaktadır. Bu alanda çalışan bilim insanları, sanallaştırmanın kaynak kullanımını iyileştirmenin ve veri merkezi yönetimini basitleştirmenin en iyi yolu olarak görmüştür.

Günümüzde sanallaştırma kritik ve yaygın olarak kullanılan bir teknolojidir. Sanallaştırma kaynakları işletim sistemleri arasında ayırarak fiziksel bilgisayarların yeteneklerini dağıtmak için kullanır. Ayrıca sanal makine, güncel bilgi işlem sistemleri için yönetilebilir ortamlar sunabilir. Sanallaştırmanın yönetilebilirlik, esneklik, ayırma, kesinti süresini azaltma, maliyet verimliliği ve ölçeklenebilirlik gibi çeşitli avantajları vardır ama en önemli işlevi, birden çok işletim sistemini ve uygulamayı tek bir bilgisayar veya sunucu üzerinde çalıştırma yeteneğidir. Bu, daha az sunucu ile elde edilen daha fazla üretkenlik anlamına gelir. Sanallaştırma, kaynakları dengeleyebilen ve yalnızca kullanıcının ihtiyaç duyduğu şeyi sağlayabilen teknoloji olması nedeniyle uygulama performansını arttırır, yönetimsel masrafları azaltır, sistem kaynaklarının daha etkin şekilde kullanılmasını ve veri merkezlerinde kullanılan alanlardan tasarruf edilmesini sağlar. Kısaca sanallaştırma fiziksel kaynakların maksimum verim ile kullanılmasına olanak sağlamaktadır.

Farklı iş gereksinimlerinin tek bir platform üzerinde çalıştırılabilmesi, yönetimsel kolaylık sağlaması, kaynak verimliliği ve maliyet azaltması açısından büyük faydalar sağlamaktadır. Sanallaştırmanın birçok çeşidi vardır ve kurumsal veri merkezlerinde fiziksel donanımı soyutlamak, CPU'lar, bellek, diskler, dosya depolaması, uygulamalar ve ağ iletişiminden oluşan büyük birleştirilmiş mantıksal kaynak havuzları oluşturmak gibi farklı iş ihtiyaçlarına göre farklı sanallaştırma teknikleri kullanılmaktadır.

Tezin Konusu

Günümüzde sanallaştırma kritik ve yaygın olarak kullanılan bir teknolojidir. Sanallaştırmanın yönetilebilirlik, esneklik, ayırma, kesinti süresini azaltma, maliyet verimliliği ve ölçeklenebilirlik gibi çeşitli avantajları vardır. Bu tezde, sanallaştırmanın potansiyel mekanizmaları ve araçları hakkında kapsamlı bir araştırma yapılmıştır.

Bu kapsamda beş bölümden oluşan "Sanallaştırma Teknolojileri Yöntemleri ve Kullanım Alanları" adlı tez çalışmasının birinci bölümünde sanallaştırma ile ilgili temel kavramlar ve sanal makinenin özellikleri anlatılmaktadır.

İkinci bölümde, sanallaştırma teknolojileri yöntemleri ve kullanım alanları incelenmiş ve sanallaştırmanın dünya ölçeğinde en yaygın kullanım alanına sahip olan sunucu sanallaştırma için yapılan çalışmalar istatistiksel verilerle ayrıntılı şekilde incelenmiştir. Ayrıca tam sanallaştırma, paravirtiualization, masaüstü sanallaştırma, ağ sanallaştırma ve konteyner tabanlı sanallaştırma gibi sanallaştırma mekanizmaları gözden geçirilmiştir.

Tezin üçüncü bölümünde, sanallaştırmada süreç ve yöntemler ile kullanılan sanallaştırma yazılımları ele alınmıştır. Bu kapsamda sanallaştırmaya geçiş süreçlerinden bahsedilmiş ve bu süreçte önerilerde bulunulmuştur. Ayrıca kullanılan sanallaştırma yazılımlarının sağladığı avantajlardan bahsedilmiştir.

Dördüncü bölümde, sanallaştırmada bilgi güvenliği incelenmiş ve sanal sistemlere yönelik güvenlik tehditleri anlatılmıştır. Bilgi güvenliğini sağlamak amacıyla öncelikle güvenlik prensipleri ortaya konulmuş ve bu kavramlara açıklık

getirilmiştir. Ardından bilgi güvenliği ile ilgili ulusal düzenlemelerden bahsedilmiştir. Kurumsal bilgi güvenliğini sağlamak için uluslararası kabul görmüş ISO 27001 standardının kurumlarda oluşturulmasını zorunlu gördüğü Bilgi Güvenliği Yönetim Sisteminden bahsedilmiştir. Sanal sistemlerde güvenlik tehditlerinin nasıl oluştuğu ve saldırıların sistemlere ne tür zararlar verdiği incelenmiştir. Sanal sistemlerin güvenliğinin sağlanması adına alınması gereken güvenlik önlemleri, uygulanmakta olan önlemler ile araştırmalar neticesinde edinilen yeni bulgularla derlenmiştir.

Tezin beşinci bölümünde ise sanallaştırmada yeni yaklaşım yakınsak ve hiper yakınsak altyapı mimarisi anlatılmıştır. Bu mimarilerin avantajlarından ve dezavantajlarından bahsedilmiş ve sanallaştırmanın sağladığı yararlar anlatılmıştır.

Sonuç ve değerlendirme bölümünde ise sanallaştırma teknolojilerinin bugün geldiği düzey ele alınmış ve uygulama alanında önerilerde bulunulmuştur. Sanal sistemlerin kullanımı ve bilgi güvenliğini sağlamak için kurum içinde alınması gereken teknik ve idari tedbirler değerlendirilmiştir.

Tezin Amacı

Bu tez çalışmasının amacı sanallaştırma teknolojileri yöntemlerinin araştırılması, uygulama öncesi doğru planlanma yapılması, uygulama sırasında ve sonrasında oluşabilecek aksaklıkların önlenmesi, sanallaştırma sistemlerinde kurumsal bilgi güvenliğini tehlikeye atabilecek tehdit ve saldırıların incelenmesi ve gereken önlemlerin alınması, yeni sanallaştırma teknoloji metotlarının araştırılmasıdır.

Tezin Önemi

Artan talep, değişen iş gereksinimleri ve yeni teknolojilerin var olan sisteme entegre edilememesi, bilgi teknolojileri altyapısının hızla karmaşık hâle gelmesine ve iş sürekliliğinin sağlanamamasına yol açmaktadır. Bu durumla karşılaşmamak için sürekli gelişen teknolojilere ayak uydurmak ve bu alanda yapılan çalışmaların güncel tutulması gerektirmektedir. Bu çalışma, iş sürekliliğinin sağlanmasında en önemli unsurlardan biri olan sanallaştırma teknolojisi farkındalığının arttırılmasına katkıda bulunacaktır. Değişen iş ihtiyaçlarına uyum sağlamak için tamamlayıcı nitelikteki sanallaştırma teknolojilerinin arasından seçim yapılması yol haritasının

belirlenmesinde büyük öneme sahiptir. Bu çalışmanın doğru hizmet alımı kararlarının verilebilmesi için hangi yöntemlerin kuruma uygun olduğunun araştırılarak belirlenmesi; bu hususta bilgi güvenliğini tehdit eden olası risklerin bertaraf edilmesi için gereken önlemlerin alınmasıyla kurumumuz bilgi varlıklarının korunması ve yeni teknolojilerine ayak uydurarak iş sürekliliğinin sağlanması kapsamında katkı sağlayacağı düşünülmektedir.

Tezin Yöntemi

Bu tez çalışmasında yöntem olarak "Kaynak Tarama Yöntemi" kullanılmıştır. Gerekli bilgi ve belgeler basılı kaynaklar, bilimsel veritabanları (IEEE Explore, ACM Digital Library, Taylor & Francis, Science Direct - ELSEVIER, Wiley Online Library, Springer, Cambridge Journals Online),yayımlanmış tezler ve kurumsal web siteleri taranarak toplanmıştır. İlgili veriler tezin amacı doğrultusunda bilimsel etik ve kurallara uygun biçimde aktarılmıştır.

Tezin Kapsamı ve Sınırlılıkları

Bu çalışmada, sanallaştırma teknolojileri kurumsal olarak kullanılabilecek yöntemler bağlamında incelenecektir. Bu bağlamda öncelikle sanallaştırma teknoloji türleri, sanallaştırma geçiş süreçleri ve sanal sistemlerin güvenliğini zaafa uğratan tehdit ve saldırı türleri incelenmiştir. Sanallaştırma yöntemlerinin sayıca çok olması sebebiyle kurum için en yararlı olabilecek yöntemler incelenmiş diğer yöntemler bu tezde konu edilmemiştir. Kurum içinde kullanılmakta olan teknoloji ve verilerin kamuya açık bir çalışmada belirtilmesinin uygun olmayacağı düşünüldüğünden bu tezde bahsedilmemiştir.

BİRİNCİ BÖLÜM

SANALLAŞTIRMA TEKNOLOJİSİ

1.1. SANALLAŞTIRMA KAVRAMI

Sanallaştırma, donanım, yazılım, ağ, depolama, zaman paylaşımı gibi bir ya da daha fazla kavram veya teknolojiyi uygulayarak farklı katmandaki kaynakların aynı fiziksel ekipman kaynaklarının birbirinden izole edilerek kullanılmasını sağlayan bir metodoloji olarak tanımlanabilir.[1]

Sanallaştırma teknolojisi fiziksel bir bilgisayarı iki veya daha fazla bilgisayarmış gibi çalıştırma yöntemidir. Sanallaştırılmış bilgisayar, fiziksel bilgisayarla aynı temel mimariye sahiptir. Sanallaştırma teknolojisi, bir işletim sisteminin gerçekten var olmayan donanım üzerine kurulmasına izin verir ve bir bilgisayarın kaynaklarının aynı anda birden çok ortama bölünmesine ya da paylaşılmasına olanak sağlar. Bu ortamlar birlikte veya birbirinden tamamen bağımsız çalışabilir. Sanal makineler (Virtual Machine) olarak bilinen ortamlar genellikle bir işletim sistemi kurulumunu barındırır (Linux, Windows vb.). Bu işletim sistemi yüklemeleri konuk işletim sistemleri olarak bilinir.[2]

Sanallaştırma; sistem yönetiminin kolaylaştırılmasını, mevcuttaki donanım kaynaklarının daha etkin kullanılmasını ve doğru kaynak planlaması için elverişli ortamın oluşmasını sağlamaktadır.

Sanallaştırmanın ilk hedefi kullanılmayan kaynakları tekrar değerlendirip aynı anda birden fazla işletim sistemini aynı fiziksel sistem üzerinde çalıştırmaktır. Günümüzde ise neredeyse her katmanda ayrı bir sanallaştırma teknolojisi kullanılmaktadır.[3]

---

[1] Thomas Olzak vd., *Microsoft Virtualization: Master Microsoft Server, Desktop, Application, and Presentation Virtualization*, United States of America, Syngress, 2010, s.3-5
[2] David Marshall vd., *Advanced Server Virtualization: VMware and Microsoft Platforms in the Virtual Data Center*, United States of America , Taylor & Francis Group, 2006, s.3-8
[3] Tuncay Merdan, *Sanallaştırmanın Bilgi Teknolojilerine Getirdiği Yenilikler ve Uygulamaları*, Yüksek Lisans Tezi, İstanbul, Haliç Üniversitesi, Fen Bilimleri Enstitüsü, 2010, s.3

Sanallaştırılmış bir ortamı daha iyi anlamak için, geleneksel bir fiziksel bilgisayarın temel bilgisayar organizasyonunu sanallaştırma platformu çalıştıran bir ortamla karşılaştırmak faydalı olacaktır.[4]

Sanallaştırma öncesi geleneksel sistem mimarisinde;

- Her fiziksel sunucu üzerine yalnızca bir işletim sistemi kurulabilmektedir.
- Her bir rol için (dosya, yedekleme, veri tabanı sunucusu gibi) ayrı fiziksel sunucular kullanılmaktadır.
- Geleneksel sistem; işletim sistemi, donanım, depolama ve uygulamadan oluşan birleşik birimdir. Bu da işletim sistemlerini ve network kaynaklarını belirli bir fiziksel donanıma, uygulamaları ise işletim sistemine ve donanıma bağımlı kılar.
- Geleneksel yapıdaki veri depolama üniteleri belirli bir yerdeki fiziksel donanıma bağımlı olduğu için depolamada yeterli alan kalmadığında yeni bir sunucu ile değiştirilmesi gerekir.
- Fiziksel sunucunun kaynakları yüksek oranda atıldır. Ayrıca fiziksel sunucuları güncellemek ve kopyalamak oldukça zordur. [5]

Geleneksel Sistem Mimarisi Şekil 1.1'de gösterilmiştir.



Şekil 1.1 : Geleneksel sistem mimarisi[6]

[4] T. Olzak, 2010, s.4.
[5]Malhotra vd., , Virtualization in Cloud Computing, Amity University, Noida, *Information Technology & Software Engineering Journal* ,/2 (2014):2
[6] D. Marshall vd.., 2006, s.4.

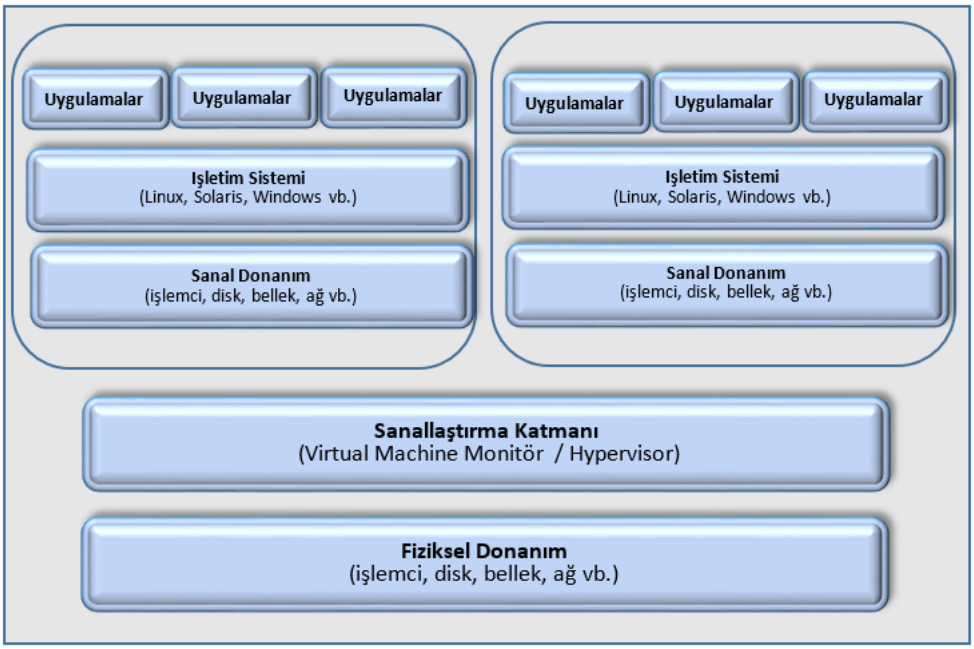
Yukarıdaki bilgiler ışığında geleneksel mimariye sahip sunucuların dezavantajları avantajlarına oranla daha fazladır.

Sanallaştırma sonrasındaki sistem mimarisinde;

- Sanal makine, disk üzerindeki gerçek bir bilgisayar gibi hareket eden bir bilgisayar dosyasıdır.
- Birden çok sanal makine aynı anda tek bir fiziksel bilgisayarda çalışabilir.
- Sanal makine yöntemi ile işletim sistemi spesifik bir fiziksel donanıma bağımlı olmaktan çıkar. Böylece fiziksel donanım sistemlerine ve bunların bakımına duyulan gereksinim azaltılarak maliyetler düşürülür.
- Sanal uygulama yöntemi ile uygulamalar çalışacağı mevcut işletim sistemine bağımlı olmaktan çıkar ve istenildiğinde herhangi bir bilgisayara taşınabilir.
- Sanal makine belirli bir yerdeki fiziksel depolama ve network kaynaklarına bağımlı değildir; Bu sayede sanal depolama ve network kaynaklarını kullanabilir. [7]
- Sanallaştırma sisteminde bir problemle karşılaşıldığında, sanal sunucuların hızlı bir şekilde önceki durumuna getirilebilme imkanı vardır. Ayrıca ihtiyaç halinde test veya yazılım geliştirme için yeni sunucular oluşturma olanağı da sağlanmış olur.[8]

Tüm bu bilgiler ışığında sanallaştırılma sonrası sistem mimarisi Şekil 1.2'de gösterilmiştir.

[7] T. Merdan, 2010, s.5-6
[8] a.g.m., s.6



Şekil 1.2 : Sanallaştırma sonrası sistem mimarisi[9]

1.1.1. Sanallaştırma Tarihi

Sanallaştırma teknolojisinin geçmişi, çoğu insanın düşündüğünden daha eskilere dayanmaktadır. Aslında sanallaştırma fikri ilk olarak 1950'lerin sonlarına kadar tartışılmıştır. [10] Sanallaştırma tarihi, IBM'de bir programcı olan Jim Rymarczyk'in IBM ana bilgisayarını (mainframe) 1960'da sanallaştırmasıyla başlamıştır. IBM, dahili kullanım için CP-40 ana çerçevesini tasarlamış ve bu sistem, aynı anda birden fazla uygulamayı çalıştırmak için bölümleme teknolojisini kullanan CP-67'ye dönüşmüştür.[11] Şekil 1.3'te IBM ana bilgisayarı gösterilmiştir.

[9] D. Marshall vd.., 2006, s.5.
[10] Shashank Mohan Jain, *Linux Containers and Virtualization A Kernel Perspective*, 2019 s.1-2, doi:10.1007/978-1-4842-6283-2
[11] a.g.m., s.2.



Şekil 1.3 : NACA'da bulunan 1957 yılına ait IBM 704 ana bilgisayarı [12]

Veri merkezlerini, 1970'lerde ana bilgisayarlar yönetmeye başlamıştır. Bölümleme, kaynakların verimli paylaşımını sağlamış ve tüm bu işlemler, veri merkezindeki depodan alınan ve depolanan verilerle tek bir bilgisayarda gerçekleştirilmiştir. Veri merkezine erişim sıkı bir şekilde kontrol edilmiş; çoğu durumda, kullanıcılar bilgisayar operatörlerinden bir pencere veya yuva aracılığıyla raporlar almış; elektronik bilgilere, yerel işleme yetenekleri olmayan aptal terminallerle[13] erişmişlerdir. [14]

Bunu takiben 1980'lerde kişisel bilgisayarların masaüstü formunun bulunmasıyla dağıtık sistemler ortaya çıkmıştır. Bunlar, istemci ve sunucu yapılandırmalarına katılan aynı zamanda ana bilgisayarın daha küçük kuzeni olan minibilgisayarla bağlantılı olan istemcilerdir.[15]

Sonrasında, x86 donanımında birden çok programın çalışmasına izin veren UNIX gelmiştir. Ancak taşınabilirlik sorunu devam etmiştir. 1990'ların başlarında, Sun Microsystems Java'yı bulmuştur. Bu sayede bir kullanıcı, çeşitli donanım mimarilerinde çalışabilen bir program yazabilir hâle gelmiştir. Java bunu, daha sonra farklı donanım mimarilerinde yürütülmesini sağlamak için bayt kodu ile yapmış ve

[12]https://en.wikipedia.org/wiki/IBM_mainframe#/media/File:IBM_Electronic_Data_Processing_Machine_-_GPN-2000-001881.jpg Erişim Tarihi : 17 Eylül 2020
[13] Aptal terminaller, kendi işlem yeteğine sahip olmayan, tuş vuruşlarını toplayan ve verileri yeşil ekran metninde sunan ana bilgisayara bağlı basit cihazlardır.
[14] Thomas Olzak vd., 2010, s.1
[15] a.g.e., s.2

POSIX katmanını sanallaştırmıştır. [16] Açık sistemler olarak tabir edilen x86 sistemlerinin sanallaştırma dünyasına uyarlanma neticesinde, sanallaştırma kısa zamanda bilgi teknolojilerinin merkezi olmuştur. [17]

VMware ise 1990'ların sonunda devreye girmiştir. Bunu takiben Microsoft'un Hyper-V ürünü devreye girerek sanallaştırmada önemli bir yer elde etmiştir ve bunu Citrix'in XenServer ürünü izlemiştir. Bu ürünler işlemci, bellek, disk gibi gerçek donanımları sanallaştırarak, kendi sanallaştırma modelini başlatmıştır. Bu ürünler ile Hiper yönetici[18] olarak da adlandırılan VMware yazılımının üzerinde, konuk işletim sistemleri çalıştırabilir hâle gelmiştir. Bu, geliştiricilerin yalnızca Java programlarını çalıştırmakla sınırlı olmadığı, konuk işletim sisteminde çalıştırılması amaçlanan herhangi bir programı çalıştırabileceği anlamına gelmekteydi. Merkezi bilgi işlem ve sanal makine ilgisinin yerini, e-posta, veritabanı, web, uygulamalar gibi özel işlevlere sahip bağımsız sunucular almıştır.

2001 civarında, VMware ESX ve GSX sunucularını başlatmıştır. GSX, Tip 2[19] bir hiper yöneticiydi, bu nedenle konukları çalıştırmak için Windows gibi bir işletim sistemine ihtiyaç duydu. ESX ise, konuk işletim sistemlerinin doğrudan hiper yönetici üzerinde çalıştırılmasına izin veren bir Tip 1 hiper yönetici idi.[20] Vmware ESX Server'ı piyasaya sürdüğünden beri bu alanda bir öncü haline gelmiştir. Ancak günümüzde Microsoft, Intel, IBM, Amazon ve Cisco gibi birçok büyük teknoloji firmaları sanallaştırmaya daha iyi destek sağlamak için sanallaştırmanın birçok alanında büyük bir ilerleme kaydederek yeni teknolojilerini piyasaya sürmektedirler. Sanallaştırma yaklaşık yarım yüzyıldan uzun bir geçmişe sahiptir ve günümüze kadar gelen sanallaştırma teknolojisindeki gelişmeler sanallaştırmayı bir endüstri standardı haline getirmiştir. Sanal Masaüstleri gibi bazı teknolojiler 1960'lara kadar izlenebilirken, uygulama sanallaştırma gibi teknolojiler ise yalnızca birkaç yıl öncesine kadar izlenebilir. [21]

[16] Jain, *Linux Containers and Virtualization A Kernel Perspective*, s.2
[17] T. Merdan, 2010, s.4
[18] Hiper yönetici: Sanal makineleri oluşturan ve çalıştıran bilgisayar yazılımı veya donanımıdır.
[19] Tip1 ve Tip2 hiper yöneticiler sayfa 13'de anlatılmıştır.
[20] S. M. Jain, 2019, s.2.
[21] T. Merdan, 2010, s.4

Sanallaştırma teknolojilerinin zaman içerisindeki ilerlemesi incelendiğinde, ilk etapta donanım kaynaklarının paylaşılması ve kaynakların daha verimli kullanılması, ikinci etapta masaüstü bilgisayarların sanallaştırılması, uygulamalara uzaktan erişimi kolaylaştırması ve uygulamaların başlangıçta amaçlanandan daha fazla sistemde çalışmasının sağlanması, yüksek kullanılabilirliğin sağlanması ve felaket kurtarma senaryosunun olması, üçüncü etapta ise kurallara bağlı olarak çalışması ve kendini yönetebilmesi ön plana çıkmaktadır.[22]

1.1.2. Sanallaştırmanın Çalışma Mantığı

Sanal makine, fiziksel bir bilgisayarın sanal bir temsilidir; genellikle "konuk" olarak adlandırılır ve çalıştırdıkları fiziksel makineye "ana bilgisayar" denir. Sanallaştırma, tek bir fiziksel makinede her biri kendi işletim sistemi (OS) ve uygulamaları olan birden çok sanal makine oluşturmayı mümkün kılar. Bir sanal makine, fiziksel bir bilgisayarla doğrudan etkileşim kuramaz, kendisiyle temeldeki fiziksel donanım arasında koordinasyon sağlamak için hiper yönetici adı verilen ince bir yazılım katmanına ihtiyaç duyar. [23]

Hiper yönetici, her bir sanal makineye (VM)[24] işlemciler, bellek ve depolama gibi fiziksel bilgi işlem kaynaklarını tahsis eder. Her bir sanal makineyi diğerlerinden ayrı tutar, böylece birbirleriyle etkileşime giremezler.

Hiper yönetici fiziksel bir bilgisayarda veya sunucuda kullanıldığında, fiziksel bilgisayarın işletim sistemini ve uygulamalarını donanımından ayırmasına izin verir. Ardından, kendisini birkaç bağımsız sanal makineye bölebilir. Bu yeni sanal makinelerin her biri, daha sonra kendi işletim sistemlerini ve uygulamalarını bağımsız olarak çalıştırabilirken, bellek, RAM, depolama gibi orijinal kaynakları hiper yöneticinin yönettiği tip 1 hiper yönetici, sunucudan paylaşmaya devam edebilir.[25]

---

[22] T. Merdan, 2010, s.4
[23] https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor Erişim Tarihi : 26 Aralık 2020
[24] Virtual Machine: bu tezde sanal makine da ya VM olarak bahsedilecektir.
[25] https://www.ibm.com/cloud/learn/virtual-machines#toc-how-virtua--B5v9urC, Erişim Tarihi: 28 Kasım 2020

1.1.3. Sanallaştırmanın Hedefleri

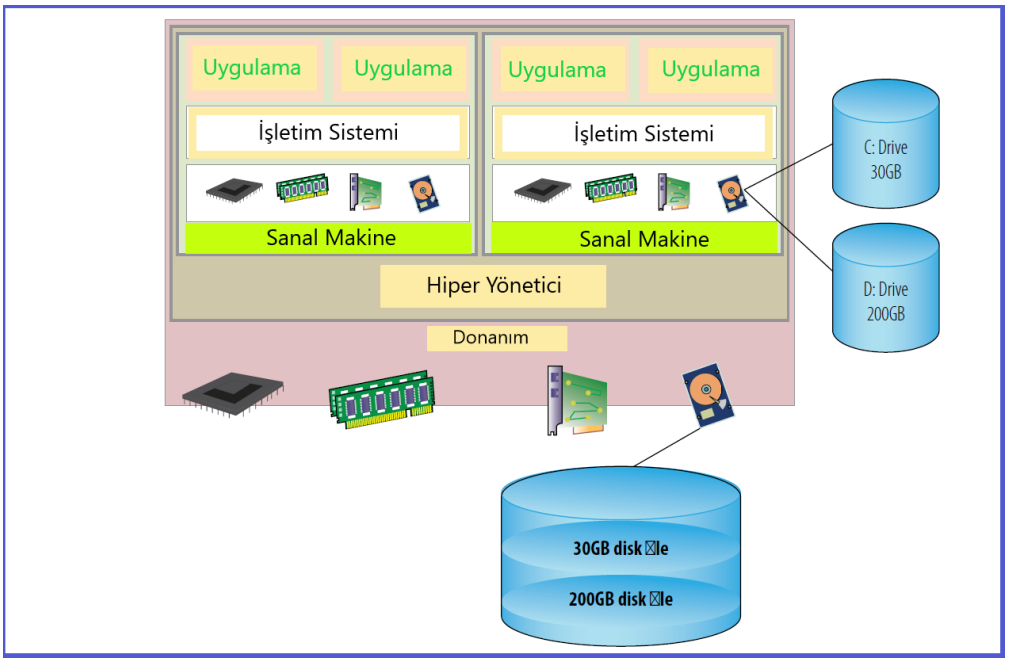
Kuruluşlar, sanallaştırma teknolojisini kullanırken genellikle farklı şeyler ararlar. Bunlar:

- Herhangi bir ağ özellikli cihazın herhangi bir ağ üzerinden erişilebilen uygulamaya erişmesine izin verilmesi,
- Ortamın güvenliğini veya yönetilebilirliğini artırmak için bir iş yükünün veya uygulamanın diğerinden yalıtılması,
- Bir uygulamanın işletim sisteminden ayrılması ve bir uygulamanın işletim sisteminin farklı bir sürümü için tasarlanmış olmasına rağmen çalışmaya devam etmesine izin vermesi,
- Bir uygulamanın yabancı bir işletim sisteminde çalışmasına izin vererek işletim sisteminden izole edilmesini sağlaması[26],
- Birden çok örneğin aynı anda farklı makinelerde çalışmasına izin vererek bir uygulamanın destekleyebileceği kişi sayısını arttırması,
- Verileri veya uygulamanın kendisini segmentlere ayırarak ve işi birçok sisteme yayarak bir uygulamanın çalışması için gereken süreyi azaltması,
- Tek bir sistemin kullanımını optimize ederek daha çok ve daha akıllıca çalışmasını sağlaması,
- Yedeklilik yoluyla bir uygulamanın veya iş yükünün güvenilirliğini veya kullanılabilirliğini arttırması (herhangi bir bileşen başarısız olursa, bu sanallaştırma teknolojisi, uygulamayı ayakta kalan bir sisteme taşır veya ayakta kalan bir sistemdeki bir işlevi yeniden başlatır).[27]

[26] Dan Kusnetzky, *Virtualization: A Manager's Guide*, O'relly, 2011, s.6
[27] a.g.e, s.6-7.

1.2. HİPER YÖNETİCİLER

Hiper yönetici, fiziksel bilgisayarda çalışan sanal makineleri koordine eden ve yöneten ana bilgisayar yazılım katmanı olarak adlandırılır. Bu katman sanal makine ile fiziksel donanım arasında bir ara yüz görevi görerek, sanal makinenin fiziksel kaynaklara erişmesini sağlar ve aynı fiziksel donanım üzerine kurulmuş sanal makinelerin birbirine müdahale etmesini engeller.[28] Bir hiper yönetici, donanım için bir tür işletim sistemi görevi görür ancak uygulama veya program talepleriyle uğraşmak yerine, tüm sanal sunuculara hizmet verir. Şekil 1.4'te, bir I/O işlemi gösterilmiştir. Şekilde, konuk bir uygulama, bir diskin okunmasını talep eder ve bu isteği konuk işletim sistemine iletir. Konuk işletim sistemi, şekilde C: veya D: sürücüsü olarak gösterilen diskte bir okuma yapar. Burada, hiper yönetici devreye girerek bu bilgiyi depolama alt sistemine geçirir ve gerçek dünyadaki fiziksel eşdeğerine çevirir.[29]



Şekil 1.4 : Konuk I/O işleme [30]

[28] Russell David Monckton, "*Incremental And Differential Backups Of Vırtual Machine Files*", Jan. 17, 2012 ,US Patent O080993.91B1
[29] Matthew Portnoy, *Virtualization Essentials*, Indiana, Sybex, 2016, s.27
[30] a.g.e., s.27

Şekil 1.4'teki veriler aslında paylaşılan depolama dizisinde bulunur ve hiper yönetici bu isteği uygun depolama cihazına ve dosya sistemine iletir. Yanıt geri döndüğünde, hiper yönetici, verileri doğrudan fiziksel aygıttan geliyormuş gibi alan konuk işletim sistemine geri iletir. Hiper yönetici yalnızca konuktan gelen tüm depolama I/O isteklerini, aynı zamanda ağ, bellek işleme ve CPU isteklerini işler. Bu işlemleri, hiper yöneticinin çalıştığı fiziksel sunucuda barındırılan tüm misafirler için yapar.[31]

Hiper yöneticiler, talep edilen tüm kaynaklara makul bir şekilde hizmet verilmesini sağlayan bir kaynak planlama sürecine sahiptir. Bazı hiper yöneticilerin konuklara öncelik verme seçenekleri vardır, böylece önemli uygulamalara öncelik tanınabilir ve çekişme nedeniyle performans düşüşü yaşanmaz.[32]

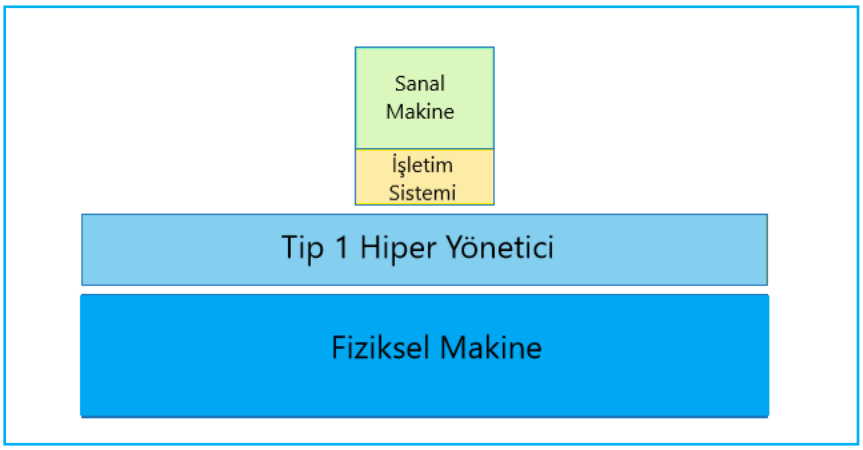
Sanal makine ana bilgisayar işletim sisteminin mevcut olup olmadığına bağlı olarak tip 1 veya tip 2 hiper yöneticiler olarak kategorize edilir. Ancak tip 1 ve tip 2 hiper yöneticilerin net veya standart bir tanımı yoktur. Hiper yönetici doğrudan donanımın üzerinde çalışıyorsa (bare-hardware), genellikle tip 1 hiper yönetici olarak kabul edilir. Bir işletim sistemi varsa ve hiper yönetici ayrı bir katman olarak çalışıyorsa, tip 2 hiper yönetici olarak kabul edilir.[33]

1.2.1. Tip 1 Hiper Yönetici

Bu hiper yöneticiler doğrudan fiziksel sunucunun üzerine kurulurlar ve temeldeki fiziksel kaynaklarla etkileşime girerek geleneksel işletim sistemini tamamen değiştirirler. Tip 1 hiper yöneticiler temel olarak, donanımı kontrol eden, kaynak planlamasını yöneten ve konuğu izleyen bir işletim sistemidir.[34] Bir aracı olmadan, tip 1 hiper yönetici, altındaki donanım kaynakları ile doğrudan iletişim kurabilir ve bu da

[31] M. Portnoy, 2016, s.28
[32] Prabhakar Chaganti, *Xen Virtualization: A fast and practical guide to supporting multiple operating systems with the Xen hypervisor*, Packt Publishing, 2007, s.7
[33] Humble Devassy Chirammal vd., *Mastering KVM Virtualization*, Birmingham, Packt Publishing, 2016, s.14
[34] Diane Barrett ve Gregory Kipper, *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments*, Burlington ,Syngress, 2010, s.10

onu tip 2 hiper yöneticiden çok daha verimli hale getirir. Şekil 1.5'te tip 1 hiper yönetici gösterilmiştir.[35]



Şekil 1.5 : Tip 1 hiper yönetici[36]

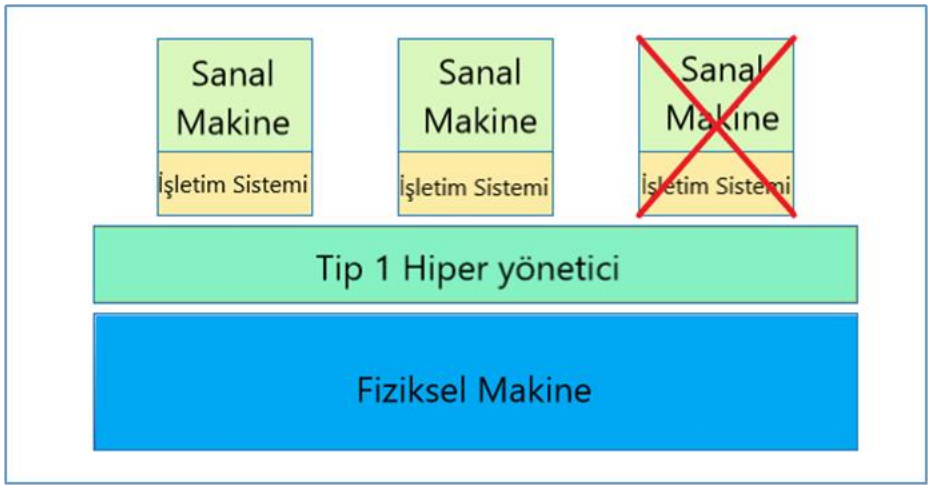
Tip 1 hiper yöneticilerin avantajları şunlardır:

- Kurulumu ve yapılandırması tip 2 hiper yöneticilere göre kolaydır.
- Fiziksel kaynakların çoğunu sanal makinelere verecek şekilde optimize edildiğinden küçük boyutludur.
- Yalnızca sanal makineleri çalıştırmak için gereken uygulamalarla birlikte çalıştığı için daha az ek yük oluşturur.
- Konuk sistemindeki sorunlar hiper yönetici üzerinde çalışan diğer konuk sistemleri etkilemediği için daha güvenlidir.

Ancak tip 1 hiper yönetici özelleştirmeyi desteklemez. Genel olarak, üzerine her hangi bir üçüncü taraf uygulama veya sürücü yüklenmesine izin vermez.[37] Daha iyi performans özelliklerine sahip olmanın yanı sıra, tip 1 hiper yöneticilerin ayrıca tip 2 hiper yöneticilerden daha güvenli olduğu kabul edilir. Konuk işlemleri devredilir ve bu nedenle bir konuk, desteklendiği hiper yöneticiyi etkileyemez. Bir sanal makine bir felaket senaryosunda yalnızca kendisine zarar vererek tek bir konuk çökmesine neden olabilir, ancak bu olay sanal makinenin sınırlarının dışına çıkmaz. Diğer konuklar

[35] M. Portnoy, 2016, s.23
[36] a.g.e., s.24
[37] H. D. Chirammal vd., 2016, s.15

çalışmaya devam eder ve hiper yönetici de bu durumdan etkilenmez. Kasıtlı olarak hiper yöneticiye veya diğer konuklara müdahale etmeye çalışan kötü niyetli bir konuk bu isteğini gerçekleştiremez. Şekil 1.6'da tip 1 hiper yöneticideki bir konuk hatası gösterilmiştir.[38]

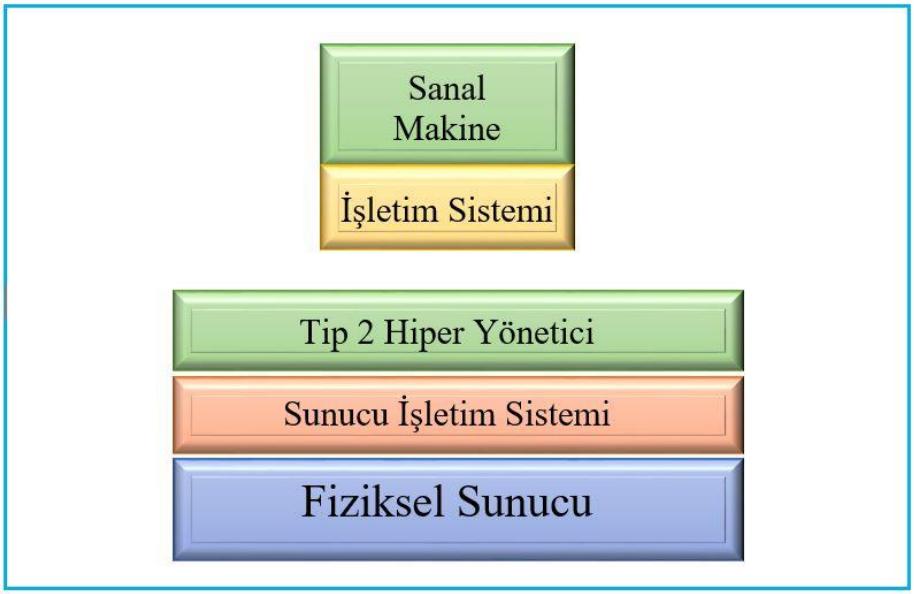


Şekil 1.6 : Hiper yöneticideki bir konuk hatası[39]

1.2.2. Tip 2 Hiper Yönetici

Tip 2 hiper yöneticiler, mevcut bir işletim sistemi üzerinde bir uygulama olarak çalışır ve çok sayıda özelleştirme yapılmasına izin verir. Tip 2 hiper yöneticiler, işlemleri için ana bilgisayar işletim sistemine bağlıdır. Bu modelin en önemli yararı, temeldeki ana bilgisayar işletim sistemi donanım erişimini kontrol ederek geniş bir donanım yelpazesini destekleyebilmesidir. Ağ oluşturma ve depolama gibi donanım yapılandırma işlerinin çoğu işletim sistemi tarafından kapsanmış olduğundan, Tip 2 hiper yöneticilerin kurulumu ve dağıtımı genellikle kolaydır.[40] Şekil 1.7'de Tip 2 hiper yönetici gösterilmiştir.

[38] Onur Milli, "Server Virtualization For Enterprises and an Application", Yayınlanmış Yüksek Lisans Tezi, Başkent Üniversitesi,2016,s.13
[39] a.g.m., s.23
[40] H. D. Chirammal vd., 2016, s.15



Şekil 1.7 : Tip 2 hiper yönetici [41]

Tip 2 hiper yöneticiler, hiper yönetici ile donanım arasındaki bu ekstra katman nedeniyle tip 1 hiper yöneticiler kadar verimli değildir. Konuk sanal makineler, barındırılan işletim sistemine kritik olarak bağımlıdır ve bu işletim sisteminin sorunları tüm konuk makineleri etkiler.[42] Sanal makine bir disk okuma, bir ağ işlemi veya başka bir donanım etkileşimi gerçekleştirdiğinde, bu isteği tıpkı tip 1 hiper yönetici ortamında olduğu gibi hiper yöneticiye iletir; bunun aksine, tip 2 hiper yönetici daha sonra bu isteği I/O taleplerini işleyen işletim sistemine teslim etmelidir. İşletim sistemi; bilgileri önce hiper yöneticiye, ardından konuğa geri gönderir ve her işlem için iki ek adım, fazladan zaman ve daha fazla ek işlem yükü ekler. Tip 2 hiper yöneticiler daha az güvenilirdir çünkü temeldeki işletim sisteminin kullanılabilirliğini etkileyen herhangi bir şey, hiper yöneticiyi ve desteklediği konukları da etkileyebilir.[43] Örneğin, sistemin yeniden başlatılmasını gerektiren standart işletim sistemi yamaları, ana bilgisayardaki tüm sanal makinelerin yeniden başlatılmasını da zorunlu kılar.[44]

[41] M. Portnoy, 2016, s.25
[42] Radek Silhavy, Petr, Prokopova, Zdenka Silhavy, *Software Engineering Perspectives and Application in Intelligent Systems*, Advances in Intelligent Systems and Computing 465, Springer International Publishing, Switzerland, 2016, s.242-245
[43] Jiri Vojtesek, Martin Pipis, *Virtualization of Operating System Using Type-2 Hypervisor*. Software Engineering Perspectives and Application in Intelligent Systems, 2016, s.239–247. doi:10.1007/978-3-319-33622-0_22
[44] M. Portnoy, 2016, s.23

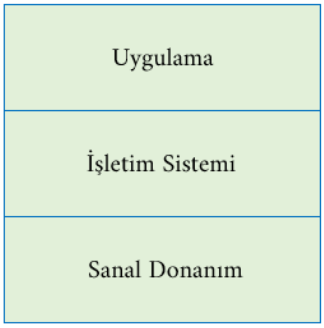
1.3. SANAL MAKİNE

Sanal makineler, sanallaştırmanın temel bileşenleridir. Sanal makineler fiziksel bir sunucudaki bir hiper yönetici üzerinde çalışan geleneksel işletim sistemleri ve uygulamalar için konteynerler olarak tanımlanır.[45]

1.3.1. Sanal Makine Kavramı

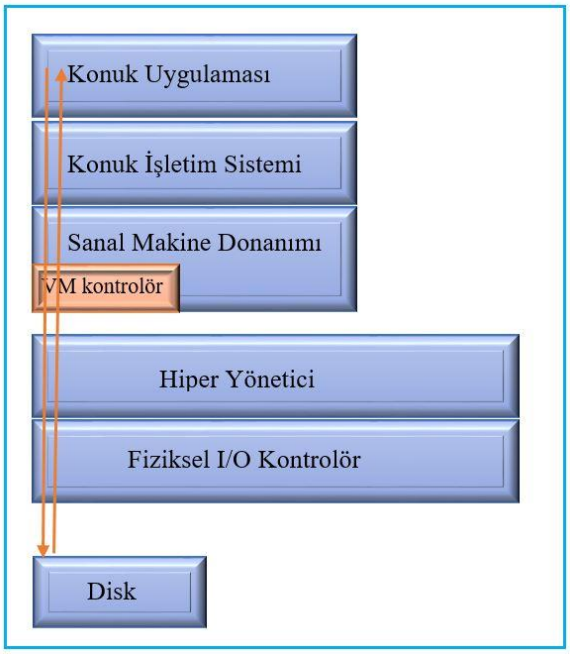
Bir sanal makine, fiziksel bir sunucunun sahip olduğu özelliklerin çoğuna sahiptir. Gerçek bir sunucu gibi işletim sistemini destekler ve üzerinde çalışan uygulamaların erişim talep edebileceği bir dizi kaynak ile yapılandırılır. Herhangi bir zamanda yalnızca bir işletim sisteminin ve genellikle birkaç uygulamanın çalıştığı fiziksel bir sunucunun aksine tek bir fiziksel sunucu içinde çalışabilir ve çok sayıda programı paralel olarak çalıştırabilir. Sanal makine bilgi işlem sisteminin organizasyonunu esnek bir şekilde değiştirebilir.[46] Fiziksel bir sunucunun aksine, bir sanal makine gerçekte sanal sunucuyu tanımlayan ve içeren bir dizi dosyadır. Bir sanal makineyi oluşturan ana dosyalar, konfigürasyon ve sanal disk dosyalarıdır. Konfigürasyon dosyası, sanal makinenin kullanabileceği kaynakları belirler ve sanal makineyi oluşturan sanal donanımı numaralandırır. Bir sanal makine boş bir sunucu olarak düşünülürse, konfigürasyon dosyası o sunucuda CPU, bellek, depolama, ağ, CD sürücüsü gibi hangi donanım cihazlarının olacağını listeler. Şekil 1.8, sanal donanım, işletim sistemleri ve uygulamalardan oluşan bir sanal makinenin basitleştirilmiş bir gösterimidir.[47]

[45] Cansu Gökhan, *Scalability Issues In Big Data On Cloud: A Comparison of Virtual Machines and Linux Containers*, Yüksek LisansTezi, 2017, Atılım Üniversitesi, s.31
[46] Saburo Kaneda, Naomi Matsumura, Fujio Ikegami, Kazuyuki Shimizu, Yukichi Ikuta, "Virtual Machine System", Feb. 20, 1980, US Patent 4,400,769
[47] O. Milli, 2016, s.16



Şekil 1.8 : Sanal makinenin basitleştirilmiş gösterimi

Hiper yönetici, desteklediği sanal konuklara giden ve gelen kaynakların taşıyıcısı ve düzenleyicisidir. Bu yeteneği, konuk işletim sistemini hiper yöneticinin aslında bir donanım olduğuna inandırarak gerçekleştirir.[48] Şekil 1.9'da bir işletim sisteminin sanallaştırma ana bilgisayarındaki donanımı nasıl yönettiğini açıklamaya yardımcı olacaktır.



Şekil 1.9 : Sanal ortamda basitleştirilmiş bir veri talebi[49]

Bir program diskteki bir dosyadan bazı verilere ihtiyaç duyduğunda, (C'deki fgets () gibi bir program dili komutuyla) istekte bulunur ve bu istek de işletim sistemine

[48] M. Portnoy, 2016, s.46
[49] a.g.m., s.47

iletilir. İşletim sistemi, kendisine erişilebilen dosya sistemi bilgilerine sahiptir ve isteği, daha sonra uygun verileri almak için fiziksel disk I/O denetleyicisi ve depolama aygıtıyla birlikte çalışan doğru aygıt yöneticisine iletir. Veriler, işletim sisteminin verileri talep eden programa döndürdüğü I/O denetleyicisi ve aygıt sürücüsü aracılığıyla geri gelir. Yalnızca veri blokları talep edilmekle kalmaz, aynı zamanda bellek bloğu transferleri, CPU zamanlaması ve ağ kaynakları da talep edilir. Ayrıca diğer programlar da ek taleplerde bulunur. Tüm bu bağlantıların doğru şekilde yapılması işletim sistemine ve hiper yöneticiye bağlıdır.[50]

1.3.2. Sanal Makine Çalışma Prensibi

Sanal makineler, sanal makinelerin konfigürasyonunu oluşturan dosyalar ve başlatıldıktan sonra çalışan bir sanal makineyi oluşturan bellekteki örnekleme olmak üzere iki fiziksel varlık olarak bulunur. Birçok yönden, bir sanal makineyle çalışmak, gerçek bir fiziksel sunucuyla çalışmaya çok benzer. Fiziksel bir sunucu gibi, ortamı veya sunucunun desteklediği çeşitli uygulamaları yüklemek, yönetmek ve izlemek için bir tür ağ bağlantısı aracılığıyla onunla etkileşim kurulabilir. Ayrıca fiziksel bir sunucu gibi, donanım yapılandırması değiştirilebilir, yetenek ve kapasite eklenebilir veya çıkarılabilir. Ancak bunu yapma yöntemleri ve bunu yapma esnekliği fiziksel sunucu ile sanal sunucu arasında çok farklıdır.[51]

Sanal sunucu kaynakları, bir VM kullanılarak yönetilebilir. Sunucu kaynaklarının sanallaştırılması faydalar sağlarken, VM kullanımı aynı zamanda karmaşıklıklar ve zorluklar da getirir.[52] Sanallaştırma teknolojilerini anlamak için öncelikle klonlar (clone), şablonlar (template), anlık görüntüler (snapshot) ve açık sanallaştırma formatı (OVF) gibi kavramları açıklamak faydalı olacaktır.

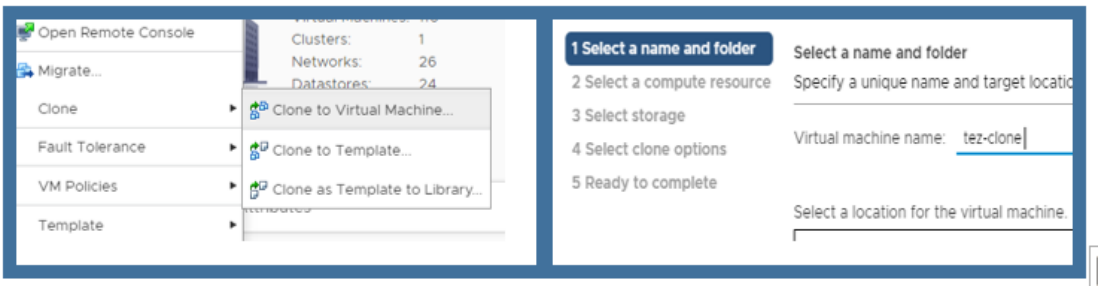
1.3.3. Sanal Sunucunun Klonlanması

Bir fiziksel sunucuyu temin etmek için insan gücü, zaman ve maddiyat açısından önemli kaynaklara ihtiyaç vardır. Sunucu sanallaştırmadan önce, fiziksel bir

[50] O. Milli, 2016, s.16
[51] M. Portnoy, 2016, s.47
[52] Alexey Vasilyev & Alexander Baranov, *Virtual Machine Backup From Storage Snapshot*, Veeam Software AG, Baar (CH), 25Ağustos 2015, US Patent 9116846B2 , s. 1.

sunucuyu istekte bulunma ve temin etme süreci haftalar hatta aylar sürebilir ve bu genellikle fazla maliyet gerektiren bir durumdur. Sunucu fiziksel olarak temin edildiğinde, bu süreye ek olarak sunucuyu sisteme hazırlama süresi de gerekir. Bir sistem yöneticisinin, bir işletim sistemini ve işletim sisteminin güncel olması için gerekli olan yamaları yükleme, ek depolama yapılandırması yapma, sunucuyu ağ altyapısına bağlama, kurum tarafından karar verilen kurumsal araçları ve uygulamaları yükleme gibi geniş bir iş listesi gerçekleştirmesi gerekir. Süreç bununla da bitmez. Sunucu kuruluktan sonra sunucu üzerinde çalıştırılacak gerçek uygulamayı kurmak saatler hatta günler sürebilir.

Bu süreç sanal bir makinede ise oldukça kısadır. Yeni bir sunucu ihtiyacı doğarsa, Şekil 1.10'da gösterildiği gibi birkaç adımda kolay bir şekilde mevcut olan sunucu klonlanabilir. Klonlama süreci, mevcut sunucuyu oluşturan dosyaların kopyalanması dışında birkaç işlem de gerektirir. Klonlama işlemi yapıldıktan sonra konuk işletim sistemi, sistem adı ve IP adresi gibi benzersiz sistem bilgileri biçiminde bazı özelleştirmelere ihtiyaç duyar. Bu değişiklikler yapılmazsa, aynı kimliğe sahip iki VM, aynı ağı ve uygulama alanını çalıştırır bu da birçok düzeyde hasara yol açar. [53]



Şekil 1.10 : Sanal makine klonlama ve özel sistem adı belirleme

Klonu oluşturmak yalnızca birkaç dakika sürebilirken, dosyaların kopyasını ve konuk özelleştirmesini gerçekleştirmek biraz zaman alır. Bir dizi faktöre bağlı olarak, dakikalar hatta saatler sürebilir. Ancak, bu süreci edinmesi ve kurması haftalarca veya daha uzun süren fiziksel bir sunucunun sağlanmasıyla karşılaştırırsak, sanal bir

[53] M. Portnoy, 2016, s.48

makinenin hızlı ve kolay şekilde klonlanabilir olması, iş yükü, zaman ve maliyet açısından kazanımlar sağlar.[54]

1.3.4. Sanal Makinede Şablon Oluşturmak

Klonlara benzer şekilde, sanal makine şablonları, tam olarak yapılandırılmış sanal sunucuları hızla sunmak için başka bir mekanizmadır. Şablon, yaygın olarak kullanılan bir sunucunun önceden yapılandırılmış ve yüklenmiş bir sanal makine kalıbıdır. Bir şablon ile bir klon arasındaki fark, klonun çalışıyor olmasıdır. Çoğu ortamda, bir şablon çalışamaz ve üzerinde değişiklik yapmak için önce sanal makineye dönüştürülmesi gerekir. Daha sonra sanal makine başlatılır, gerekli yamalar uygulanır, sanal makine kapatılır ve ardından sanal makine tekrar şablona dönüştürülür. Klonlama gibi, bir şablondan bir VM oluşturmak, yeni oluşturulan sanal makineye uygulanacak benzersiz bir kimlik gerektirir. Klonlamada olduğu gibi, bir şablondan sanal bir makine oluşturma zamanı, yeni bir fiziksel sunucu oluşturmak ve sağlamaktan daha hızlıdır.[55]

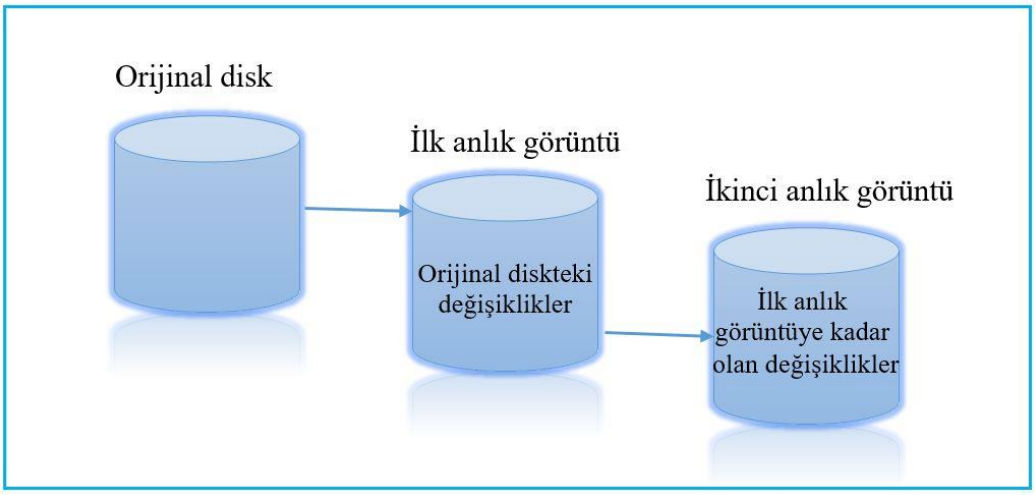
1.3.5. Sanal Makinelerde Anlık Görüntü Almak

Anlık görüntü bir sanal makinenin belirli bir zamandaki durumunun anlık olarak yakalanmasıdır.[56] Sanal makinede yapılan bazı değişikliklerin bir soruna neden olması durumunda makinenin kolayca eski haline geri dönmesini sağlar. Genel olarak anlık görüntüler çok hızlı bir şekilde oluşturulabilir. Çünkü anlık görüntü, verilerin gerçek bir kopyası yerine sanal bir kopyasını temsil eder.[57] Anlık görüntü, bir sanal makinenin durumunu, verilerini ve donanım yapılandırmasını korur. Bir sanal makinenin anlık görüntüsü alındığında, yapılan değişiklikler sanal makinede gerçekleşmez sadece anlık görüntü üzerinde olur. Anlık görüntü alt disk adı verilen bir delta diske gider. Bu delta disk, başka bir anlık görüntü veya bir konsolidasyon olana kadar tüm değişiklikleri saklar ve anlık görüntü sürecini sonlandırır. Başka bir anlık görüntü alınırsa, ikinci bir delta diski oluşturulur ve sonraki tüm değişiklikler oraya

[54] M. Portnoy, 2016, s.48
[55] a.g.e, s.49
[56] Robert Fries vd., *Virtual Machine Anlık görüntüting And Analysis, Microsoft Technology Licensing*, LLC, 2011, US Patent US 2016/9,286,182 B2
[57] Kedar Patwardhan , Kiran Dudala , *Systems and Methods for Snapshot - Less Backups*, 16 Haziran 2020, US Patent US 2020/0019466 A1

yazılır. Bir konsolidasyon yapılırsa, delta disk değişiklikleri temel sanal makine dosyalarıyla birleştirilir ve güncellenmiş VM haline gelir.[58]

Anlık görüntü alındığı andaki sanal makinenin durumuna geri dönülebilir ve o zamandan beri yapılan tüm değişiklikler silinir. Anlık görüntüler, test ve geliştirme alanlarında çok yararlıdır. Anlık görüntü ile ortamlar sağlıklı bir duruma geri yüklenebilir. Bu sayede riskli veya bilinmeyen süreçlerin denenmesine olanak tanır. Anlık görüntüler, sonucun emin olmadığı bir yamayı veya güncellemeyi test etmek için kullanılabilir ve uygulanan bir işlemi geri almanın kolay bir yolunu sağlar. [59] Şekil 1.11, anlık görüntülerin nasıl çalıştığına dair temel bir gösterimdir.



Şekil 1.11 : Anlık görüntü disk zinciri[60]

Kullanıcı hatasını düzeltmek, sabit disk arızası gibi donanım arızasından kaynaklanan veri kaybını önlemek, uygulama veya işletim sistemi çökmeleri gibi yazılım hatalarını kurtarmak içinse yedekleme yöntemi kullanılabilir. Bir çökmeden sonra kurtarmanın amacı, tüm sistem için bilinen son iyi çalışma durumunu geri yüklemektir. Bu, dosya sistemini uygun bir yedeklemeden geri yükledikten sonra aynı donanımı yeniden başlatarak yapılabilir, ancak tüm dosya sisteminin geri yüklenmesi gerekiyorsa kurtarma prosedürü çok zaman alabilir. Bu nedenle, sanal makinelerde anlık görüntü bazen kısa zaman için yedekleme amacıyla kullanılmaktadır. Bir sanal

[58] M. Portnoy, 2016, s. 50-51
[59] Cheng Li , Li Ding , Bret Needle , Foster City , Mayank Rawat , *System And Method For Checking And Characterizing Snapshor Metadata Using Snapshot Metadata Database*,17 Kasım 2016, US Patent US010802927B2
[60] M. Portnoy, 2016, s.51

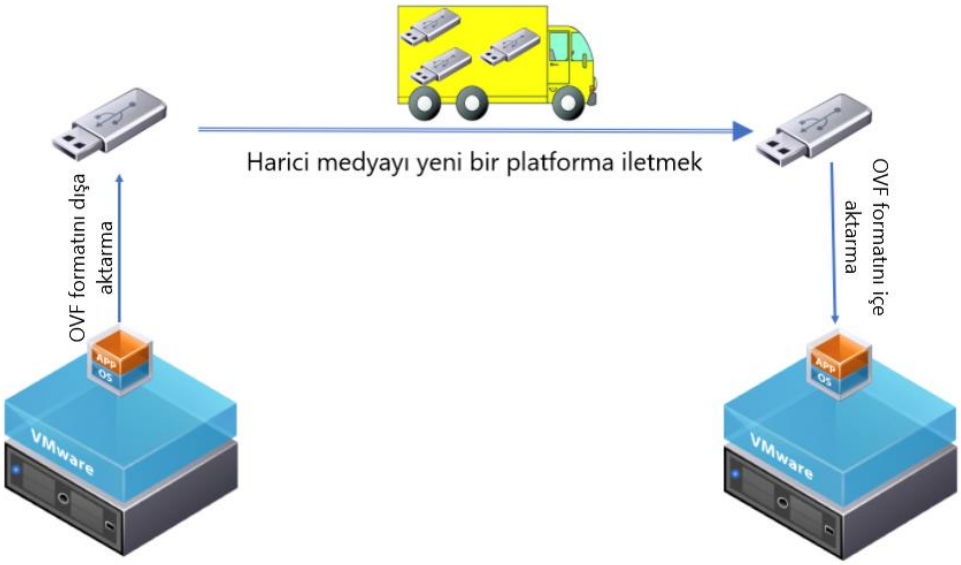
makineyi yedek olarak kullanmak, kaynak makine arızalanırsa, sanal makinenin yerine hızla çalıştırılabilmesi açısından faydalıdır. Geleneksel yedekleme yöntemleriyle, tam sistem geri yüklemesi saatler sürebilirken, sanal makine birkaç dakika içinde açılıp çalışmaya başlayabilir.[61]

Yedekleme amacıyla sanal makine görüntüsünün tam bir kopyasını oluşturmak için kullanılabilir olsa da gerçek yedeklemelerin yerini asla tutmamaktadır. Bir sanal makineye birden fazla anlık görüntünün uygulanması bir test ortamı için iyidir ancak VM'nin ve ilişkili ana bilgisayarın bilgi işlem kaynaklarının performansını azaltır. Ancak ister geleneksel dosya sistemi yedeklemeleri ister yedekleme olarak VMS[62] kullanılsın, son yedekleme işleminden bu yana yapılan değişiklikler kaybolur. [63]

1.3.6. Açık Sanallaştırma Formatı (OVF)

Sanal makineleri paketlemenin ve dağıtmanın bir başka yolu da OVF kullanmaktır. OVF, sanal makinelerin paketlenmesi ve dağıtımı için bir format tanımlayan, platformdan bağımsız bir endüstri standardıdır. Bu standardın amacı, sanal makineleri bir platformdan başka bir platforma kolayca taşınabilen bir dosyada bir araya getirmek için platformdan bağımsız bir format oluşturmaktır. Çoğu sanallaştırma üreticisi, sanal makineleri OVF formatına dışa aktarma seçeneklerinin yanı sıra OVF formatlı VM'leri kendi formatlarına içe aktarma yeteneğine sahiptir. Bu Şekil 1.12'de gösterilmiştir.

[61] Aleksey Pershin, Ilia Langouev, Sudarsana R. Piduri, Parag Ratankumar Shah, Joshua M. Silver, *Managing Backups Using Virtual Machines*,11 Ekim 2011, US Patent 8037032B2 s.1
[62] VMS : Virtual Memory Sistem : Sanal bellek sistemi olarak bilinen VMS, büyük orta sınıf bilgisayarlarda çalışan dijital ekipman işletim sistemidir.
[63] A. Vasilyev, A. Baranov, 2015, s.2.



Şekil 1.12 : OVF dışa ve içeri aktarma[64]

OVF standardı, sanal makinelerin paketlenmesi için iki farklı yöntemi destekler. OVF şablonu, sanal makineyi temsil eden bir dizi dosya oluşturur ve ayrıca tüm bilgileri tek bir dosyada toplayacak ikinci bir formatı, Open Virtual Appliance(OVA) formatını destekler. Aslında standart, bir OVF paketi, TAR (Tape Archive) formatı kullanılarak tek bir dosya olarak saklanabilir. Bu dosyanın uzantısı ".ova" olacaktır. [65]

OVF'in faydaları:

- Sanal Makine verileri, veri miktarını en aza indirmek için dışa aktarma sırasında sıkıştırılır.
- Tek seferde büyük miktarda veriyi taşıma yeteneği vardır.
- Kaynak ve hedef siteler arasında ağ bağlantısı olmadığında veya güvenlik politikaları ortamlar arasında trafiğe izin vermediğinde taşıma yapılabilir.

[64] https://www.starwindsoftware.com/blog/virtual-workload-migration-with-vmware Erişim tarihi: 24.03.2021
[65] O. Milli, 2016, s.15-31.

OVF'in zararları:

- Hedef alana fiziksel olarak teslim edilene kadar veriler ortaya çıkarılamayacağından sanal makineler için daha uzun kapalı kalma süresi oluşur.

- Göç sırasında hırsızlık ihtimalinden dolayı veri ihlali riski vardır.

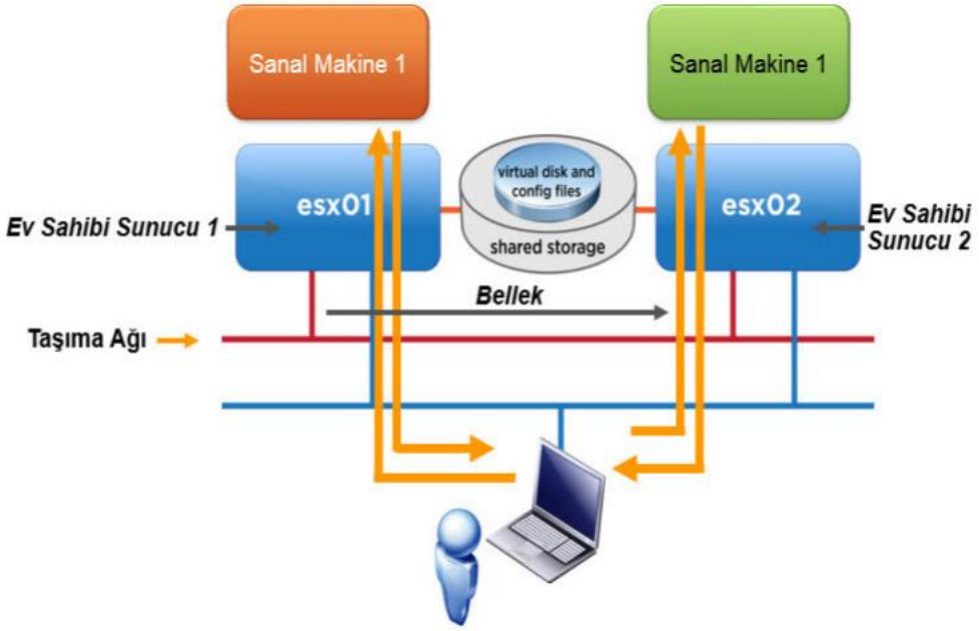
Sunucular hassas bilgiler içeriyorsa, dışa aktarılan VM'leri şifrelenmiş depolama alanına kopyalaması yapılabilir.

1.3.7. Sanal Makinelerin Taşınması

Bir host sunucusu donanımsal bir değişiklik, yazılımsal bir yükseltme veya yazılımsal bir konfigürasyon değişikliği gibi işlemler neticesinde yeniden başlatılmaya ihtiyaç duyabilir. Bu gibi durumlarda sanal sunucular çalışır durumdayken herhangi bir servis veya uygulama durdurulmadan başka bir host sunucusu üzerine taşınabilmektedir. Bu özellik sayesinde bilgi işlem altyapıları daha esnek bir hale gelmektedir.

Sanal makinelerin taşınması sırasında, ilk başta sanal makinenin RAM'i kaynak host sunucudan hedef host sunucuya kopyalanır. Kopyalanma işleminin ardından sanal makine, kaynak host sunucu üzerinde sahip olduğu tüm donanımsal ve yazılımsal konfigürasyonları hedef host sunucudan talep eder. Bu süreçte hedef host sunucu bu kaynakları karşılamak için uygun ise sanal makine hedef hosta taşınır ve artık bu fiziksel sunucu üzerinde çalışmaya devam eder.[66] Şekil 1.13'te sanal makine taşınması işlemi gösterilmektedir.

[66] Ersin Büyükyılmaz, *Sunucu Sanallaştırma Teknolojili Veri Merkezi Ve Bir Uygulaması*, Yüksek Lisans Tezi, 2016, s.24-25



Şekil 1.13 : Sanal makinenin taşınması[67]

1.3.8. Sanal Makinenin Güvenliği

Bir sanallaştırma ortamında, hiper yönetici, bir sanal makineyi yürütme sırasında herhangi bir noktada askıya alabilir; CPU durumlarının, belleğinin ve diskinin anlık görüntüsünü alabilir ve konuk sanal makinenin farkında olmadan anlık görüntüyü daha sonra devam ettirebilir. Bu özellik, hata toleransı ve VM bakımı gibi yararlı işlevleri destekler ve yaygın olarak kullanılmaktadır. Ne yazık ki, kötü niyetli saldırganlar tarafından VM geri alma saldırısı başlatmak için de kullanılabilir.[68]

Bir sanal makine geri alma saldırısında, güvenliği ihlal edilmiş bir hiper yönetici, kullanıcının farkında olmadan eski bir anlık görüntüden sanal makineyi çalıştırabilir. Burada kullanıcı, bulut hizmetini kullanan konuk sanal makinelerin sahibidir. Sanal makinenin yürütme geçmişinin bir kısmı kaybolduğundan, bir saldırgan sanal makinedeki bazı güvenlik kontrollerini atlayabilir veya güvenlik açısından kritik bazı güncellemeleri geri alabilir. Örneğin, bir saldırgan bir sanal

[67] E. Büyükyılmaz, s.25
[68] Yubin Xia, Yutao Liu, Haibo Chen, Binyu Zang, Defending against VM Rollback Attack, *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, 2012, doi: 10.1109/dsnw.2012.6264690

makinenin oturum açma şifresini tahmin etmek için brute-force saldırısı[69] başlatabilir. Konuk işletim sisteminin başarısız deneme sayısı konusunda kısıtlaması olsa bile saldırgan VM içindeki sayacı temizlemek ve kısıtlamayı atlamak için her denemeden sonra sanal makineyi sonsuz bir şekilde başlangıç durumuna geri alabilir.

Başka bir örnek de, bir saldırganın, bir kullanıcının izin değişikliğini geri almak ve böylece kullanıcının sonraki bilgilerini engellenmesi gereken kişilere ifşa etmek için bir izin kontrol modülünü geri alabilmesidir. Geri alma saldırısının, tekrar saldırısıyla benzer ancak farklı olması dikkat çekicidir. Tekrar ya da yeniden çalıştırma saldırısında, rakip daha önce görülen bir mesajı bir sanal makineye yeniden gönderir. Bir geri alma saldırısındayken, sanal makinenin kendisi yeniden çalıştırılır.[70]

Ne yazık ki, önceki sistemler yalnızca kullanıcı kodunun ve verilerin bütünlüğünün ve gizliliğinin korunmasına odaklandığı ve geri alma saldırılarını ihmal edildiği için büyük bir güvenlik açığı meydana getirmektedir. Anlık görüntü almak kendisi yasal ve dahili olarak tutarlı olduğu için, geri alma saldırısı bu güvenlik kontrollerinden geçebilir.[71]

Geri alma saldırılarını savunmanın çeşitli zorlukları vardır. İlk olarak, sanallaştırmanın normal işlevlerinin korunması gerekir. Bulut platformunun kendisinde daha yüksek düzeyde anlamsal bilgi bulunmadığından, bir geri alma saldırısını normal bir askıya alma ya da devam ettirme işleminden ayırt etmek genellikle zordur. Güvenlik için askıya alma / devam ettirme mekanizması devre dışı bırakılabilir, ancak bu, anlık görüntü veya VM geçişi gibi bazı normal işlemleri kullanılamaz hale getirir. İkinci olarak, gereksiz kullanıcı etkileşimi en aza indirilmelidir. Bazı sistemler, örneğin, güncelliğini sağlamak için son kullanıcıların VM önyüklemesi, devam ettirme veya taşıma sırasında dahil olmasını gerektirir. Bu, hiper yöneticinin bir sanal makineyi her başlattığı, yeniden başlattığı, devam ettirdiği

[69] Brute-force, kaba kuvvet saldırıları bir uygulamanın önemli bilgileri ele geçirmek amacıyla parolaların kırılması için kullanılan bir saldırı türüdür.
[70] Yubin Xia vd., 2012
[71] Jakub Szefer, Ruby B. Lee, "*Architectural Support for Hypervisor-Secure Virtualization*", Princeton University, ASPLOS, 2012 s. .437-439

veya taşıdığı her seferinde, önce kullanıcıdan izin istemesi gerektiği anlamına gelmektedir.[72]

[72] J. Szefer, R. B. Lee, 2012, s.1-3

İKİNCİ BÖLÜM

SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ VE KULLANIM ALANLARI

2.1. SANALLAŞTIRMA TEKNOLOJİSİ YÖNTEMLERİ

2.1.1. Tam Sanallaştırma

Tam sanallaştırma, donanımın eksiksiz bir simülasyonudur. Tam sanallaştırma, donanım özelliklerinin birkaç sanal makineye yansıtılmasını gerektirir. Bellek işlemi ve aritmetik kayıtlar gibi bazı talimatlar, doğrudan hiper yönetici tarafından kullanılan donanım tarafından yürütülebilir. Ancak diğer talimatlar simülasyon tarafından yürütülür.[73] Tam sanallaştırmada, konuk bir hiper yönetici üzerinde çalıştığını bilmez ve konuk işletim sistemi, bir hiper yönetici üzerinde çalışmak için herhangi bir değişikliğe ihtiyaç duymaz. Konuk I/O çağrıları yaptığında, bunlar hiper yöneticide hapsolur ve hiper yönetici, I/O'u fiziksel aygıt üzerinde gerçekleştirir. [74] Tam sanallaştırma, ikili kod[75] ve doğrudan yürütmenin bir kombinasyonu kullanılarak elde edilir. Tam sanallaştırma, sanal makineler için en iyi izolasyonu ve güvenliği sunar ve aynı konuk işletim sistemi örneği sanallaştırılmış veya yerel donanım üzerinde çalışabildiğinden geçişi ve taşınabilirliği basitleştirir.[76]

2.1.2. Kısmi Sanallaştırma

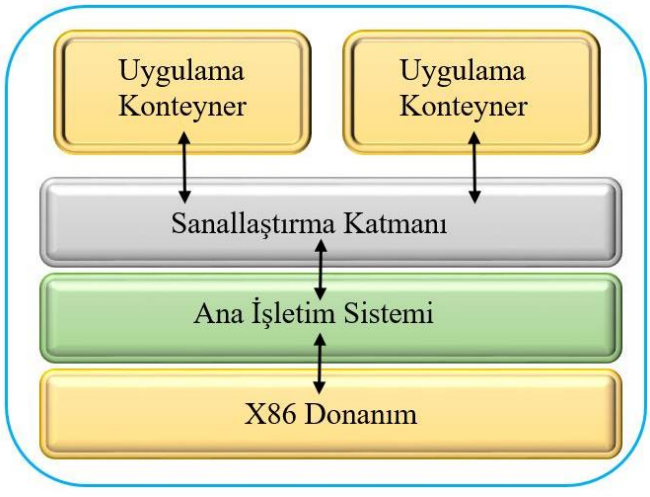
Donanım işleminde kısmi sanallaştırma, tam sanallaştırmadan farklıdır. Kısmi sanallaştırmada, hiper yönetici donanımda bulunur. Bu nedenle, kısmi sanallaştırma bir tip 1 hiper yönetici sanallaştırma mimarisidir. Kısmi sanallaştırma donanım işlemleri, değiştirilmiş bir işletim sistemi gerektiren API[77] tarafından yürütülür. Kısmi

[73] Paul Barham vd., *"Xen and the Art of Virtualization*", University of Cambridge Computer Laboratory, Cambridge, UK, 2004 s.1-2.
[74] S. M. Jain, 2020, s.10-14.
[75] Binary code (İkili kod): Bilgisayar işletim yapısının ikili rakam sisteminin 0 ve 1 kullanılarak gösterilmesidir.
[76] Diane Barrett ve Gregory Kipper, 2010, s.12-13.
[77] API (Application Programming Interface): Uygulama programlama arayüzü, bir yazılımın, uygulamanın, servisin veya platformun başka bir yazılımda tanımlanmış işlevlerini kullanabilmesi için oluşturulmuş bir tanım bütünüdür.

sanallaştırma, bir donanım ortamını taklit etmeye çalışmaz. Bunun yerine, bir sanallaştırma hiper yöneticiyi, sunucunun temelindeki donanım kaynaklarına erişimi koordine eder. Konuk işletim sistemi sanallaştırılmış bir ortamda çalıştığı konusunda bilgilendirilir ve I/O ile ilgilenmek için konuğa özel sürücüler yüklenir. Sistem I/O çağrıları, hiper çağrılarla değiştirilir. Kısmi sanallaştırma, işletim sistemi çekirdeğini değiştirmeyi içerir. İşletim sistemi çekirdeği, uygulamalar ve donanım düzeyinde yapılan işlem arasında bir köprü görevi görür. Sonuç olarak, kısmi sanallaştırma, sanal makinelerin performans düşüşünü azaltır.[78]

2.1.3. İşletim Sistemi Düzeyinde Sanallaştırma

İşletim sistemi düzeyinde sanallaştırma, bir işletim sisteminin çekirdeğinin birden çok izole edilmiş kullanıcı alanı örneklerine izin verdiği bir sunucu sanallaştırma yöntemidir. Bu örneklere konteyner adı verilir. Yazılım konteynerları ve sanallaştırma motorları kullanıcılara gerçek bir sunucu gibi gelir. Şekil 2.1, işletim sistemi düzeyinde sanallaştırmayı göstermektedir. İşletim sistemi düzeyinde sanallaştırma genellikle çok az ek yük getirir çünkü öykünmeye veya sanal bir makinede çalışmasına gerek yoktur. İşletim sistemi düzeyinde sanallaştırma, yalnızca aynı çekirdeğe sahip bir işletim sisteminin işletim sistemini barındırmasına izin verir.[79]



Şekil 2.14 : İşletim sistemi düzeyinde sanallaştırma[80]

[78] Paul Barham vd., 2004, s.2-3
[79] MinSu Chae, HwaMin Lee, Kiyeol Lee, "*A performance comparison of linux containers and virtual machines using Docker and KVM*", Cluster Comput, 2017, s.2. https://doi.org/10.1007/s10586-017-1511-2
[80] M. Chae, H. Lee, K. Lee, 2017, s.3.

İşletim sistemi düzeyinde sanallaştırma aslında tam sanallaştırmaya benzer olmasına rağmen oldukça farklıdır. Tam sanallaştırma, bir makinenin tüm donanımının sanallaştırılmasını içerir. Her sanal ortam daha sonra kendi işletim sistemi ve daha da önemlisi kendi çekirdeği altında çalıştırılır. İşletim sistemi sanallaştırma ise kendi ayrı çekirdekleriyle birlikte ayrı sanal ortamlar oluşturulmaz. Bunun yerine, işletim sistemi sanallaştırma, tek bir çekirdek altında sanal ortamları (konteyner) çalıştırır. Bir işletim sistemi sanallaştırma çözümü içindeki her bir konteyner ortamı, diğer konteynerlerden izole edilir ve fiziksel bir sunucu gibi hareket eder. Bir konteyner ortamı daha sonra uygulamaları çalıştırabilir ve fiziksel makinesinin iş yükünü kabul edebilir. İşletim sistemi sanallaştırma ve tam sanallaştırma çözümleri benzer sonuçlar sağlar, ancak ikisi arasında belirgin farklılıklar vardır ve işletim sistemi sanallaştırmanın kendi artıları ve eksileri vardır.[81]

İşletim sistemi sanallaştırması kullanılarak farklı etki alanı adları için güvenli yalıtılmış ortamlar sağlanabilir. Tek bir makinenin kaynakları, yalnızca bir alan adı için bir ana bilgisayar olarak kullanıldığında kaynaklar boşa harcanmış olur. İşletim sistemi sanallaştırmasını kullanmanın diğer faydaları arasında uygulamaların ayrılması ve kaynakları daha kolay yönetme yeteneği yer alır. Örneğin, işletim sistemi sanallaştırması kullanılarak uygulamalar farklı konteynerlara ayrılabilir veya gruplanabilir.

İşletim sistemi sanallaştırmanın tam sanallaştırma çözümlerine göre diğer avantajı, çok daha verimli olmasıdır. İşletim sistemi sanallaştırmasının çok az ek yükü vardır ve donanıma öykünmesi gerekmez. Donanım ve yazılım arasındaki iletişim, bir konteyner ana işletim sistemi çekirdeği tarafından gerçekleştirilir; bu durum daha az ek yük sağlar.[82]

2.1.4. Sunucu Sanallaştırma

Klasik yapıda uygulama entegrasyon problemleri nedeniyle yedekleme, mail, ftp gibi her rol için ayrı sunucu kullanılmaktadır. Donanım teknolojisinin çok ileri

[81] Ivanka Menken, Gerard Blokdijk, *Virtualization- The Complete Cornerstone Guide to Virtualization Best Practices_ Concepts, Terms, and Techniques*, Emereo Pty Ltd, 2010,2.ed, s.75
[82] a.g.m., s.76

seviyeye gelmesiyle sunucunun kaynakları yüksek oranda atıl durumda kalmaktadır. Sunucular işlemci, bellek, network adaptörleri gibi aygıtlardan oluşan donanım katmanı ile işletim sistemi, uygulamalar, donanım bileşenlerini kontrol eden aygıt sürücülerinden oluşan yazılım katmanından oluşmaktadır. Bu katmanlar sistem olarak adlandırılan mimariyi oluşturur. [83]

Sunucu sanallaştırma daha az fiziksel donanım kullanımı ile maliyet açısından sağladığı avantajla beraber, kurulum sonrasında daha az elektrik tükettiği, daha az soğutma ihtiyacı duyduğu için işletme maliyetlerini de büyük oranda azaltmaktadır.

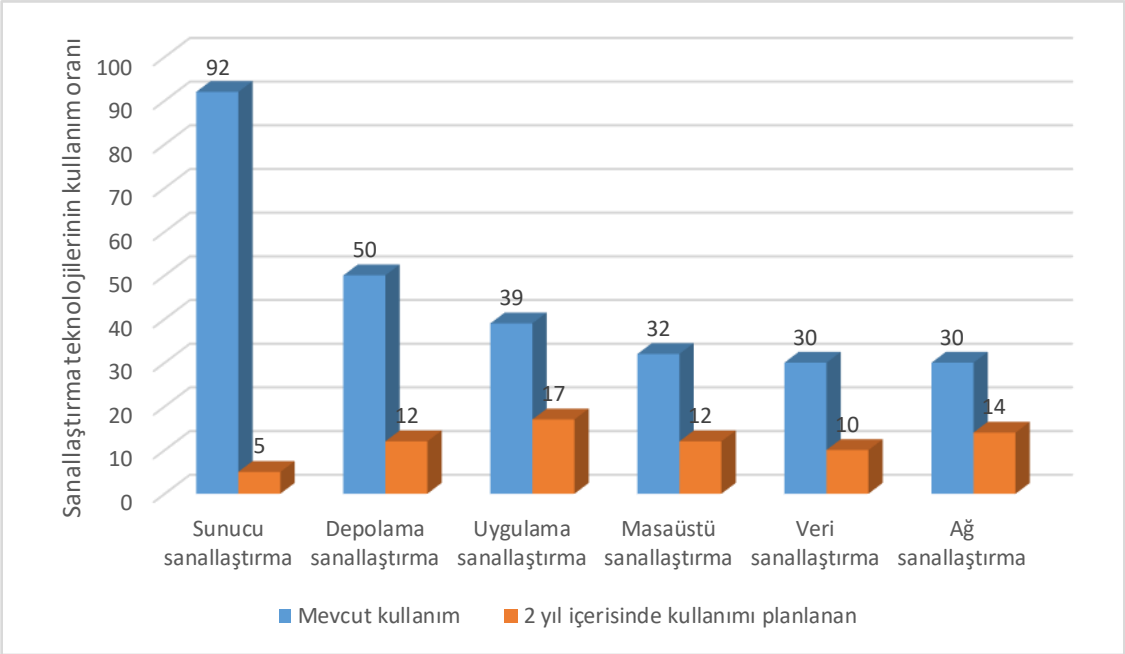
Donanım sanallaştırma olarak da atfedilen sunucu sanallaştırma, sağladığı önemli ekonomik faydalar ve verimli kaynak yönetimi özelliğiyle Bilgi Teknolojileri alanının en stratejik noktalarından biri haline gelmiştir. Kolay yönetilebilirlik özelliği ile daha dinamik bir Bilgi Teknolojisi altyapısı oluşturulmasına zemin hazırlamıştır.[84]

Yapılan araştırmalara göre 2019 yılının sonunda sunucu sanallaştırma, yüzde 92'lik bir benimseme oranıyla Kuzey Amerika ve Avrupa'daki işletmeler tarafından en yaygın kullanılan sanallaştırma teknolojisi olmuştur ve işletmelerin yüzde beşi de 2021 yılı sonuna kadar sunucu sanallaştırma teknolojisini kullanmayı planlamaktadır. Bu istatistik Şekil 2.2'de gösterilmiştir. İkinci olarak ortaya çıkan en yaygın sanallaştırma teknolojisi, aynı zamanda yazılım tanımlı depolama olarak da adlandırılan depolama sanallaştırmasıdır ve şu anki benimsenme oranı yüzde 40'tır.[85]

[83] Abdulkadir ÖKLÜ, "*Yeşil Bilgi Teknolojisi, Özel Bulut ve Karma Bir Sanallaştırma Uygulaması: Orman Genel Müdürlüğü*", Yüksek Lisans Tezi, Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü, 2013,s.37

[84] a.g.m., s.37-38

[85] https://www.statista.com/statistics/1139931/adoption-virtualization-technologies-north-america-europe/ Erişim tarihi 14.03.2021



Şekil 2.15 : 2019'da Kuzey Amerika ve Avrupa'daki işletmeler tarafından mevcut ve planlanan sanallaştırma teknolojilerinin türe göre benimsenmesi[86]

2.1.4.1. Fiziksel Sunucu ve Sanal Sunucu Tarafından İhtiyaç Duyulan Kaynakların Karşılaştırmalı Analizi

Sunucu sanallaştırmanın önemli bir özelliği enerji tasarrufu sağlamaktır. Güç kuruluşlarında, orijinal fiziksel sunucuların sayısı, normal şartlar altında değişmeyecek olan sabit bir değerdir, ancak ağ mimarisi tarafından oluşturulan sanal sunucuların sayısı değişkendir.[87] Bu, işletmenin sanal sunucuyu gerçek zamanlı durumuna göre ayarlayabildiğini gösterir.

Yu ve arkadaşları[88] fiziksel ve sanal makinelerin karşılaştırmalı analiz çalışması yapmışlardır. Yapılan bu çalışmada bir adet fiziksel sunucu ve Vcenter platformu aracılığıyla oluşturulan fiziksel sunucu ile aynı kapasite özelliklerine sahip sanal sunucunun performanslarını karşılaştırmışlardır. VCenter, sanallaştırma

[86] https://www.statista.com/statistics/1139931/adoption-virtualization-technologies-north-america-europe/ Erişim Tarihi: 14.02.2021
[87] Bakhan T. Ahmed, *Virtualization mechanisms and its tools: A comprehensive survey*, 2020, Researchgate, Vol. 9 No. 4,s.346-355 doi: 10.21817/ijcsenet/2020/v9i4/200904022
[88] Hai Yu, Jing Guo, Lei Wu, Shun Wu, Bo Peng, *Application of Server Virtualization Technology in Power Information Construction*, 2021,doi: 10.1088/1742-6596/1744/2/022008,s.3

platformunda etkin bir şekilde sürdürebilen, kurtarma süresini kısaltabilen ve operasyon ve bakımı azaltmak için sanal makine sunucusunu merkezi olarak kontrol edip yönetebilen ölçeklenebilir bir platformdur.[89]

Tablo 2.1'deki karşılaştırma sonuçlarına göre, sanal makinenin bellek kullanımını, CPU kullanımını ve yerden tasarrufunu iyileştirmede bariz avantajları vardır.

Tablo 2.1 : Fiziksel sunucu ile sanal makine arasındaki kaynak karşılaştırması[90]

	Fiziksel sunucu	Sanal sunucu
Alan kullanımı	3U-5U	-
Ağ bağlantısı	Özel kullanım	Ağ paylaşımı
CPU kullanımı	% 8 -% 20	% 30 -% 60
Bellek kullanımı	% 15 -% 35	% 60 -% 90
Hata giderme	1-2 gün	1 saatten az
İşletme ve bakım maliyeti	Yüksek maliyet	Düşük maliyet
Fiziksel optik disk sürücüsü	Özel kullanım	Ağ paylaşımı

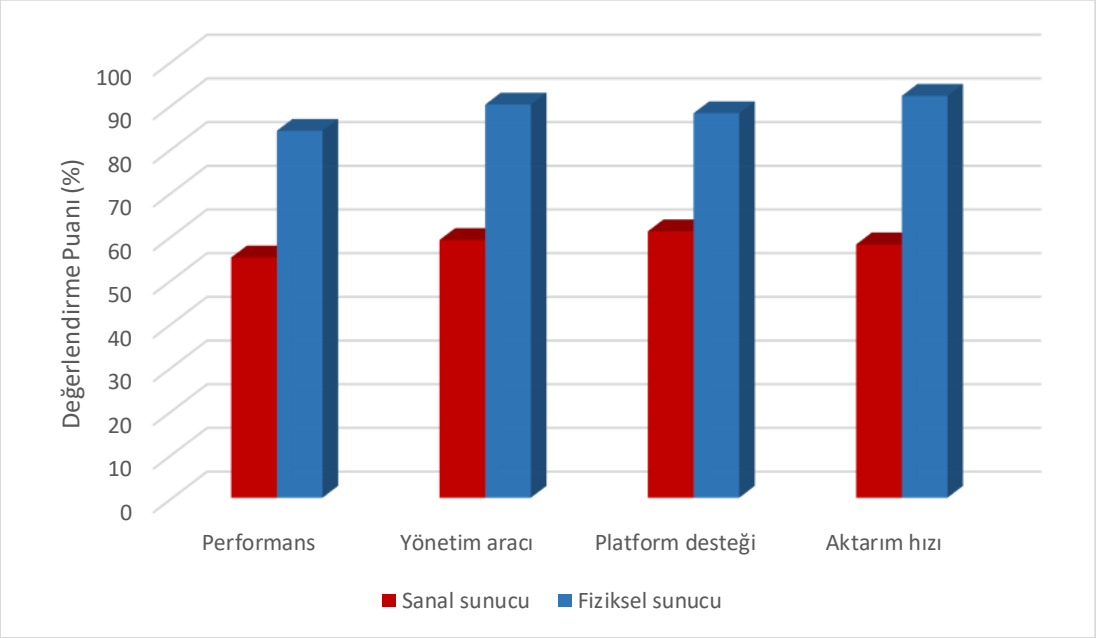
2.1.4.2. Sunucu Sanallaştırmasının Uygulama Etkisi Analizi

Yu ve arkadaşları tarafından yapılan bu analiz öncesinde ağ sunucusunun uygulama hızı büyük ölçüde geliştirilmiştir. Mevcut sanal ağ sunucusunun fiziksel uygulama işlevlerinin tam olarak entegre edilmesi temelinde, mevcut sanal sunucu uygulamalarının sayısı azaltılmış ve otomatik olarak kontrol edilmiştir. Sanal sunucu kullanmadan önce, fiziksel sunucuyu ve terminal CPU'sunu kullanan ağ kaynaklarının ortalama kullanım oranı yalnızca yaklaşık %13 olduğu gözlenmiştir. Sanal bellek sunucusuna uygulandıktan sonra, sunucunun sanal kaynaklarının ve disk CPU'sunun ortalama kullanım oranı yaklaşık %65 olduğu görülmüştür.

Şekil 2.3'teki karşılaştırma sonuçlarına göre, sanal sunucular geleneksel fiziksel sunucularla karşılaştırıldığında, performans, yönetim araçları, platform desteği ve geçişte bariz avantajlara sahiptir ve değerlendirme puanındaki her bir endeks %20'nin üzerindedir. Analiz, bunun esas olarak sistemin uyumluluğunu ve esnekliğini büyük ölçüde artıran sanal sunucunun ağ mimarisinden kaynaklandığını

[89] http://vcenter.com/ Erişim Tarihi: 18.06.2020
[90] Hai Yu, Jing Guo, Lei Wu, Shun Wu, Bo Peng, 2021, s.4

göstermektedir. Ancak geleneksel fiziksel sunucunun bu açıdan hiçbir avantajı yoktur ve daha fazla kaynak tüketmektedir.[91]

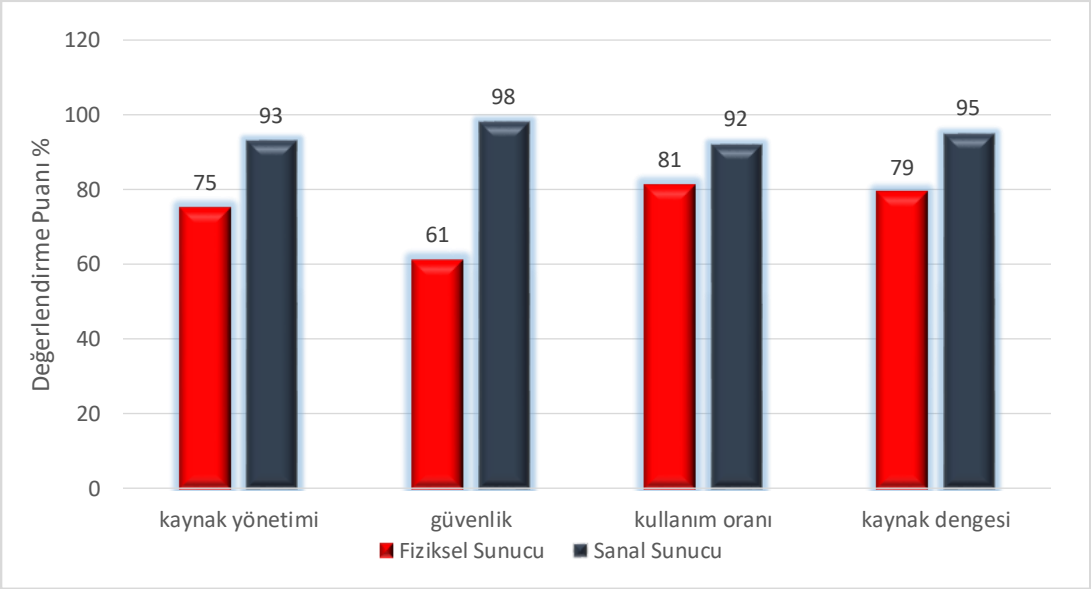


Şekil 2.16 : Sanal sunucu ile fiziksel sunucu arasındaki ana performansın karşılaştırmalı analizi[92]

Şekil 2.4'teki karşılaştırma sonuçlarına göre sanal sunucular geleneksel fiziksel sunucularla karşılaştırıldığında kaynak yönetimi, bilgi güvenliği, kullanım ve kaynak dengesi konularında da önemli avantajlara sahiptir. Tek puan açısından, her bir dizinin puanı, özellikle bilgi güvenliği açısından büyük ölçüde iyileştirilmiştir.

Analiz, bunun temel olarak sanal sunucunun kaynakların daha bilimsel ve makul şekilde kullanılmasından kaynaklandığını, dolayısıyla kaynak yönetimi ve kullanımında iyi bir avantaja sahip olduğunu göstermektedir.[93]

[91] a.g.m, s.4-5
[92] Hai Yu, Jing Guo, Lei Wu, Shun Wu, Bo Peng,2021,s.4-5
[93] a.g.m, s.5



Şekil 2.17 : Sanal sunucu ile fiziksel sunucu arasındaki ana performansın karşılaştırmalı analizi[94]

Bu bağlamda sunucunun sanallaştırılması, bilgi güvenliğini artırabilir, enerji tüketimini azaltabilir ve kullanımı iyileştirebilir.

2.1.4.3. Sunucu Sanallaştırma Güvenlik Önlemleri

Sanallaştırmanın güvenliği karmaşık bir sorundur. Güvenlik dağıtımı açısından, yalnızca sanal makinenin güvenliği değil, aynı zamanda sanal makine ana bilgisayarı ve ağ ortamının güvenliği de göz önünde bulundurulmalıdır.[95] Sanal makinenin güvenliği aşağıdaki yönlerden düşünülebilir:

- Ağ bölümü oluşturulmalıdır. Ağ ayırma ayarları optimize edilmeli ve kablosuz ağ izole edilmelidir.
- Yazılım sistemi yapılandırmasının makul olduğundan emin olunmalıdır ve dosya paylaşım hizmeti yönetim sistemi işlevleri ciddi şekilde organize edilmelidir.
- Her sanal makineye virüsten koruma yazılımı yüklenmeli ve virüs koruma yazılımı her gün otomatik olarak taranmalıdır.

[94] Hai Yu, Jing Guo, Lei Wu, Shun Wu, Bo Peng,2021,s.5
[95] Steven J. Vaughan-Nichols, *Virtualization sparks security concerns*, Computer 41 (8), 2008, 13–15, doi:10.1109/mc.2008.276

➢ Sanal yedekleme çözümü yazılımı aracılığıyla uygun donanım sanal makine veri yedekleme çözümlerinin geliştirilmesi ve önemli donanım verilerinin her gün otomatik olarak gerçek zamanlı yedeklenmesi gerekmektedir.[96]

2.1.5. Depolama Sanallaştırma

Depolama sanallaştırma, mantıksal depolamayı fiziksel depolamadan soyutlama işlemidir. Oluşturulan ve depolanan veri miktarı hızla artmaktadır. Depolama gereksinimlerindeki bu muazzam artış, depolama mimarisinin bir veri merkezi modeline dönüşmesini sağlamıştır. Sanallaştırılmış depolama dizileri, geleneksel disk dizilerine kıyasla daha fazla esneklik, basitleştirilmiş yönetim, daha iyi performans ve kapasite kullanımı sunmaktadır.[97]

Geleneksel olarak, bir Depolama sanallaştırma katmanı, sunucuların mevcut fiziksel depolamayı sanal disklere veya birimlere bölmek için kullandıkları yazılımda uygulanan bir soyutlama düzeyini ifade eder. Sanal birimler işletim sistemi (OS) tarafından fiziksel disklermiş gibi kullanılır. Depolama Sanallaştırma Katmanı, bir sanal diske karşı yapılan I/O isteklerini gerçek depolamadaki bloklara yönlendirir. Bu yönlendirme, depolama bloklarının fiziksel konumundaki değişikliklerin (hizmet erişim modellerine, performans gereksinimlerine, büyüme gereksinimlerine veya arıza kurtarmaya), sanaldan gerçeğe eşlemelerin basit bir güncellemesi ile karşılanabileceği anlamına gelir. Bir sanal birim, üzerinde bulunduğu depolama alt sistemlerinden bağımsız olarak oluşturulabilir, genişletilebilir, silinebilir, taşınabilir ve seçilerek sunulabilir. Ayrıca, bir sanal birim, her biri farklı özelliklere sahip olan farklı depolama alt sistemlerinde depolama alanı içerebilir.[98]

Depolama sanallaştırmasında en çok NAS ve SAN depolama sistemi kullanılır. Canlı sanal makinelerin taşınması, yüksek kullanılabilirlik, hata toleransı ve olağanüstü durumdan kurtarma gibi gelişmiş sunucu sanallaştırma özelliklerinden yararlanabilmesi için bir paylaşılan depolama sistemi gereklidir.

---

[96] Steven J. Vaughan-Nichols, 2008, s.13–15.
[97] Emin Şeşen, *Masaüstü Sanallaştırma Teknolojilerinin Performanslarının Analizi*, Düzce Üniversitesi, Yüksek Lisans Tezi, 2017, s.10-11
[98] Wayne Karpoff, Brian Lake, *Storage Virtualization System And Methods*, 2002, s.7-8, Patent No.: US 6,857,059 B2

2.1.5.1. Depolama Alan Ağı (SAN)

SAN sanallaştırmada en çok kullanılan depolama alanıdır. Sunucu tabanlı depolamadan ağ tabanlı depolamaya geçmenin bir yolu olarak daha büyük ağlarda depolama ihtiyacının artmasıyla daha çok kullanılmaya başlanmıştır.[99] Sunucu tabanlı depolama (server-based storage), dosya depolaması için yerel disklerini kullanıcılarla paylaşan bir sunucuya kalıcı olarak bağlanılan geleneksel dosya sunucusu depolamadır. Ağ tabanlı depolama (network-based storage) ise herhangi bir sunucu için yerel olmayan, ancak disk dizileri, teyp kitaplıkları, optik disk dizileri ve çeşitli ağa bağlı depolama aygıtları biçiminde bir ağa yayılan depolamadır. SAN, sunucular tarafından erişilebilen bir depolama aygıtıdır. Bir SAN, genellikle normal ağ üzerinden normal aygıtlar tarafından erişilemeyen kendi depolama aygıtları ağına sahiptir. Tek başına SAN, NAS gibi "dosya" soyutlamasını sağlamaz, yalnızca blok düzeyinde işlemler sağlar. Tipik olarak, ağlar büyüdükçe ve geliştikçe, SAN mimarisine yönelik aşağıdaki aşamalı adımlar atılmıştır:[100]

- Sunucu tabanlı depolama
- Ağa bağlı depolama (NAS)
- Depolama alanı ağları (SAN)
- Sanal depolama alanı ağları (VSAN'lar)

Genel olarak, büyük, karmaşık ağlar için sanallaştırılmış depolamanın bazı önemli avantajları vardır. Başlıca avantajı, depolama yönetimi ve bir SAN içindeki ağ trafiğinin ayrılmasıdır. Büyük kapasitedeki bir SAN segmentlere veya VSAN'lara[101] bölündüğünde, SAN altyapısı daha yönetilebilir bir yapıya dönüşür; aynı zamanda SAN'ın performansı ve ölçeklenebilirliğini de gelişmektedir. SAN'larda kullanılan

[99] Ersin Büyükyılmaz, 2016, s.15

[100] Kenneth Hess and Amy Newman, Practical Virtualization Solutions Virtualization from the Trenches, 1st ed, 2010, Pearson Education, s.188-189

[101] Bilgisayar ağında, bir sanal depolama alanı ağı (VSAN), sanal bir yapı oluşturan bir dizi bağlı Fiber Kanal anahtarından bir bağlantı noktaları koleksiyonudur. Tek bir anahtardaki bağlantı noktaları, donanım kaynaklarının paylaşılmasına rağmen birden çok VSAN'a bölünebilir. Tersine, birden çok anahtar, tek bir VSAN oluşturmak için bir dizi bağlantı noktasını birleştirebilir.

cihazlar, ağ üzerinden veri aktarmak için özel iletişim protokolleri kullanır. Fiber kanal ve ISCSI, SAN'larda kullanılan iki ana protokoldür.[102]

ISCSI, depolama sunucuları ile diğer sunucular ve istemciler veya kullanıcılar arasında bir bağlantı olarak internet protokolüne dayalı bir depolama ortamıdır. Başka bir deyişle, ISCSI, sabit disk sürücüsü (HDD) veya Katı Hal Sürücüsü (SSD) gibi depolama ortamlarını veri aktarım ortamı olarak bir internet ağı veya intranet ile bağlamak için kullanışlı bir protokoldür.[103]

Fiber kanal (FC), ham blok verilerinin sırayla ve veri kaybı olmadan teslim edilmesini sağlayan yüksek hızlı bir veri aktarım protokolüdür. Fiber kanal, öncelikle ticari veri merkezlerindeki depolama alanı ağlarında (SAN) bilgisayar veri depolamasını sunuculara bağlamak için kullanılır.

SAN'ın yaygın kullanımları arasında, e-posta sunucuları, veritabanları ve yüksek kullanımlı dosya sunucuları gibi depolama sabit sürücülerine yüksek hızlı blok düzeyinde erişim gerektiren işlemsel olarak erişilen verilerin sağlanması yer alır.[104] VLAN'lar ve VSAN'lar, cihazların ve bir ağ bölmesine giden trafiğin mantıksal olarak ayrılması açısından çok benzerdir. VLAN ve VSAN oluşturma, anahtar düzeyinde gerçekleşir. Ayrı depolama aygıtları, benzersiz bir kimlik numarasına sahip bir mantıksal birim (VSAN) halinde gruplanır. Anahtar daha sonra verileri ID'ye göre doğru VSAN'a iletmekten sorumludur. VSAN, SAN yöneticilerinin SAN'ları daha verimli bir şekilde yönetmesini sağlar çünkü VSAN, konum sorununu SAN'dan kaldırır. Ayrıca SAN'ın tamamını kapatmadan depolama aygıtlarını değiştirerek, ekleyerek veya kaldırarak bakımın kesintiye uğramadan yapılmasına da olanak tanımaktadır.[105]

[102] K. Hess, A. Newman, 2010, s.188-189.
[103] Moh. Thoip Abdullah, Sulhan Qidri, Wadi Nuryadi, Septian Rheno Widianto, *Failover Cluster Nodes and ISCSI Storage Area Network on Virtualization Windows Server 2016*, JOIN (Jurnal Online Informatika) Volume 5 No.1, 2020, s.89-96 doi: 10.15575/join. v5i1.564.
[104] T.Merdan, 2010, s.21.
[105] Kenneth Hess and Amy Newman, 2010, s.190.

2.1.5.2. Ağa Bağlı Depolama (NAS)

NAS, ağda bulunan ve ağdaki sunuculara depolama sağlayan bir depolama cihazıdır. PC kullanıcıları gibi birden çok istemcinin ve sunucuların bir Yerel Alan Ağı (LAN) üzerinden dosya paylaşmasına izin verir. NAS, depolamanın uzak olduğu ve bilgisayarların bir disk bloğu yerine bir dosya talep ettiği NFS veya SMB / CIFS gibi dosya tabanlı protokoller kullanır. Dahası, tüm dosyalar merkezi bir konuma taşındığında, onlarca, yüzlerce ve hatta binlerce makineye yayılan dosyaları takip etmek zorunda kalmak yerine onları yönetmek çok daha kolaydır; tüm veriler tek bir yerde bulunur ve bu sayede yedekleme ve arşivleme daha iyi hale gelir.

NAS'ın en önemli avantajı, IP tabanlı olması ve kurulumu ve yönetiminin basit olmasıdır. NAS'ın yaygın kullanımları arasında zengin medya, belge ve yedekleme dosyaları ve e-posta için hızlı dosya depolaması bulunur.[106]

2.1.6. Ağ Sanallaştırma

Ağ Sanallaştırma geleneksel olarak donanımdan yazılıma teslim edilen ağ kaynaklarının soyutlanması anlamına gelir. Ağ sanallaştırma, birden çok fiziksel ağı tek bir sanal, yazılım tabanlı ağda birleştirebilir veya bir fiziksel ağı ayrı, bağımsız sanal ağlara bölebilir.

Ağ sanallaştırma yazılımı, ağ yöneticilerinin ağı yeniden yapılandırmadan sanal makineleri farklı etki alanlarına taşımasına olanak tanır. Yazılım, aynı fiziksel ağ yapısı üzerinde ayrı sanal ağ çalıştırabilen bir ağ katmanı oluşturur.[107]

Ağ sanallaştırma, ağ hizmetlerini temeldeki donanımdan ayırır ve tüm ağın sanal provizyonuna izin verir. Paket iletme arka planı olarak altta yatan fiziksel ağı kullanmaya devam ederken, programlı olarak ağları tamamen yazılım içinde oluşturmayı, sağlamayı ve yönetmeyi mümkün kılar. Anahtarlama, yönlendirme, güvenlik duvarı, yük dengeleme ve sanal özel ağlar (VPN'ler) fiziksel ağ kaynakları

[106] K. Hess, A. Newman, 2010, s.191.
[107] https://www.vmware.com/topics/glossary/content/network-virtualization Erişim Tarihi: 19.12.2020

havuzda toplanır, yazılım içinde sunulur ve temeldeki fiziksel ağdan yalnızca İnternet Protokolü (IP) paket iletimini gerektirir.

Yazılımdaki ağ ve güvenlik hizmetleri, sanal bir katmana dağıtılır ve sanal makineler veya konteynerlar gibi her bağlı uygulama için tanımlanan ağ ve güvenlik politikalarına uygun olarak ayrı iş yüklerine eklenir.[108]

Bir iş yükü başka bir ana bilgisayara taşındığında, ağ hizmetleri ve güvenlik politikaları da onunla birlikte hareket eder. Bir uygulamayı ölçeklendirmek için yeni iş yükleri oluşturulduğunda, gerekli ilkeler bu yeni iş yüklerine dinamik olarak uygulanır ve daha fazla ilke tutarlılığı ve ağ çevikliği sağlar.

2.1.6.1. Ağ Sanallaştırmanın Faydaları

Ağ sanallaştırma, kuruluşların bir veri merkezi ağını çalıştırmaya ve buluttaki ağı ve güvenliği yönetmeye giden süreçlerin çoğunu otomatikleştirip basitleştirerek, hız, çeviklik ve güvenlikte büyük ilerlemeler elde etmelerine yardımcı olur. Ağ sanallaştırmanın temel avantajlarından bazıları şunlardır:

- Ağ sağlama süresini haftalardan dakikalara indirmektedir.
- Manuel süreçleri otomatikleştirerek daha yüksek operasyonel verimlilik elde edilmesini sağlar.
- İş yükleri fiziksel topolojiden bağımsız olarak yerleştirilebilir ve taşınabilir.
- Veri merkezi içindeki ağ güvenliğini arttırmaktadır.
- Sanallaştırma özellikli ağ cihazları uzaktan yönetilir ve mantıksal olarak yeniden yapılandırılabilir.[109]

2.1.7. Ağ İşlevleri Sanallaştırma

Ağ işlevleri sanallaştırma (NFV), geleneksel olarak özel donanım üzerinde çalıştırılan yönlendirici (router), güvenlik duvarı (firewall) ve yük dengeleme (load balancer) gibi ağ hizmetlerini sanallaştırmanın bir yoludur. Bu hizmetler, donanımı

[108] G.Schaffrath, C.Werle, P.Papadimitriou, A.Feldmann, R.Bless, A.Greenhalgh, A.Wundsam, M.Kind, O.Maennel, L.Mathy ,Network Virtualization Architecture: Proposal and Initial Prototype, Published in VISA, Barselona, 2009, s.1-8.
[109] G.Schaffrath, C.Werle, P.Papadimitriou, A.Feldmann, R.Bless, A.Greenhalgh, A.Wundsam, M.Kind, O.Maennel, L.Mathy, 2009, s.1-8

üzerinde VM olarak paketlenmiştir ve bu, hizmet sağlayıcıların ağlarını özel sunucular yerine standart sunucularda çalıştırmalarına olanak tanır. NFV, telekomünikasyon endüstrisini yeniden şekillendiren bir telekomünikasyon bulutunun temel bileşenlerinden biridir.

NFV ile, her ağ işlevi için özel donanıma sahip olunmasına gerek yoktur. NFV, hizmet sağlayıcıların ek donanım kaynakları gerektirmeden talep üzerine yeni ağ hizmetleri ve uygulamaları sunmalarına izin vererek ölçeklenebilirliği ve çevikliği artırmaktadır.[110]

Ağ işlevleri sanallaştırmanın birçok avantajı vardır. NFV ile servis sağlayıcılar, ağ işlevlerini özel donanım yerine standart donanım üzerinde çalıştırabilir. Ayrıca, ağ işlevleri sanallaştırıldığı için, tek bir sunucuda birden çok işlev çalıştırılabilir. Bu, daha az fiziksel donanıma ihtiyaç duyulduğu anlamına gelir, bu da fiziksel alan, güç ve genel maliyet düşüşleriyle sonuçlanan kaynak konsolidasyonuna izin verir.

NFV, sağlayıcılara VNF'leri [111] farklı sunucularda çalıştırma veya talep değiştiğinde bunları taşıma esnekliği sağlar. Bu esneklik, servis sağlayıcıların hizmetleri ve uygulamaları daha hızlı sunmasını sağlar.

NFV hizmet sunumunu kolaylaştırır ve ağları nispeten daha esnek hale getirir. Maliyet tasarrufu sağlamanın yanı sıra yüksek kapasiteli sunucu altyapısı kurma olasılığını da sağlamaktadır. Standart sunuculardaki yazılıma geçiş yoluyla ağ ekipmanı satın alma maliyetleri azalır. NFV sayesinde daha hızlı dağıtım süresi sağlanır. Ayrıca alandan tasarruf, güç ve soğutmada verimlilik sağlamaktadır. [112]

2.1.8. Uygulama Sanallaştırma

Uygulama sanallaştırma, kullanıcıların bir uygulamaya, uygulamanın yüklü olduğu bilgisayardan farklı bir bilgisayardan erişmesine ve onu kullanmasına olanak tanıyan bir teknolojidir. BT yöneticileri, uygulama sanallaştırma yazılımını kullanarak uzak uygulamaları bir sunucuda kurabilir ve ardından uygulamaları bir son

[110] https://www.redhat.com/en/topics/virtualization/what-is-nfv Erişim tarihi :29.01.2021
[111] Virtualized network functions (VNF) :Sanallaştırılmış ağ işlevleri dosya paylaşımı, dizin hizmetleri ve IP yapılandırması gibi ağ işlevleri sunan yazılım uygulamalarıdır.
[112] https://www.intraway.com/blog/nfv-benefits Erişim Tarihi: 29.11.2021

kullanıcının bilgisayarına teslim edebilir. Kullanıcı için sanallaştırılmış uygulamanın deneyimi, yüklü uygulamayı fiziksel bir makinede kullanmakla aynıdır.

Uygulama sanallaştırmanın sağladığı birtakım avantajlar vardır:

Uygulama Yönetimi: Uygulama sanallaştırma, BT departmanlarının bir kuruluştaki uygulamaları yönetmesini ve sürdürmesini çok daha kolay hale getirir. Uygulama sanallaştırma, uygulamaları her kullanıcının makinesine manuel olarak yüklemek yerine, BT yöneticilerinin bir uygulamayı merkezi bir sunucuya bir kez yüklemesine ve ardından uygulamayı gerektiği şekilde kullanıcı cihazlarına dağıtmasına olanak tanır.

Ölçeklenebilirlik: Uygulama sanallaştırma, BT yöneticilerinin sanal uygulamaları, bu cihazların işletim sistemlerinden veya depolama alanından bağımsız olarak her tür bağlı cihaza dağıtmasına olanak tanımaktadır. Ayrıca uygulama aslında merkezi sunucuda çalıştığı için normalde işletim sisteminde çalışmayan uygulamalara erişmesine de olanak tanır. Bu, genellikle bir Windows uygulamasını bir Linux işletim sisteminde sanal olarak çalıştırmak için kullanılır.

Güvenlik: Uygulama sanallaştırma yazılımı, BT yöneticilerine hangi kullanıcıların hangi uygulamalara erişebileceği konusunda merkezi denetim sağlar. Bir kullanıcının bir kuruluş içindeki uygulama izinleri değişirse, BT yöneticisi o kullanıcının bir uygulamaya erişimini kaldırabilir. Uygulama sanallaştırma olmasaydı, BT yöneticisinin uygulamayı kullanıcının cihazından fiziksel olarak kaldırması gerekirdi. Uygulama erişimi üzerindeki bu merkezi kontrol, özellikle bir kullanıcının cihazları kaybolursa veya çalınırsa önemlidir; çünkü BT yöneticisi, eksik cihazı bulmak zorunda kalmadan hassas verilere uzaktan erişimi iptal edebilir.[113]

2.1.9. Masaüstü Sanallaştırma

Masaüstü sanallaştırma, sanallaştırma teknolojisine odaklanan pratik bir uygulamadır. Masaüstü sanallaştırmanın amacı, masaüstünü sanal hale getirmektir, böylece kullanıcılar herhangi bir zamanda ve herhangi bir yerde herhangi bir cihazla

[113] https://www.citrix.com/tr-tr/glossary/what-is-application-virtualization.html Erişim Tarihi: 28.01.2021

ağ üzerinden kişisel masaüstlerine giriş yapabilirler.[114] Bu teknolojinin, insanların hayatlarını büyük ölçüde kolaylaştırmak için mobil bilgi işlem, güvenlik, daha kolay yönetim ve maliyet azaltma gibi birçok avantajı vardır. [115] Masaüstü sanallaştırma, diğer sanallaştırma stratejileri türlerine uygulanabilen bir terimdir. Örneğin, bir masaüstü iş istasyonu, birkaç işletim sisteminin aynı anda tek bir yerel masaüstü makinede çalışmasına izin vermek için bir masaüstü sanallaştırma ürününü kullanabilir.[116]

Masaüstü sanallaştırma teknolojisinin gelişimi aşağıdaki üç aşamadan geçer:

İlk aşama: İstemci işletim sistemi sanallaştırmasının uygulanmasıdır. Bu aşama, esas olarak işletim sistemi ve donanım aygıtlarının sanallaştırma teknolojisi ile yalıtılmasını gerçekleştirir; böylece sanal bilgisayar masaüstleri, donanım sınırlamaları olmaksızın birden çok bilgisayar arasında özgürce çoğaltılabilir ve uygulanabilir.

İkinci aşama: Ağın uygulanması ve sanal masaüstünün merkezi yönetimidir. Bu aşama, esas olarak ağda depolanan sanal masaüstü işletim sistemlerinin merkezi yönetimini gerçekleştirir; böylece kullanıcılar kendi masaüstlerini herhangi bir makinede ağ üzerinden kolayca kullanabilirler.

Üçüncü aşama: Masaüstü sanallaştırma teknolojisinin kullanılabilirliğinin ve önceden tahmin edilmesinin uygulanmasıdır. İşletim sistemi ve donanım ortamının izolasyonu tamamen gerçekleştiğinde, herkes kolaylıkla daha fazla masaüstüne sahip olabilir.[117]

---

[114] Sadettin Uygur Eren, *Vmware Ve Hyper-V Sanallaştırma Sistemlerinin Performans Ve Yüksek Kullanılabilirliğinin Deneysel Olarak Karşılaştırılması*, Yüksek Lisans Tezi, T.C. Maltepe Üniversitesi,2020, İstanbul,s.7

[115] Selma Büyükgöze, "*Kırklareli University Kayalı Campus' Desktop Virtualization*", Research Journal of Business and Management Dergisi 3/4 (2016): 306-313

[116] Karissa Miller, Mahmoud Pegah, *Virtualization, Virtually at the Desktop*, Ringling College of Art and Design, SIGUCCS '07: Proceedings of the 35th annual ACM SIGUCCS fall conference, 2007 s. 255–260 doi:10.1145/1294046.1294107

[117] Li Yan, *Development and Application of Desktop Virtualization Technology*, IEEE 3rd International Conference on Communication Software and Networks, 2011, s.326-329, doi: 10.1109/ICCSN.2011.6013725

Masaüstü sanallaştırma teknolojisinin göz önünde bulundurulması gereken en önemli konu, bilgisayarın kolay, güvenli ve verimli bir şekilde nasıl yönetileceği olmalıdır. Mevcut masaüstü sanallaştırma ürünleri, temelde işletim sistemi ile donanım aygıtlarının ayrılmasını sağlayan ilk aşamada yoğunlaşmıştır. Devam eden ikinci aşamanın çalışması şu anda çok popüler bir sanallaştırma çözümü olan bulut bilişimdir. Masaüstü sanallaştırma için en çok kullanılan iki çeşit dağıtım modeli vardır:

2.1.9.1. Sanal Masaüstü Altyapısı (VDI)

VDI, sanal masaüstlerini sağlamak ve yönetmek için sanal makineleri kullanan bir sanallaştırma çözümüdür. VDI, masaüstü ortamlarını merkezi bir sunucuda barındırır ve bunları istek üzerine son kullanıcılara dağıtır. Şekil 2.5'te gösterildiği üzere ağ üzerinden dizüstü bilgisayar, tablet gibi bir uç nokta cihazıyla erişilebilmektedir.[118]



Şekil 2.18 : Sanal masaüstü altyapısına uç nokta cihazlarla erişim

Bir VDI çözümü ile kuruluşlar bir dizi avantaj elde edebilir. Masaüstü bilgi işlem, uç nokta cihazı yerine ana sunucuda gerçekleşir, bu nedenle uç nokta için donanım gereksinimleri daha düşüktür. Bu, potansiyel olarak bir uç nokta cihazına yapılan yatırımı düşürmektedir ve çok çeşitli uzak ve mobil cihazları desteklemek daha kolay olmaktadır. VDI masaüstlerini sağlamaya yönelik iki yaklaşım vardır:

[118] L. Yan, 2011, s.326-329.

Kalıcı masaüstü: Her kullanıcıya, kendi tercihlerine göre özelleştirebilecekleri benzersiz bir masaüstü örneği atanır.

Kalıcı olmayan masaüstü: Kullanıcılar, görevleri gerçekleştirmek için gerektiği gibi tek tip masaüstü görüntüleri havuzuna erişebilirler. Bu kalıcı olmayan masaüstü bilgisayarlar, kullanıcı için kişiselleştirilmek yerine, her kullanımdan sonra orijinal durumlarına geri döner.[119]

VDI altyapısı birçok avantaj sağlamaktadır. En önemli avantajlardan birkaçı aşağıda sıralanmıştır:

Arttırılmış ölçeklenebilirlik: Bulut bilişim, tüm VDI altyapısını bir ana sunucu üzerinde konsolide etmektedir. Bu sayede kullanıcılar ortamlarına herhangi bir cihazdan erişebildikleri için donanım gereksinimleri azalmaktadır.

Merkezi yönetim: VDI'ler, yöneticilerin tüm sanallaştırılmış masaüstlerini tek seferde yamalamasına, güncellemesine ve değiştirmesine olanak tanıyan merkezi bir yönetim yapısı sağlar. Bu aynı zamanda eksiksiz bir masaüstü felaket kurtarma stratejisine olanak tanır çünkü tüm bileşenler veri merkezinde kaydedilir ve yedeklenir.

Güvenlik: VDI, uygulamalar istemci cihazda değil, veri merkezindeki ana sunucuda çalıştığı için işletmelerin tam gizliliklerini korumalarına yardımcı olmaktadır.

Erişilebilirlik: VDI, son kullanıcıların kendi cihazlarını kullanarak herhangi bir konumdan dosyalarına, uygulamalarına ve bulut hizmetlerine uzaktan erişim elde etmelerine olanak tanımaktadır. Bu, dijital bir çalışma alanı / uzak masaüstü oluşturmakta bu sayede çalışanlar PC'leri, tabletleri, akıllı telefonları ve ince istemcileri kullanabildiği için evden çalışmayı önemli ölçüde kolaylaştırmaktadır.

Maliyet tasarrufu: BT'nin yeni donanım satın almaya devam etmesine gerek olmadığı için donanım giderleri önemli ölçüde azaltmaktadır. [120]

---

[119] https://www.netapp.com/virtual-desktop-infrastructure/what-is-virtual-desktop-infrastructure/ Erişim tarihi 17.09.2020

[120] https://www.nakivo.com/blog/key-differences-between-vmware-horizon-and-vdi/ Erişim tarihi: 14.02.2021

2.1.9.2. Hizmet Olarak Masaüstü (DaaS)

DaaS, üçüncü taraf bir sağlayıcı tarafından barındırılan bulut tabanlı bir masaüstü sanallaştırma hizmetidir. Üçüncü taraf bulut sağlayıcısı, masaüstü işletim sistemlerini çalıştıran sanal bulut makineleri dahil olmak üzere masaüstü depolama, bilgi işlem ve ağ oluşturma gibi tüm arka uç kaynaklarını yönetir.

Bir servis sağlayıcı olarak sanal masaüstlerini son kullanıcı cihazlarına aktararak, masaüstlerine ve uygulamalara her zaman, her yerden erişime izin verir. Diğer bulut masaüstü sanallaştırma türleri gibi DaaS, değişken iş yükleri ve değişen depolama talepleri için destek sağlama, uygulamaları ve verileri neredeyse tüm internet bağlantılı cihazlardan erişilebilir hale getirme yeteneği dahil olmak üzere bulut bilişimin birçok genel avantajını sağlamaktadır. DaaS'ın başlıca dezavantajı, özelliklerin ve konfigürasyonların her zaman gerektiği kadar özelleştirilebilir olmamasıdır.[121]

2.1.10. Servis Sanallaştırma

Uygulama sanallaştırma, bir uygulamayı yürütüldüğü temel işletim sisteminden kapsülleyen bir teknolojidir. Hedef cihaza kurmaya gerek kalmadan bir uygulamaya erişim sağlamaktadır. Kullanıcının bakış açısından, uygulama cihazdaki yerel gibi çalışır ve etkileşim kurar. Kullanıcı, uygulama penceresini yeniden boyutlandırabilir, taşıyabilir veya küçültebilir, ayrıca bilindik klavye ve fare işlemlerini kullanabilmektedir.[122]

Uygulama sanallaştırmanın sağladığı birçok faydası vardır ve bunlardan bazıları aşağıda listelenmiştir:

- **Basit kurulum:** Bir uygulama sunucuya bir kez yüklendiğinde, istenilen kadar uç noktaya sanallaştırma imkânı sağlamaktadır.
- **Kolay dağıtım**: Uygulamaları istemciler için dağıtmak son derece kolaydır.

[121] https://www.nutanix.com/info/desktop-as-a-service-daas Erişim tarihi: 22.09.2020
[122] https://www.citrix.com/tr-tr/glossary/what-is-application-virtualization.html Erişim Tarihi: 02.10.2020

- **Daha iyi taşınabilirlik:** Sanallaştırılmış uygulamalar, Windows, Android veya iOS gibi herhangi bir uç noktada her yerde kullanılabilir. Bu ekstra taşınabilirlik, kritik bilgilerin sunucuda kalmasına da olanak tanımaktadır.
- **Kolay bir şekilde istenmeyen uygulamaların sistemden çıkartılması**: İstenmeyen uygulamalardan kurtulmak için uygulamayı her bilgisayardan kaldırmak yerine sanal uygulamalar silinmektedir.
- **Uygulamalar arasındaki çakışmaların azalması**: Bir uygulamanın yüklenmesi bazen sorunlara ve diğerinin çökmesine neden olabilir. Sanallaştırılmış uygulamalar uç noktalarda çalışan sanal versiyonlar olduğundan bu sorun büyük ölçüde azaltılır.
- **Daha kolay geri alma:** Bir uygulama beklendiği gibi çalışmazsa, kolayca merkezi olarak en kararlı durumuna geri döndürülebilir.
- **Gelişmiş güvenlik:** Sanallaştırılmış uygulamalar birbirlerinden ve işletim sisteminden izole edildiğinden, birinde görünen kötü amaçlı yazılımlar diğerini etkileyemez.
- **Daha kolay güncellemeler:** Sanallaştırılmış uygulamaları merkezi bir konumdan bir kez güncelleyebilirsiniz ve bu güncellemelerin tüm masaüstlerinde ayrı ayrı yapılması gerekmez.
- **Basitleştirilmiş destek:** Sanal uygulamaların çalışmasıyla ilgili sorunlar varsa, yardım masası personeli bunu merkezi bir konumdan kolayca görüntüleyebilir ve sorunları merkezi olarak çözebilir.
- **İşletim sisteminden bağımsızlık:** Sanallaştırılmış uygulamalar, kullanılan işletim sisteminden bağımsızdır, dolayısıyla onları Microsoft, iOS veya Android gibi herhangi bir uç noktada kullanılabilir kılmaktadır.[123]

2.1.11. Konteyner Tabanlı Sanallaştırma

Konteyner tabanlı sanallaştırmalar, geleneksel sanallaştırma teknolojisine bir alternatif olarak ortaya çıkmıştır. Hiper yönetici tabanlı sanallaştırmanın aksine, konteyner tabanlı sanallaştırma işletim sistemi düzeyinde yapılır. Bu nedenle, işletim

[123] https://www.parallels.com/blogs/ras/application-virtualization/ Erişim tarihi:16.10.2020

sistemi düzeyinde sanallaştırma olarak da adlandırılır.[124] Tüm hiper yönetici tabanlı sanal sunucuların kendi konuk işletim sistemine sahip olması gerekir. Konteyner tabanlı sanallaştırmada, konteynerlar ana işletim sisteminin çekirdeğini kullanır, bu da ortak bir işletim sistemi kullandıkları anlamına gelir.[125]

Bu teknikte, işletim sisteminin çekirdeği, üzerine birçok yalıtılmış misafirin kurulu olduğu donanım üzerinde çalışır. İzole edilen konuklara konteyner adı verilir. Her konteyner sisteminin kendi dosya sistemi, işlemleri, bellek alanı, cihazı ve ağ ara yüzü vardır. Aynı işletim sistemi içinde çalışsalar bile, konteynerlar birbirinden izole edilmiştir ve istemeden birbirleriyle iletişim kuramazlar. Her uygulama kendi konteynerinde izole olarak çalışır. Konteynerlar ve ana bilgisayar işletim sistemi arasındaki kaynakları izole etmek için Linux çekirdeği, "namespace" adı verilen bir özellik kullanır. Konteyner tabanlı sistemlerde, Kontrol Gruplarını (Cgroups) kullanarak kaynak kullanımını kısıtlamak, izlemek ve yönetmek mümkündür. Ayrıca Cgroups, bir konteyner içindeki tüm süreçleri sonlandırmak için güvenilir bir yol sağlar.[126]

2.1.11.1. Konteyner Tabanlı Sanallaştırma Örnekleri

Bu tür sanallaştırma örnekleri arasında Linux-VServer, OpenVZ, LXC (Linux Konteynerları), LXD, Docker, Kubernet ve Rocket bulunur.

- **Linux-VServer:** Linux için konteyner tabanlı sistemin en eski uygulamasıdır. Bu nedenle "namespace" özelliğini desteklememektedir ancak CPU, ağ ve süreç izolasyonu sağlamak için Linux çekirdeğinde kendi mekanizmalarını uygulamaktadır.[127]
- **OpenVZ:** OpenVZ, Virtuozzo tarafından sunulan ücretsiz ve açık kaynaklı sanallaştırma çözümüdür. Çekirdek namespace üzerine inşa edilmiştir ve farklı

[124] Miguel G. Xavier, Marcelo V. Neves, Fabio D. Rossi, Tiago C. Ferreto, Timoteo Lange, Cesar A. F. De Rose, *Performance Evaluation of Container-based Virtualization for High Performance Computing Environments*, 2013, 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, s.233-240 doi 10.1109/PDP.2013.41

[125] Zheng Li, Maria Kihl , Qinghua Lu and Jens A. Andersson, *Performance Overhead Comparison between Hypervisor and Container based Virtualization*,2017, College of Computer and Communication Engineering, China University of Petroleum, s.1-8.

[126] C. Gökhan, 2017, s.16.

[127] http://www.linux-vserver.org/Welcome_to_Linux-VServer.org Erişim Tarihi: 11.01.2021

bağlamlardan süreçler arasında izolasyon sağlamak için PID ve IPC ad alanlarını kullanır. OpenVZ altında çalışan bir sanal sistem 64 GB'a kadar belleği desteklemektedir. Bir OpenVZ çekirdeği aynı zamanda 100 sanal işletim sistemini de işleyebilmektedir.[128]

- **LXC (Linux Container):** LXC, tek bir Linux çekirdeği kullanarak bir ana bilgisayarda birden çok izole edilmiş konteyner çalıştırır. İki Linux çekirdeği özelliğine, yani "Cgroups" ve "namespace"e dayanmaktadır. Kaynak kullanımını izlemek ve yönetmek için Cgroups kullanır. Namespace ile LXC, konteyner ve ana bilgisayar işletim sistemi arasındaki kaynakları izole eder.[129]
- **LXD (The Linux Container Daemon):** LXD, bazı önemli özellikler eklenerek LXC (Linux Container'lar) teknolojisinin bir sonraki adımı olarak yorumlanabilir. Üç bileşenden oluşur: sistem çapında bir arka plan programı (lxd), bir komut satırı istemcisi (lxc) ve bir OpenStack Nova eklentisi (nova-compute-lxd).[130]
- **Rocket (Rkt):** Rkt, CoreOS tarafından Docker'a alternatif olarak geliştirilmiş bir konteyner sistemidir. Docker'dan farklı olarak systemd-nspawn konteyner yönetimi kitaplığını kullanır. "App Container" veya "app" spesifikasyonu olarak bilinen açık bir konteyner standardını temel alır. Bu, rkt görüntülerinin "uygulama" açık biçimini izleyen birçok konteyner sisteminde taşınabilir olmasını sağlar.
- **Docker:** Kodu ve tüm bağımlılıklarını paketleyerek uygulamanın bir bilgi işlem ortamından diğerine hızlı ve güvenilir bir şekilde çalışmasını sağlayan standart bir yazılım birimidir. Docker konteyner görüntüsü, bir uygulamayı çalıştırmak için gereken her şeyi içeren hafif, bağımsız, yürütülebilir bir yazılım paketidir: kod, çalışma zamanı, sistem araçları, sistem kitaplıkları ve ayarlar.[131]

Docker açık kaynaklıdır. Linux uygulamasını otomatik olarak dağıtmak için konteynerları kullanmaya güvenir. Kodlar, çalışma zamanı sistem araçları ve sistem kitaplıkları gibi tüm gereksinimler Docker konteynerlerine dahildir. Docker, 0.9 sürümüne kadar Linux konteyner (LXC) kitaplığını kullanmıştır, ancak bu sürümden sonra Docker, Linux çekirdeği tarafından sağlanan sanallaştırma yetenekleri için bir

[128] https://openvz.org/ Erişim Tarihi: 11.01.2021
[129] https://linuxcontainers.org/lxc/documentation/ Erişim Tarihi: 11.01.2021
[130] https://linuxcontainers.org/lxd/ Erişim Tarihi 18.01.2021
[131] https://www.docker.com/ Erişim Tarihi 14.01.2021

kitaplık konteyner kullanmaktadır. Yüksek düzeyli bir uygulama programı arabirimi (API) aracılığıyla yalıtılmış bir konteyner uygulamak için kullanır. Docker'da işletim sistemi (OS) gerekli değildir. Aynı Linux çekirdeği bir Docker konteyneri tarafından kullanılır, ancak kullanıcı alanını ana işletim sisteminden izole ederek gerçekleştirilir.[132]

Bu sanallaştırılmış uygulamalar, herhangi bir değişiklik olmaksızın her yerde kolayca çalıştırılabilir. Üstelik docker, aynı ekipman üzerinde farklı yeniliklerden daha fazla sanal durumu aktarabilir. İşleri bitirmek için docker, docker konteynerlerini kolayca dağıtmaya ve yönetmeye yardımcı olan üçüncü taraf araçlarla kolayca koordinasyon sağlayabilir. Docker konteynerları bulut tabanlı ortama kolayca dağıtılabilir.[133]

Docker, uygulamaları konteynerlara yerleştirildiklerinde otomatikleştirmek için bir tesis sağlar. Uygulamaların sanallaştırıldığı ve yürütüldüğü bir konteyner ortamında, docker bunun üzerine fazladan bir dağıtım motoru katmanı ekler. Docker'ın tasarlanma şekli, kodun verimli bir şekilde çalıştırılabileceği hızlı ve hafif bir ortam sağlamaktadır ve ayrıca, kodun bilgisayardan üretimden önce test edilmesi için bir kolaylık sağlar.[134]

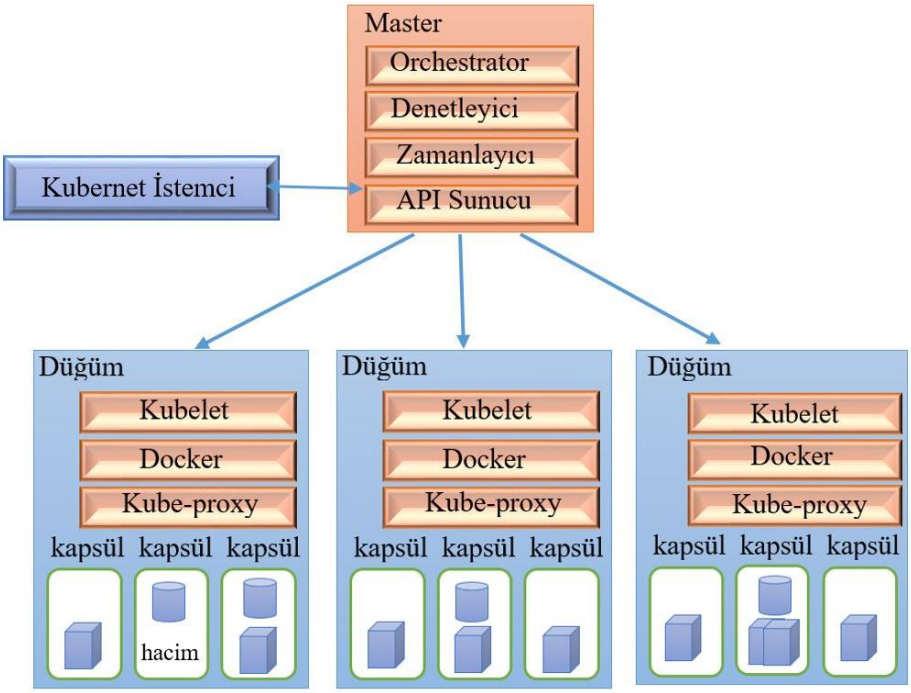
2.1.11.2. Kubernets

Kubernetler(K8) kapalı uygulamaların devreye alınmasına, yükseltilmesine ve yönetilmesine olanak tanıyan açık kaynaklı bir sistemdir. Bu platform uygulama konteynerlarına, bilgisayar kümelerine (cluster) ve sunucularda yükseltilmesine ve uygulanmasına olanak tanır. Bu açık kaynaklı yazılım, örneğin Docker gibi çok çeşitli konteyner teknolojileri ile çalışmaktadır.

Kubernet mimarisi Şekil 2.6'da gösterilmektedir. Bir donanım kümesine ait sunucular tarafından barındırılan konteynerları veya bir grup konteyneru olan kapsülleri (pods) görülmektedir. ETCD, yüksek bulunabilirlik, tutarlılık ve

[132] Carl Boettiger, "*An introduction to Docker for reproducible research, with examples from the R environmen*t", 2014, s.3-8
[133] Thanh Bui, "*Analysis of Docker Security*", Aalto University School of Science, 2015, arXiv preprint arXiv:1501.02967
[134] James Turnbull, "*The Docker Book: Containerization is the new virtualization*.",2019,s.10.-17

izlenebilirlik özelliklerine sahip dağıtık mimari ile tasarlanmış; tüm kümenin yapılandırma verileri için kalıcı depolama birimidir. Planlayıcının (scheduler) amacı, iş yükünü sunuculara paylaşmak ve böylece kapsüllerin yürütülmesini mümkün olan en iyi şekilde yönetmektir. Son olarak kubelet, her sunucunun yürütme durumundan sorumludur.



Şekil 2.19 : Kubernetes orkestratörünün mimarisi[135]

2.1.11.3. Konteyner Tabanlı Sanallaştırmanın Avantajları

Linux konteynerlarının talebi ve gelişimi son birkaç yılda görülebilir hale geldi. Konteynerlerın ana avantajları hız, taşınabilirlik, ölçeklenebilirlik, hızlı teslimat ve yoğunluktur.

- **Hız**

Hız, konteynerların en çok öne çıkan avantajlarından biridir. Konteynerları küçük olduğundan bir konteyner inşa etmek için gereken süre çok azdır. Ayrıca geliştirme, test ve dağıtım daha hızlı yapılabilir.

[135] Guy Pujolle, Software Networks: Virtualization, SDN, 5G and Securit, 2020, John Wiley & Sons, Inc., USA, s.8

- **Taşınabilirlik**

Konteynerların içinde oluşturulan uygulamalar son derece taşınabilirdir. Bu uygulamalar kolaylıkla taşınabilir ve performans aynı kalır. [136]

- **Ölçeklenebilirlik**

Çeşitli fiziksel sunucular, veri sunucuları ve bulut platformlarında dağıtılabilme yeteneğine sahiptir. Ayrıca her Linux makinesinde çalıştırılabilir. Konteynerlar, bir bulut ortamından yerel ana bilgisayara ve oradan da hızlı bir şekilde tekrar buluta kolayca taşınabilir. [137]

- **Hızlı Teslimat**

Konteynerların biçimi standartlaştırılmıştır, böylece programcılar birbirlerinin görevleri üzerinde strese girmek zorunda kalmazlar. Yöneticinin sorumluluğu, sunucuyu konteynerlara dağıtmak ve sürdürmektir, programcının sorumluluğu ise konteynerlerın içindeki uygulamalara bakmaktır. Uygulamaların içinde tüm gerekli bağımlılıklara sahip oldukları için konteynerler her ortamda çalışabilir. Konteyner ortamı güvenilir, tutarlı ve iyileştirilmiş bir ortam sağlar, böylece kodlar geliştirme, test ve üretim sistemleri arasında taşındığında tahmin edilebilir sonuçlar elde edilebilir.

- **Yoğunluk**

Konteyner, bir hiper yönetici kullanmadığı için mevcut olan kaynakları daha verimli kullanmaktadır. Sanal makinelere kıyasla tek bir ana bilgisayarda daha fazla konteynerin çalıştırılmasının nedeni budur. Kontneynerların performansı, daha yüksek yoğunluk ve kaynak israfı olmaması nedeniyle daha yüksektir.[138]

---

[136] Tuomas Vase, *Advantages of Dockers* , Information Systems Science, Lisans Tezi,2015,University of Jyväskylä, 2015, s.24

[137] Prof. Ann Mary Joy, Performance comparison between Linux containers and virtual machines. 2015, *International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College*, Ghaziabad, India, s.342-346

[138] Prof. A. M. Joy, 2015, s.342-346.

2.1.11.4. Konteyner Tabanlı Sanallaştırmanın Dezavantajları

Konteyner tabanlı sanallaştırma birçok açıdan sunduğu avantajları ön plana çıksa da mükemmel değildir. Konteyner ile ilişkili dezavantajlar şunlardır:

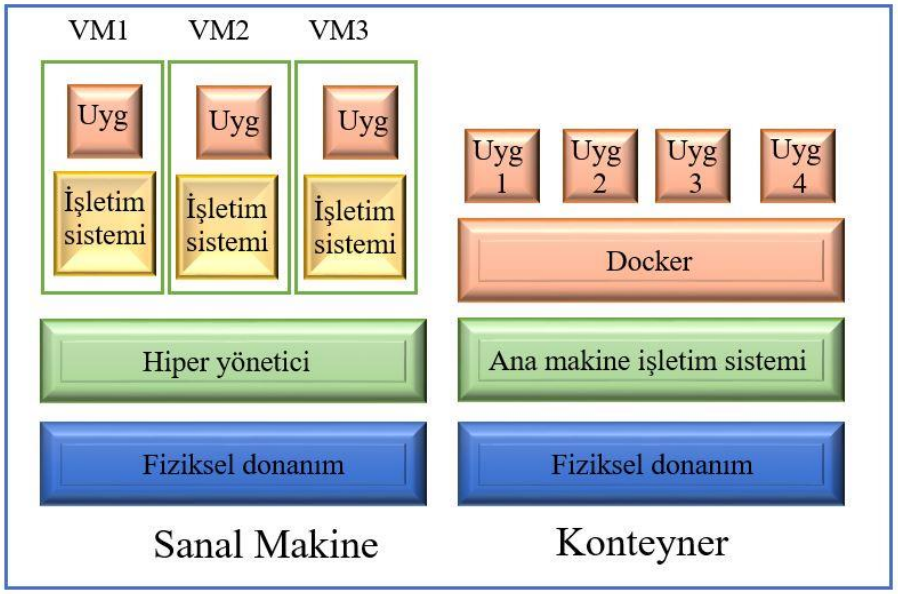
- Tam sanallaştırma konteyner tarafından sağlanmamaktadır çünkü Linux çekirdeğine bağlıdır. Konteynerlar eski makinelerde çalışmamaktadır. Yalnızca 64 bit yerel makineleri desteklenmektedir.
- Konteyner platformu açık kaynaklı olmasına rağmen, genellikle onları destekleyen şirketler arasındaki rekabet nedeniyle bazı konteyner ürünleri diğerleriyle çalışamaz. Örneğin, Red Hat'in hizmet olarak konteyner platformu olan OpenShift, yalnızca Kubernetes orkestratörü ile çalışır.
- Sanallaştırılmış ortamın tamamı, Windows ve Mac makineleri için konteynerlar tarafından tam performanslı bir şekilde sağlanamamaktadır. Boot2docker gibi araçlar bu boşluğu doldursa da kullanıcıları tarafından kabul edilmesine engel olup olmadığı veya ana makinenin işletim sistemi ile entegrasyon ve performansın yeterli olup olmadığı kontrol edilmelidir. [139]
- Konteynerler, kaynakları sanal makinelere göre daha verimli tüketseler de tip 1 hiper yönetici hızlarında çalışamamaktadırlar. Konteynerlar ağ oluşturma, ana bilgisayar sistemi arasındaki arabirim gibi nedenlerden dolayı performans ek yüküne maruz kalmaktadır.
- Kalıcı veri depolama birimleri karmaşıktır. Tasarım gereği, başka bir yere kaydedilmediği sürece, konteyner kapandığında içindeki tüm veriler sonsuza kadar kaybolur. [140]Docker Data Volumes gibi Docker'da verileri kalıcı olarak kaydetmenin yolları vardır, ancak bu ele alınması gereken bir sorundur.
- Grafik uygulamaları sanal makinelere göre iyi çalışmamaktadır. Çünkü konteynerlar, grafik arabirim gerektirmeyen sunucu uygulamalarını dağıtmak için bir çözüm olarak tasarlanmıştır.

[139] Ashif S. Harji, Peter A. Buhr, Tim Brecht, *Our Troubles with Linux Kernel Upgrades and Why You Should Care, Appears in: ACM SIGOPS Operating Systems Review*, Vol. 47, Issue 2, s. 66-72, 2013
[140] https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/containers-vs-vm Erişim Tarihi 13.01.2021

- Bir konteyner içinde bir GUI uygulamasını çalıştırmak için X11 video yönlendirme gibi kullanabilen bazı yaratıcı stratejiler olsa da, bu çözümler en iyi ihtimalle hantaldır. Tüm uygulamalar konteynerlardan yararlanmaz.
- Genel olarak, yalnızca bir dizi gizli mikro hizmet olarak çalışmak üzere tasarlanmış uygulamalar, konteynerlardan en iyi şekilde yararlanmaya hazırdır. Aksi takdirde, tek gerçek yararı, kolay bir paketleme mekanizması sağlayarak uygulama teslimini basitleştirebilmesidir.[141]

2.1.11.5. Sanal Makineler ile Konteynerler'ın Karşılaştırılması

Konteynerler ve VM'ler, benzer kaynak izolasyonu ve kaynak tahsisi avantajlarına sahiptir, ancak farklı şekilde işlev görür, çünkü konteynerler işletim sistemi bölümünü (en azından çekirdek bölümünü) içermez. Konteynerler ayrıca daha hafiftir, bu nedenle potansiyel olarak daha taşınabilir ve verimlidirler. Her konteyner için temel bir işletim sistemine ihtiyaç duyulmaz, ancak ayrı konyetnerler, paylaşılan Ana Bilgisayar İşletim Sisteminde çalıştırılır. Sanal makineler ve konteynerler Şekil 2.7'de gösterilmiştir.



Şekil 2.20 : Sanal makine ve konteyner kıyaslama

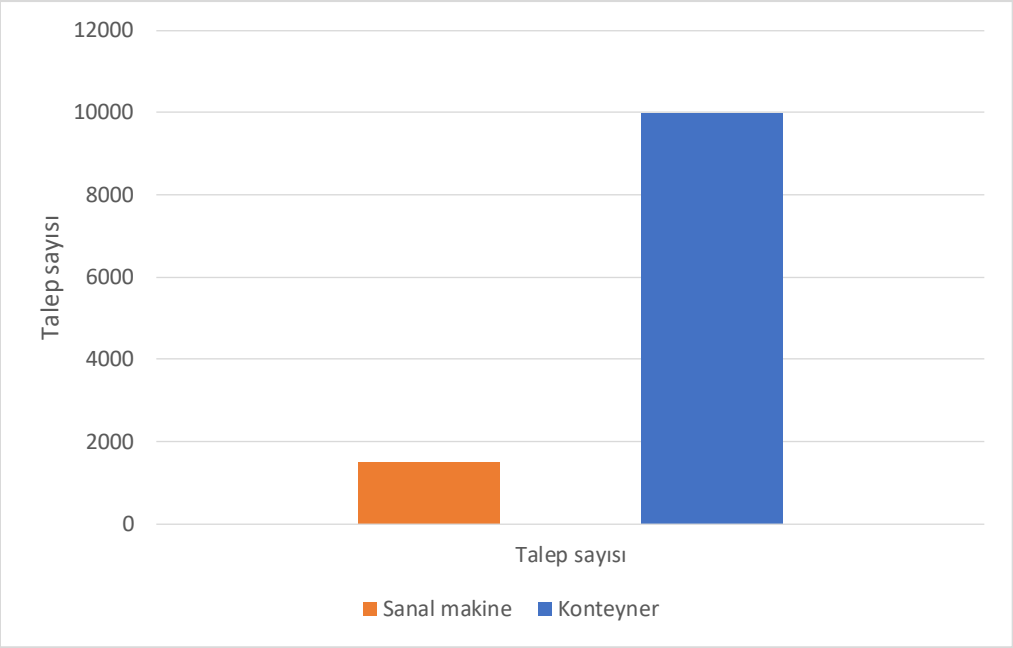
[141] Rajdeep Dua, A Reddy Raja, Dharmesh Kakadia, Virtualization vs Containerization to support PaaS, 2014, *IEEE International Conference on Cloud Engineering*, s.610-614 doi:10.1109/ic2e.2014.41

Ann Mary [142], ağ gecikmesi ve hata toleransı açısından sanal makineler ve konteynerlar arasındaki farkı ele almak için, tüm uygulama altyapısına odaklanarak makro karşılaştırmalar yapmıştır. Sanal makineleri ve Linux konteynerlarını uygulama performansını karşılaştırmak için AWS ec2 [143] bulutu ve iki fiziksel sunucu kullanılmıştır. Ec2 sanal makineler için her biri 2GB RAM'e sahip Ubuntu 14.04 işletim sistemi kullanılmıştır. Fiziksel sunucular ise Docker'ı barındırmak için kullanılmıştır. Uygulama performansı iki ortamdaki sanal makine ve konteyner ortamlarında çalışan aynı uygulama için (Joomla uygulaması) ölçülmüştür. Joomla uygulaması test verileriyle doldurulmuştur ve Jmeter yardımcı programı [144], sunucu performans sorunları yaşayana kadar Joomla uygulamasına aynı anda istek göndererek uygulamanın stres testi için kullanılmıştır.

600 saniyede JMeter, artan paralel talep hacmiyle olabildiğince çok isteği tamamlamaya çalışmıştır. Başlangıç zamanında t = 0ms, test yazılımı eşzamanlı bir istekle başlamakta ve sonraki isteği yalnızca önceki istek sona erdiğinde göndermektedir. Eşzamanlı isteklerin sayısı doğrusal olarak artırılarak 520 saniyeye kadar eşzamanlı olarak yaklaşık 80 isteğe ulaşmıştır.

Şekil 2.8, 600 saniye içinde başarılı olan isteklerin sayısını göstermektedir. Ayrıca, Docker konteynerinin 400 saniye içinde sanal makinenin üç katından çok daha fazla isteği işleyebildiğini göstermektedir. [145]

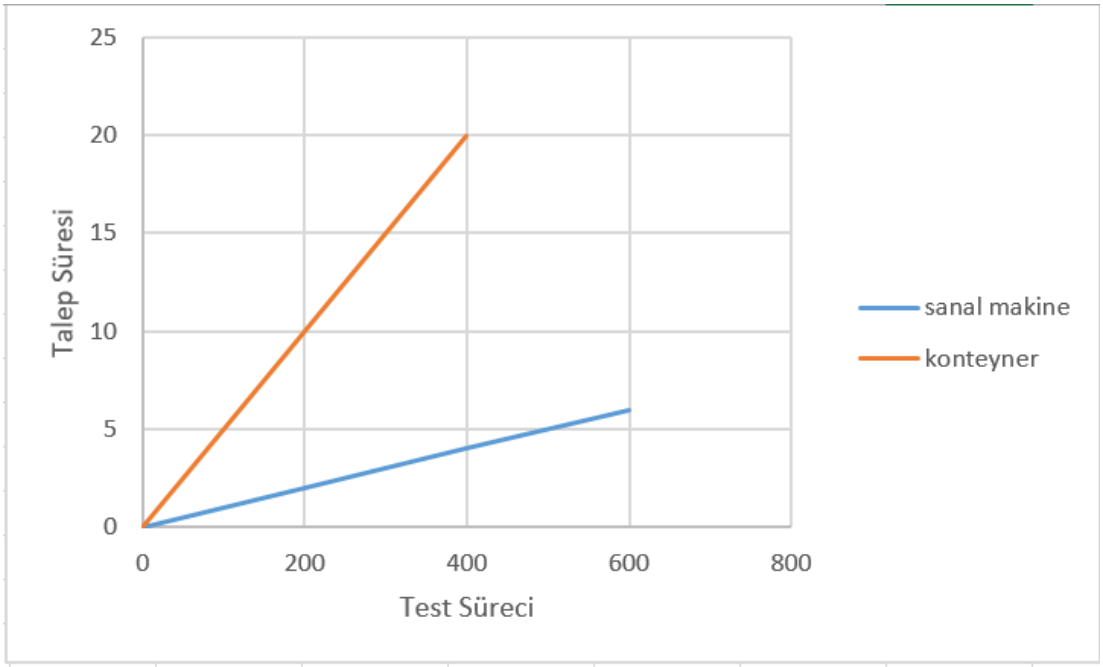
[142] A. M. Joy, 2015, s.342-346.
[143] Amazon Elastic Compute Cloud (Amazon EC2), bulutta güvenli, yeniden boyutlandırılabilen işlem kapasitesi sağlayan bir web hizmetidir. Geliştiriciler için web ölçeğinde bulut bilişimi kolaylaştırmak amacıyla Amazon tarafından tasarlanmıştır.
[144] http://jmeter.apache.org/ Erişim Tarihi: 07.02.2021
[145] A. M. Joy, 2015, s.345.



Şekil 2.21 : 600 saniyede işlenen talepler[146]

Şekil 2.9, sanal makinenin tek bir isteği bile işlemesinin daha fazla zaman aldığını göstermektedir. Veri noktaları arasına çizilen trend çizgisi ortalama 20 veri noktası alır. Ayrıca, erişilebilir fiziksel belleğe sahip olduğunda bile sanal makinenin Docker kadar tutarlı bir şekilde çalışmadığı görülmüştür. Bağlantı sayısı, sunucunun fiziksel bellek kullanımıyla başa çıkabileceğinden daha fazla arttığında, ana bilgisayar, sabit diski ile fiziksel bellek arasında bellek değiştirmeye başlamaktadır.

[146] A. M. Joy, 2015, s.346.



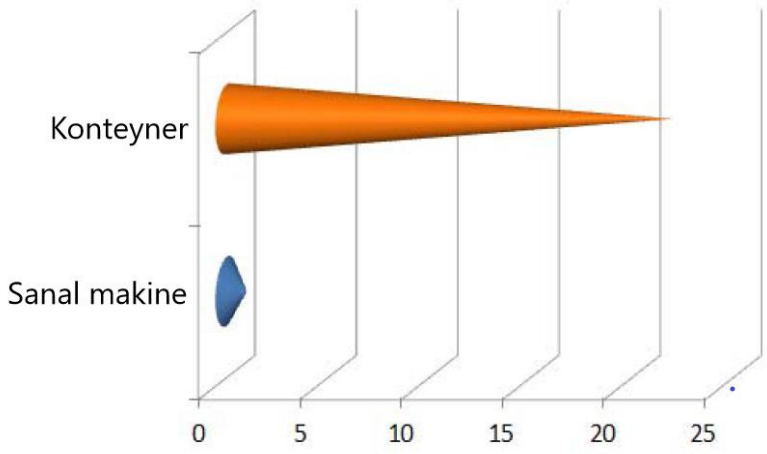
Şekil 2.22 : İlk 400 saniye için talep süresi[147]

Ann Mary, sanal makineler ile konteynerler arasında ölçeklenebilirlik karşılaştırması da yapmıştır; sanal makine ölçeklenebilirlik testi için AWS ec2 otomatik ölçeklendirme özelliği kullanmıştır. [148] Otomatik ölçeklendirme özelliği, maksimum CPU yüküne ulaştığında sanal makine örneklerini ölçeklendirmektedir. Linux konteynerı ölçeklenebilirliğini test etmek için kubernetes kümeleme aracı kullanılmıştır ve kubernetes kullanılarak docker ana bilgisayarına sahip iki fiziksel sunucu kümelenmektedir. Yapılan bu çalışmada hem sanal makine hem de konteyner ortamları yük dengeli bir WordPress uygulamasını çalıştırılmış ve Jmeter, sanal makineyi ölçeklendirmek için CPU kullanımını %80'in üzerine çıkararak ölçeklendirmeyi tetiklemek için kullanılmıştır.[149]

Sonuçlar, konteynerin hizmet talebini ölçeklendirmek ve işlemek için harcadığı sürenin, talebi işlemek için yeni bir sanal makineyi ölçeklendirmek için harcanan süreden çok daha az olduğunu göstermiştir. Sanal makinenin ölçeğini büyütmek için hesaplanan süre üç dakika sürmekteyken, bir konteynerin ölçeği büyütmesi ve isteği yerine getirmesi yalnızca sekiz saniye sürmüştür. Bu, ölçeklenebilirlik açısından

[147] A. M. Joy, 2015, s.346.
[148] https://aws.amazon.com/tr/autoscaling/ Erişim Tarihi : 08.02.2021
[149] A. M. Joy, 2015, s.345-346.

büyük bir farktır. Konteynerlr Şekil 2.10'da gösterildiği gibi sanal makinelerden ölçeklenebilirlikte 22 kat daha hızlı makineler olduğunu göstermiştir.[150]



Şekil 2.23 : Sanal makineler ve konteynerlar arasında ölçeklenebilirlik[151]

Bu çalışmada konteynerler, performans ve ölçeklenebilirlik açısından sanal makinelerden daha iyi performans göstermiştir. Daha iyi ölçeklenebilirliği ve kaynak kullanımı nedeniyle, konteynerlar kaynak ek yükünü azaltmak için uygulama dağıtımlarında kullanılabilir. Bununla birlikte, Docker gibi bir konteyner sanallaştırmaya geçmeyi düşünürken avantajları ve dezavatajları birlikte değerlendirmekte fayda vardır. Çünkü konteyner, uygulama dağıtımı için her zaman en iyi seçenek değildir. Bazı durumlarda, geleneksel sanal makineler veya fiziksel sunucular daha iyi çözümlerdir; sanal makinelerin Linux konteynerlarından daha uygun olacağı kullanım durumları vardır. Hem sanal makine hem de konteyner yaklaşımlarının artıları ve eksileri vardır, dolayısıyla birinin diğerinden üstünlüğü söz konusu değildir. Farklı iş yükleri, BT ve iş gereksinimlerini veya hedeflerini karşılamak için farklı altyapı platformları gerektirebilir.[152]

[150] Prof. A. M. Joy, 2015, s.342-346.
[151] a.g.m., s.344-346.
[152] Martin Gavanda, Andrea Mauro, Paolo Valsecchi, Karel Novak, *Mastering VMware vSphere 6.7*, Birmingham, Packt Publishing, second edition, 2019, s.13

2.2. SANALLAŞTIRMANIN KULLANIM ALANLARI

Sanallaştırma, bir dizi senaryoda yararlıdır. Günümüzde sanallaştırma artık her alanda kullanılmaktadır. Bu bölümde sanallaştırmanın bazı temel kullanımları anlatılmaktadır.

2.2.1. Sunucu Sanallaştırma Kullanım Alanları

- Sunucu konsolidasyonu: Donanım, yönetim ve altyapı yönetiminden tasarruf etmek için, yetersiz kullanılan birden çok makinenin iş yüklerini daha az makinede konsolide etmek için kullanılmaktadır.

- Performansa duyarlı iş yüklerinin paylaşımı: Birçok temel ve kritik iş yükünün yüksek performans ve kullanılabilirlik gereksinimleri vardır. Bu ihtiyaçları sürekli olarak karşılamak için, BT kuruluşları sıklıkla hassas iş yüklerini ayrılmış altyapıya dağıtır. Talebin zirve yaptığı anlarda performansı sağlamak için kaynaklar aşırı tedarik edilir. Olası arızalarla başa çıkmak için yedekli altyapı dağıtılır. Son olarak, ölçeklendirme, yeni sunucuların ve kaynakların satın alınmasını, yapılandırılmasını ve yönetilmesini gerektirir. Tüm bunlar, daha yüksek maliyetlere ve operasyonel verimsizliklere yol açmaktadır. İş yüklerinin performansını ve kullanılabilirliklerini sağlamak için bu alanda sunucu sanallaştırma teknolojisi kullanılmaktadır. Bu sayede paylaşılan, yüksek performanslı sanallaştırılmış bir ortam, fazlalıkları ortadan kaldırır, kullanımı artırır ve kolayca ölçeklenir.

- Geliştirme ve test ortamları: Geliştirme ve test ortamları, uygulama ve hizmetlerin oluşturulması ve iyileştirilmesi için kritik öneme sahiptir. Ancak, optimize edilmemiş altyapı, kaynakların geliştiricilere dağıtımını yavaşlatabilir ve tüm geliştirme döngüsünü geciktirebilir.

- BT altyapısını optimize etmek, kaynakları daha hızlı teslim etmeye yardımcı olabilmektedir. Kaynakların verimliliğini ve kullanımını artırmak, geliştirme ve test ortamı maliyetlerini takip etmek için de sunucu sanallaştırma kullanılmaktadır.

- Teknik iş istasyonları: Pek çok sektörde BT kuruluşları, yüksek performanslı grafik işleme ve hesaplama gücü gerektiren görselleştirme uygulamalarını desteklemek için teknik ve grafik yoğun iş istasyonları kullanır. Ancak, farklı

konumlara sahip masaüstü bilgisayarlar, yönetim ve güvenlik endişelerine neden olabilir. Bu iş istasyonu ortamlarını sanallaştırmak, yönetimi basitleştirmeye, erişim ve veriler üzerinde kontrolü yeniden kazanılmasına ve teknik iş istasyonu donanım maliyetlerini azaltılmasına yardımcı olmaktadır.

2.2.2. Depolama Sanallaştırma Kullanım Alanları

- Veri işlemleri: Depolama sanallaştırma, ofis uygulamaları, mail, sunuculardaki işlemler gibi aksiyonların yer aldığı tüm veri kümelerinin yedeklenmesi, geçmişe dönük istenilen verinin ulaşılabilmesi, verinin versiyon değişikliğinin yapılması, verinin saklanması, verinin eskitilmesi, verinin silinmesi gibi veri ile ilgili tüm işlemlerde kullanılmaktadır.

- Yazılım tabanlı veri merkezleri (SDDC): Yazılım tabanlı veri merkezine geçme noktasında temel ihtiyaçlardan biri de depolama sistemlerinin sanallaştırılmasıdır. Veri depolama sistemlerinin sanal katmanda yer alması ile birlikte donanım üreticisine bağımlık ortadan kalkmakta ve yazılım tabanlı olmanın getirmiş olduğu esneklik gibi avantajları sağlamaktadır.

2.2.3. Ağ Fonksiyonları Sanallaştırma Kullanım Alanları

Ağ fonksiyonları sanallaştırma (NFV), sabit ve mobil ağlar dahil olmak üzere çok çeşitli ağ işlevlerinde uygulanabilir. Bazı önde gelen NFV uygulamaları şunları içerir:

- Ağ sanallaştırma: NFV teknolojilerinin dünya genelindeki başlıca telekom şirketleri tarafından kullanıldığı ana kullanım ağ sanallaştırmasıdır. NFV donanımı yazılımdan ayırır. İşlem, fiziksel ağın üstünde bir sanal ağ oluşturur. Donanım ve yazılımın ayrıştırılması, hizmet sağlayıcıların hizmet kalitesini geliştirmesine olanak tanır. Ayrıca, kritik ağ gereksinimlerini iyileştirmeye yardımcı olmaktadır.

Kullanıcılar, ağ hizmetlerini optimize etmek için, DNS, önbelleğe alma ve güvenlik duvarı gibi ağ işlevlerini özel donanımdan ayırmak için ağ sanallaştırma teknolojisini kullanmaktadır.

Ağ sanallaştırma, servis sağlayıcılara yeni ağ hizmetleri kullanıma sunulurken ihtiyaç duyulan çevikliği ve esnekliği sağalmaktadır. Hantal fiziksel donanım harcamalarını ve çalıştırma, bakım ve zaman zaman tamir etme ile ilgili maliyetleri azaltmalarına yardımcı olmak amacıyla da kullanılmaktadır.

- Mobil uç bilgi işlem: Mobil uç bilgi işlem, son birkaç yılda gittikçe güçlenen bir başka teknolojik yeniliktir. Ağ işlevi sanallaştırmanın kullanılması, uç aygıtların hesaplama hizmetleri gerçekleştirmesine ve tek veya birden çok sanal makine (VM) oluşturup kullanarak ağ işlevleri sağlamasına olanak tanır. Multi-Access Edge Computing (MEC) bu teknolojilerin açık bir örneğidir. MEC, ultra düşük gecikme süreleri sağlamak için mobil uç bilişimi kullanmaktadır. Bu teknoloji, 5G ağlarının devam eden sunumlarından doğmuştur. MEC mimarisinde NFV'ye benzer bireysel bileşenler kullanmaktadır.

Mobil uç bilgi işlem; radyo kuleleri, mini veri ve yerel veri merkezleri gibi bileşenleri ifade eder. NFV, bu mobil ağ hizmeti işlevlerini donanımdan yazılıma çevirir.

- Orkestrasyon motorları: En faydalı NFV kullanım durumlarından biri, düzenleme motorlarıdır. Geleneksel eski ağlarla, düşük çeviklik, insan hatası ve otomatik süreçlerin ve uyarıların olmaması gibi sorunlar bu tür ağların yeteneklerini son derece sınırlı hale getirmiştir. Ağ kesintisinin en büyük nedenlerinden biri insan hatasıdır. NFV sistemi otomatik hale getirmek için kullanılmaktadır. Bu sistemler ayrıca, önemli ölçüde daha az insan müdahalesi gerektirdiklerinden, bakım ve onarım için maliyetleri azaltma avantajına da sahiptir.

- Video analizi: NFV'in diğer bir kullanım alanı da, video analiz sistemleri ve yazılımlarıdır. Artık fabrikalarda, mağazalarda, ofislerde kısacası günlük yaşamın her alanında kurulu olan IoT video ve akıllı cihazları kullanarak büyük miktarda veri yakalanmaktadır.

2.2.4. VDI Kullanım Alanları

- Çağrı merkezleri: VDI, çağrı merkezindeki çalışanların yalnızca görevlerini tamamlamak için gereken bilgi ve araçlara erişmesine izin verir. Bu, verimliliği ve maliyet etkinliğini kolaylaştırır.

- Sağlık hizmetleri: VDI, yönetim ekibinin bireysel sanal masaüstüne dayalı olarak kuralları ve izinleri özelleştirmesine olanak tanır. Özel izinler belirleyerek, her tıp uzmanı, yalnızca ilgili hasta kayıtlarını görmelerine izin veren kendi sanal masaüstüne sahip olabilir. Ayrıca, gün boyunca cihazdan cihaza geçebilir, sanallaştırılmış masaüstünü başlatabilir ve ihtiyaç duydukları kayıtlara erişebilirler.

- Uzaktan çalışma: VDI, ekip üyelerinin aynı şirket ağlarına, uygulamalarına ve kaynaklarına coğrafi olarak dağılmış durumdayken erişmesini sağlar, çünkü VDI'lerin tümü merkezi bir noktadan konuşlandırılabilir ve yönetilebilir.

- Mevzuata uygunluk: Çalışanlarının gizli bilgileri uygunsuz bir şekilde saklamasında sorunlarla karşılaşılmaktadır. Yönetimi VDI ile merkezileştirmek, verilerin ve uygulamaların yanlış depolanması sorununu ortadan kaldırmaya yardımcı olur.

- Eğitim kurumları: Bir okulda, öğrenciler öngörülebilir saatlerde binadadır ve kuruma yalnızca sınırlı bir süre devam ederler. Ayrıca, öğrencilerin okul tarafından sağlanan bilgisayarları ve dizüstü bilgisayarlarıyla yapabilecekleri ve yapamayacakları konusunda katı kısıtlamalara sahip olmaları gerekir. VDI ile BT ekibi, her öğrenciye kayıt süresi boyunca gerekli kısıtlamaları kendi sanal masaüstünü sağlayabilir. Daha sonra, BT ekibi mezun olduklarında sanal masaüstünü yalnızca birkaç tıklamayla silebilir.

- Üçüncü taraf erişimi: Bir yüklenici veya iş ortağından yararlanırken, bu çalışanların tüm sisteme bağlanmak için şirkete ait donanıma ihtiyacı vardır. VDI yüklenicilere donanım sağlamaya veya satın almaya gerek kalmadan şirket bilgilerine güvenli erişim sağlamak için ideal bir çözüm yapar.[153]

[153] https://www.ibm.com/cloud/blog/what-is-virtual-desktop-infrastructure Erişim Tarihi: 19.02.2021

VDI, çok sayıda sektördeki birçok işçi türü için önemli bir teknolojidir. Uzaktan ve mobil çalışanlar, yükleniciler, görev çalışanları, saha teknisyenleri, tıp uzmanları, öğretmenler ve diğerleri, bir veya daha fazla konumdan güvenilir bir sanal masaüstüne erişmek için VDI kullanmaktadır. VDI'nın farklı dağıtım türlerindeki çok yönlülüğü sayesinde, VDI teknolojisi, kullanıcıların standart, kalıcı olmayan masaüstüne erişmesi veya sanal masaüstünü son derece kişiselleştirilmiş bir dijital çalışma alanına dönüştürmesi için ortam sağlar.[154]

2.2.5. Servis Sanallaştırma Kullanım Alanları

Servis sanallaştırma, öncelikle bulut ve hizmet odaklı mimarilere bağlı uygulamaları veya üçüncü taraf verileri ve uygulama programı arabirimi (API'ler) ile iletişim kuran uygulamaları entegre etmek için kullanılır.

Geliştiriciler, bağımlı sistemin sanallaştırılmış bir kopyasını uygulayabilir, böylece entegrasyon test uzmanları uygulamalarının ne kadar iyi entegre olduğunu görebilmektedir. Bu, geliştirme ekiplerinin geliştirme süreci boyunca test ederek para ve zamandan tasarruf etmesini sağlamaktadır. Aksi takdirde, entegrasyonu test etmek için bağımlı sistemler kullanılabilir olana kadar beklemek gerekmektedir.[155]

2.2.6. Konteyner Sanallaştırmanın Kullanım Alanları

- Mikro hizmetler: Konteynerlar, sonsuz sayıda kullanım durumu için ayrıştırılmış süreçlere sahip olabilen karmaşık uygulamalar oluşturmak için mikro hizmetleri mümkün kılmaktadır.

- Konteynerler ve IoT: Konteynerlar, yazılımı kolayca dağıtılabilir taşınabilir paketler içinde sundukları için, IoT cihazlarında, özellikle de minimum işlem gücüne sahip olanlarda çalışan uygulamaları kurmak ve güncellemek için ideal bir araçtır. Sensöre özgü kitaplıklar, IoT cihazlarında uygulama taşınabilirliği sağlayan bir kapta uygulama ile birlikte paketlenebilir.

[154] https://www.citrix.com/tr-tr/glossary/vdi.html Erişim Tarihi: 22.02.2021
[155] https://searchservervirtualization.techtarget.com/definition/service-virtualization Erişim Tarihi: 22.02.2021

- Hizmet olarak Konteyner(CaaS): CaaS, konteyner motorlarının, düzenlemenin ve temeldeki bilgisayar kaynaklarının bir bulut sağlayıcı hizmeti olarak sunulduğu, konteyner tabanlı bir sanallaştırma biçimidir. DevOps ekipleri, herhangi bir konteyner alınmış uygulama için geliştirme sürecini daha fazla otomatikleştirebilir, böylece devreye alma ve üretime geçme süresini kısaltır.

- Sunucu Konsolidasyonu: Sunucu konsolidasyonu, veri merkezi ayak izlerini azaltarak, maliyetleri düşürerek ve diğerlerinin yanı sıra sunucu kapasitesini en üst düzeye çıkararak kuruluşlara sayısız avantaj sağlar. Sunucu konsolidasyonu elde etmenin bir yolu, konteynerler aracılığıyladır. Konteynerların birden fazla işletim sistemi bellek izleri yoktur ve kullanılmayan belleği örnekler arasında paylaşabilirler; bu da yoğun birleştirme olanağı sağlayabilir.[156]

2.2.7. Sanallaştırmada Bulut Bilişim Kullanımı

Sanallaştırma, bulut bilişimin temel bileşenidir. Sanallaştırmanın kullanımıyla birlikte, bulut bilişim, yalnızca kolaylık ve verimlilik avantajları sağlamakla kalmaz, aynı zamanda veri güvenliği ve gizlilik koruması alanında da büyük zorluklar getirir. Örneğin, farklı kiracıların sanal kaynaklarını aynı fiziksel kaynağa bağlayabilir, ardından kullanıcı verilerine diğer kullanıcılar erişebilir.[157]

Bulut bilişimde sanallaştırma, depolama sanallaştırma veya yazılım sanallaştırma yoluyla iki şekilde yapılabilir.

- **Depolama sanallaştırma:** Mevcut depolama, büyük sanal depolama erişimi elde etmek için sanallaştırılır ve ayrıca bulut istemcilere bellek ayırmak için kullanılır. [158]

[156] https://www.netapp.com/devops-solutions/what-are-containers/ Erişim Tarihi: 23.02.2021
[157] Yuping Xing and Yongzhao Zhan, Virtualization and Cloud Computing, Future Wireless Networks and Information Systems, Lecture Notes in Electrical Engineering book series v.143, Springer-Verlag Berlin Heidelberg 2012, s. 305–312,
[158] Pankaj Sareen, *Cloud Computing: Types, Architecture, Applications,Concerns, Virtualization and Role of IT Governance in Cloud*, International Journal of Advanced Research inComputer Science and Software Engineering ,3/3 (2013): 533-537

- **Yazılım sanallaştırma:** Şirket tarafından oluşturulan yazılım, sanallaştırma yardımıyla aynı anda çok sayıda sistem tarafından kullanılabilir. Yazılımın kurulduğu ve kullanıldığı sanal bir katman oluşturulur.[159]

[159]https://www.academia.edu/31096053/Cloud_Computing_Types_Architecture_Applications_Concerns_Virtualization_and_Role_of_IT_Governance_in_Cloud Erişim Tarihi: 23.02.2021

ÜÇÜNCÜ BÖLÜM

SANALLAŞTIRMADA SÜREÇ VE YÖNTEMLER, KULLANILAN YAZILIMLAR

3.1. SANALLAŞTIRMADA SÜREÇ VE YÖNTEMLER

Sanallaştırma teknolojisini başarılı bir şekilde uygulamak için ciddi bir planlama yapılması gerekmektedir. Planlama yapılırken göz önünde bulundurulması gereken temel nitelikler uygulamanın yönetilebilir, ölçeklenebilir, esnek ve güvenli olmasıdır. Ayrıca uygulamanın ihtiyaçlara da hızlı bir şekilde cevap verebilir olması bir diğer asli unsurdur. Bu bölümde söz konusu unsurlar göz önünde bulundurularak sanallaşma uygulamasının süreç ve yöntemleri ayrıntılı bir şekilde incelenecektir.

3.1.1. Sanallaştırmaya Geçiş Süreci

Sanallaştırmaya geçiş süreci hazırlık, etkinleştirme, bakım ve sürdürülme olarak kategorize edilebilecek üç temel adımdan oluşur.

3.1.2. Sanallaştırmaya Hazırlık

Sanallaştırmaya hazırlık aşamasında dikkat edilmesi gereken hususlar ve adımlar aşağıda özetlenmektedir:

- **Mevcut kurumsal bilişim altyapısı envanterinin çıkarılması:** Kurum öncelikli olarak sanallaştırmanın gerekli olup olmadığına karar vermeli, hali hazırdaki kurumsal envanterini çıkararak sanallaştırma altyapısına uygun olup olmadığını araştırmalıdır. Altyapının uygun olduğu konusunda bir fikir birliği varsa eksik kalan noktalar üzerine sanallaştırma tasarımı yapılarak projeye devam edilmesi uygun olacaktır.[160]

- **Kapasitenin planlanması:** Sanallaştırma teknolojilerine geçilmeden önce gerekli teknolojik araçlar kullanılarak bir kapasite planlaması yapılmalıdır.[161] Eğer bu kapasite planlaması başarılı bir şekilde yapılırsa işlemci, hafıza, disk ve iletişim ağı

[160] A. Öklü, 2013,s.50
[161] H. Yu, J. Guo, L. Wu, S. Wu, B. Peng, 2021 ,s.5-6.

gibi bilişim altyapı ihtiyacı net bir şekilde ortaya çıkacaktır. [162]Kapasite planlama hizmeti konusunda birçok üreticinin hazır yazılım ürünleri mevcut olduğu gibi, bu hususta çözüm sağlayıcılardan da hizmet alınabilmektedir. Ortaya çıkan kapasite planlama raporunun mevcut altyapıyla ne kadar örtüştüğünün değerlendirilmesi ve ihtiyacın bu ölçütler göz önünde bulundurularak gerçekleştirilmesi doğru olacaktır. [163]

- **Planlama sonrası yeni yatırım kararının alınması:** Mevcut altyapı potansiyelinin değerlendirilmesi sonucunda yeni yatırım ihtiyacı doğabilir. Bu ihtiyaç belirlenirken sanallaştırma yazılımı, disk, iletişim ağı cihazları bir bütün olarak değerlendirilmeli ve uygun topolojinin ortaya çıkarılması gerekmektedir. Ortaya çıkan çözüme ilişkin yatırım yapılmadan önce mutlaka daha küçük sistem bileşenleri ile çalışabilirliğinin test edilmesi gerekmektedir.

- **Fayda maliyet analizinin yapılması:** Sanallaştırma teknolojisine geçiş kararı verilmeden önce bir fayda ve maliyet analizi yapılmalıdır. Bu analiz yapılırken mevcut altyapı potansiyeli ve gelecekteki ihtiyaçlar öngörülerek kapsamlı bir değerlendirmeye gidilmelidir. Sunucu, disk, iletişim ağı, işletim sistemi ve enerji maliyetlerinde ne kadar kazanç sağlandığının yapılan analizlerde ayrıntılı olarak incelenmesi gerekmektedir.

- **Kapasite planlama raporunun oluşturulması:** Gerekli teknolojik araçlar kullanılarak yapılan kapasite planlaması bir rapor haline getirilmelidir. Planlamayı rapor haline getirebilecek birçok yazılım araçları mevcuttur. Bu yazılım araçları bir maliyet oluşturabilir. [164]

- **Sanallaştırma çözümünün alt yapıya uygunluğunun tespitine yönelik test çalışmalarının yapılması:** Sanallaştırma teknolojisine geçiş çalışmalarının hazırlık aşamasında tercih edilecek ürünlerin test edilmesi gerekmektedir. Bu kapsamda yapılacak testler de bir maliyet oluşturacaktır. Sanallaştırma alt yapısı hazırlandığı sırada ilgili teknik birimlerin rol ve sorumluluk alanlarına göre ihtiyaçları belirlenmelidir. Teknik

[162] H. Yu, J. Guo, L. Wu, S. Wu, B. Peng, 2021 ,s.6.
[163] Ahmet Öztürk, *Bilgi Teknolojisi Altyapılarının Yönetiminde Yeni Nesil Yaklaşımlar;Bilgi Teknolojileri ve İletişim Kurumu Altyapısına Yönelik Bir Model Önerisi*, Bilgi Teknolojileri İletişim Kurumu, Teknik Uzmanlık Tezi,2013 s.21
[164] A. Öklü, 2013, s.51.

birimlerce ürünlere karar verildikten sonra üst yönetimin ortaya çıkan topolojiyi değerlendirmesi ve toplam fayda maliyet analizi çerçevesinde yatırımın gerçekleştirilip gerçekleştirilmeyeceğine karar vererek projeye yön vermesi beklenir.

3.1.3. Sanallaştırmanın Etkinleştirilmesi

Altı adımdan oluşan sanallaştırma hazırlık çalışmaları tamamlandıktan sonra sanallaştırmanın etkinleştirilmesi aşamasına geçilmelidir. Sanallaştırma teknolojisinin etkinleştirilmesi çalışmalarında kurum sahip olduğu tüm bilişim hizmetleri unsurlarından faydalanmalıdır. Bu birimlerin birbirleriyle koordineli olarak çalışması önem arz etmektedir. Kurumda sistem yöneticileri çalışma alanlarında yer alan, disk ortamı, sunucu, işletim sistemleri ve sanallaştırma yazılımlarının kurulum çalışmalarını gerçekleştirmelidir. Ağ yöneticileri ise bu platformun üzerinde çalışacağı ağ topolojisini belirlemeli ve ilgili donanım ve yazılımlar üzerinde gerekli yapılandırmaları gerçekleştirmelidir. Tüm ağ aktif cihazlarının sorunsuz bir şekilde çalışıp çalışmadığı test edilerek gözden geçirilmelidir. Yazılım geliştirme birimleri sanal ortama geçiş sonrasında uygulama ortamlarında herhangi bir değişiklik yapılması gerektiği bir durum söz konusu olursa bu çalışmaları başlatmalıdırlar.

Sanallaştırmanın etkinleştirilmesi için bu aşamada aşağıdaki iş kalemlerinin sırasıyla uygulanması gerekir:

- Alınan donanımların çalışır vaziyette kurulması, montajlarının tamamlanması
- Aktif ağ cihazlarının kurulması ve donanımların mevcut çalışan sistemlerle ilgili protokoller üzerinden iletişimlerinin sağlanması
- Sunucular üzerinde sanallaştırma yazılımlarının kurulması ve yapılandırılması
- Sunucuların ve sanallaştırma yazılımlarının harici disk ortamındaki dosya sistemlerine erişimleri için gereken ayarların yapılması
- Sanallaştırma için gereken yönetim yazılımlarının kurulması ve tüm ortamı yönetecek şekilde bağlantılarının ayarlanması
- Mevcut fiziksel ortamdaki sunucuların, uygulamaların sanal ortama aktarılması

3.1.4. Sanallaştırmanın Bakımı ve Sürdürülmesi

Sanallaştırmanın etkinleştirilmesi aşamasından sonra kurumsal alanda kaynak etkin davranmak amacıyla hem yapısal hem de teknik bazı değişikliklere gidilmesi gerekmektedir. Yapısal anlamda, sanal ortamın daha az personelle idamesi mümkün olacağından ihtiyaç fazlası personel başka bölümlere kaydırılabilir. Bu durum insan kaynağının yeniden planlanmasıyla sonuçlanır.

Teknik açıdan ise, sanallaştırma ortamında iş anlamında devamlılığın sağlanması için süreçler adım adım tanımlanmalıdır. Bu konuda etkin bir geri bildirim mekanizması oluşturmak amacıyla yedekleme stratejilerinin iyi yapılandırılmış olması gerekir. Alınan yedeklerin ve anlık kopyaların geri dönüş senaryoları planlamalı ve bu senaryolar belirlenen periyotlarda test ortamlarında denenmelidir. Aynı zamanda sanallaştırma ile ilgili yazılım ve donanımların da önceden belirlenen periyotlarda bakımlarının yapılması gereklidir. Sunucuların, disk sistemlerinin ve ağ cihazlarının düzenli olarak monitör edilmesi oldukça önemlidir. Bu ihtiyaca yönelik olarak tüm donanımların durumlarını takip eden çeşitli yazılımların yapılandırılması ve log dosyalarının düzenli olarak takip edilmesi önem arz etmektedir. Sanallaştırma ortamında kullanılan tüm yazılımların güncelleştirmelerinin takip edilmesi ve test ortamında denendikten sonra canlı sistemde devreye alınmasına ilişkin süreçlerin tanımlanması oldukça önemlidir.

Sanallaştırmanın etkinleştirilmesi aşamasında ana maliyet kalemleri şu şekilde sıralanabilir:

- **Yedekleme:** Kurumun mevcut yedekleme sistemlerinin sanallaştırma sonrası oluşacak ihtiyaca cevap verip veremeyeceği araştırılmalıdır. Eğer bu durum yeni bir yatırım yapılmasını gerekli kılarsa yatırımı planlanan diğer bileşenler göz önünde bulundurularak gerekli önlemler alınmalıdır.
- **Destek ve yönetim:** Sanallaştırma sürecinde kapasite planlaması konusunda danışmanlık alınması ne kadar önemliyse projenin gerçekleştirilmesi ve idamesi hususlarında da destek alınması o kadar önemlidir. Bu süreç içerisinde yaşanacak sorunların çabuk ve etkin bir şekilde çözülebilmesi için destek

sürecinin çok iyi tarif edilmesi gerekmektedir. Bu konuda gerek üretici gerekse çözüm sağlayıcı destek sürecine dâhil edilmelidir.

- **Eğitim:** Sanallaştırma sürecine geçiş ile birlikte bu hizmeti sağlayan yazılım, disk, ağ ve sunucu sistemlerinde yeni teknolojilerin kullanımı gündeme gelebilir. Bu nedenle sanallaştırma geçişlerinde kullanılan yazılım ve donanım ürünlerine yönelik teknik personelin eğitilmesi ihtiyacı oluşabilir. Bu konuda birçok ürünün akredite edilmiş sertifikasyon ve eğitim hizmetleri mevcuttur.

Bu aşamada sanallaştırma sürecinin yönetimini kolaylaştıracak araçlar ise şunlardır:

- **Sanal makineleri tek bir konsoldan yöneten yönetim yazılımları:** Sanallaştırma sürecinin etkinleştirilmesinden sonra tüm sanal makineleri tek bir merkezden yöneten yazılımlar süreci yöneten teknik personele büyük kolaylık sağlamaktadır. Söz konusu yazılımlar sayesinde sanallaştırma sunucularıyla birlikte bunların üzerinde çalışan sistemlere doğrudan erişilerek etkin bir yönetim sağlanabilmektedir.
- **İzleme yazılımları:** Bu yazılımlar sayesinde sanal ortamdaki makineler ve donanımlar anlık olarak takip edilerek herhangi bir sorunla karşılaşılması durumunda otomatik uyarı sistemiyle sorunlara çabuk ve etkin bir şekilde müdahale edilebilmektedir.[165]
- **Yedekleme ve anlık kopya yaratma yazılımları:** Yedekleme ve anlık kopya yaratma yazılımları sanallaştırma süreçleri için çok önemlidir. Burada dikkat edilmesi gereken önemli bir husus yedekleme yazılımlarının sanal ortama uygunluğunun olmasıdır. Yedekleme yazılımları belirli periyotlar halinde geriye dönük olarak test edilmeli ve sanallaştırma alt yapısı harici disk kullanımını zorunlu hale getirmişse bu sistemlerin desteklediği teknolojilerden de faydalanılmalıdır.
- **Afet kurtarma için çözüm sağlayan yazılımlar:** Ciddi bir sorunla karşılaşılması durumunda sanal makinelerin kopyalarını alan yazılımlar

[165] https://pandorafms.com/tr/sanallastirma-izleme/ Erişim Tarihi:22.03.2021

sayesinde işleyen sisteme hızlı ve maliyet etkin bir geri dönüş sağlanabilmektedir.[166]

3.1.5. Süreç Konusunda Öneriler ve Uyarılar

Kurumsal olarak sanallaştırma teknolojisine geçiş ile ilgili bir düşünce olduğunda bu süreç teknik personel ve yönetim tarafından geniş bir perspektifte değerlendirilmelidir. Kurumun mevcut altyapısının sanallaştırma teknolojisine geçiş açısından uygun olup olmadığı derinlemesine araştırılmalıdır. Sanallaştırma süreci öncesinde kullanılacak sanal platform için kapasite konusunda planlamanın mutlaka yapılması ve bu konuda deneyimli personel bulunmaması durumunda danışmanlık hizmetinin de alınması gerekmektedir. Benzer projeleri başarıyla tamamlayan diğer kurum ve firma yöneticileri ve teknik ekipleri ile görüşmeler yapılarak geri bildirimler alınmalıdır.

Tüm bunlarla birlikte bilinmelidir ki, bazı fiziksel ortamlar sunucular üzerinde bulunan fiziksel kartlar nedeniyle sanallaştırılamamaktadır. Yine yüksek işlem hacmine sahip uygulamaların, veri tabanı sistemleri vb. hizmetlerin sanal teknolojiye geçirilmesinde başarı şansı düşük olabilmektedir.

Sanallaştırma teknolojisine geçmek kadar bu teknolojiyi kurumsal ve teknik olarak yönetebilmek de önemlidir. Bu alanda birçok ürün olduğu bilinmekle birlikte dosya yapılarını ve disk üzerindeki alanları anlayan, yük dengelerinin takibi, otomatikleştirme ve klonlama gibi yetenekleri olan araçları kullanmak fayda sağlayacaktır. Sanallaştırma ürünlerinin en belirgin özelliği fiziksel bir makineyi sanala, sanal bir makineyi de fiziksel bir ortama aktarabilmesidir.

Dosya yapıları arasındaki problemler nedeniyle sistemleri kendi aralarında taşımak soruna yol açabilir. Bu demektir ki bir sanallaştırma ürününün dosya kullanımı ile diğer bir sanallaştırma ürününün dosya kullanımı birbirinden farklıdır. Bu sorunu gidermek için de öncelikle sanallaştırma yapısı ortak bir alana çevrilmelidir.[167]

[166] A. Öklü , 2013, s.54.
[167] a.g.e., s.56.

3.2. SANALLAŞTIRMADA KULLANILAN YAZILIMLAR

Sanallaştırmada kullanılan yazılımlar genel olarak açık kaynak kodlu sanallaştırma yazılımları ile ticari yazılımlar olarak ikiye ayrılmaktadır.

3.2.1. Açık Kaynak Kodlu Sanallaştırma Yazılımları

Açık kaynak kod mantığı ve lisansı ile dağıtılan bu yazılımlar başlıca VirtualBox, Xen, Bochs, CoLinux, KVM ve QEMU olarak sıralanabilir.

- **Virtual Box**

VirtualBox, güçlü bir x86 ve AMD64 / Intel64 sanallaştırma ürünüdür. VirtualBox, GNU Genel Kamu Lisansı (GPL) sürüm 2 koşulları altında Açık Kaynak Yazılım olarak sunulan yüksek performanslı bir üründür. VirtualBox Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS / Windows 3.x, Macintosh, Linux (2.4, 2.6, 3.x ve 4.x), Solaris ve OpenSolaris, OS / 2 ve OpenBSD gibi birden çok işletim sistemini uygulama tabanlı çalıştırmakta ve bunlarla sınırlı olmamak üzere çok sayıda konuk işletim sistemini desteklemektedir. VirtualBox, sık sürümlerle aktif olarak geliştirilmektedir ve sürekli büyüyen bir özellik listesine ve desteklenen konuk işletim sistemlerine sahiptir.[168]

- **Citrix XenServer**

XenServer, alt yapısı itibari ile açık kaynak tasarımına dayanan ücretsiz bir sanallaştırma platformudur. Hem tam sanallaştırma hem de kısmi sanallaştırmayı desteklemektedir. XenServer, kolay sunucu kurulumu, veri depolama ve ağ kurulumu yapılmasına imkan tanımaktadır. Bunun yanında site yedekleme, yüksek kullanılabilirlik, otomatik iş yükü dengeleme, sunucular için güç yönetimi, bellek optimizasyonu gibi temel özellikleri barındırır.[169]

[168] https://www.virtualbox.org/ Erişim tarihi 07.02.2021
[169] https://www.citrix.com/ Erişim tarihi 08.02.2021

- **Bochs**

Bochs, en popüler platformlarda çalışan, C ++ yazılım dili ile yazılmış, taşınabilir bir açık kaynaklı IA-32 (x86) PC emülatörüdür. Intel x86 CPU öykünmesini, ortak I/O aygıtlarını ve özel bir BIOS'u içerir. Boch'lar, x86-64 Intel ve AMD işlemcilerine kadar pek çok farklı x86 CPU'ları taklit etmek için derlenebilir. Bochs, Linux, DOS veya Microsoft Windows dahil olmak üzere çoğu işletim sistemini çalıştırabilir. Bochs'lar, bazıları hala geliştirme aşamasında olan çeşitli modlarda derlenebilir ve kullanılabilir. [170]

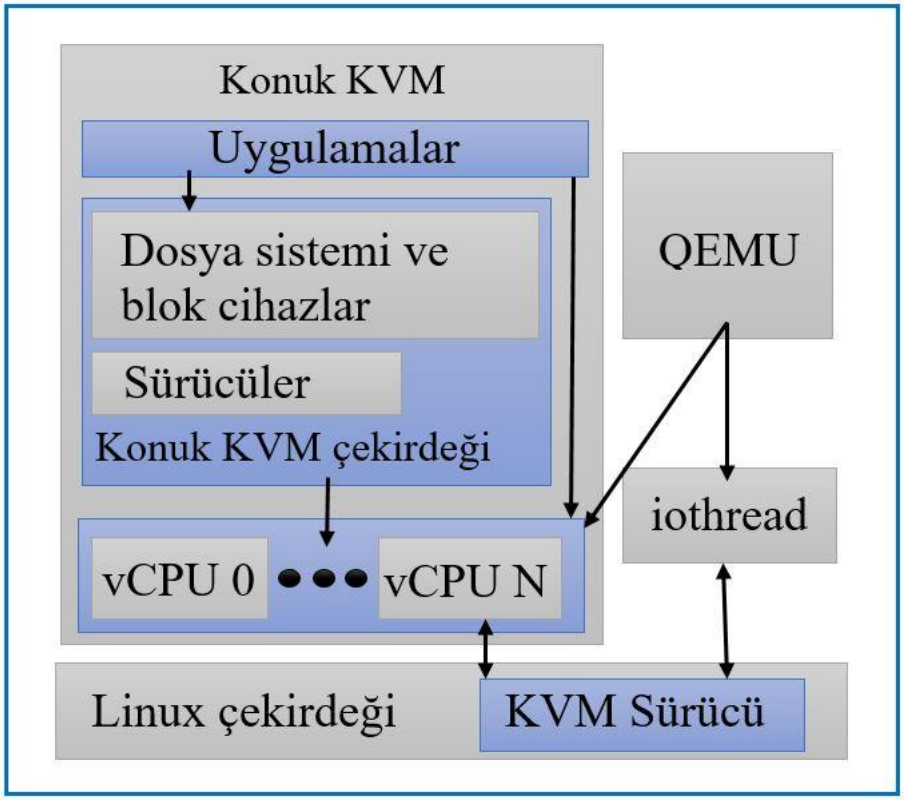
- **CoLinux**

CoLinux, Linux'u Microsoft Windows üzerinde yerel olarak çalıştırmak için kullanılan ücretsiz ve açık kaynaklı yöntemdir. Daha genel olarak ifade edersek CoLinux, Linux çekirdeğinin tek bir makinede başka bir işletim sistemi ile birlikte işbirliği içinde çalışmasına izin veren bir bağlantı noktasıdır. Örneğin, herhangi bir genel amaçlı PC sanallaştırma yazılımını kullanmaktan daha elverişli bir şekilde, VMware gibi ticari bir PC sanallaştırma yazılımı kullanmadan Linux'u Windows 2000 / XP / Vista / 7 üzerinde özgürce çalıştırma olanağı sağlar.[171]

- **Kernel-Based Virtual Machine**

KVM, sanallaştırma uzantıları (Intel VT veya AMD-V) içeren x86 donanımında Linux için tam bir sanallaştırma çözümüdür. Ancak, bazı cihazlar için KVM, kısmi sanallaştırma mekanizmasını da destekler. KVM kullanılarak, değiştirilmemiş Linux veya Windows görüntüleri çalıştıran birden çok sanal makine çalıştırılabilir. Şekil 3.1, KVM'nin mimarisini göstermektedir.[172]

[170] https://bochs.sourceforge.io/ Erişim Tarihi: 25.01.2021
[171] http://www.colinux.org/ Erişim Tarihi: 25.01.2021
[172] https://www.linux-kvm.org/page/Main_Page Erişim Tarihi: 25.02.2021



Şekil 3.24 : KVM Mimarisi[173]

Düşük maliyetli olması, doğrudan kernel ile etkileşime girebilmesi ve kendi çekirdeğini kullanması KVM'e avantaj sağlamaktadır. Temeli Linux'a dayandığı için SE Linux gelişmiş güvenlik sistemini kullanmaktadır. Bu yüzden son derece yüksek güvenliğe sahiptir.

KVM kullanmanın dezavantajları ise karmaşık kurulum sürecinin olması ve KVM sanallaştırmanın sadece belirli işlemcilerde mevcut olmasıdır.[174]

- **Qemu**

Bu sanallaştırma aracı, Linux ve Windows gibi işletim sistemlerinde sanallaştırmayı yürütmek için kullanılmaktadır. Dinamik çeviri yardımıyla hızlı bir emülasyon sunan açık kaynaklı emülatör olarak kabul edilmekedir. Qemu, çeşitli donanım mimarileri için başlıca açık kaynaklı araçtır.

[173] M. Chae, H. Lee, K. Lee, 2017, s.2-5.
[174] https://lwn.net/Articles/705160/ Erişim tarihi 14.12.2020

- **OpenVZ**

OpenVZ, Linux için açık kaynaklı konteyner tabanlı sanallaştırma aracıdır. Tek bir fiziksel sunucu üzerinde birden çok güvenli yalıtılmış Linux konteynerları çalıştırabilme özelliği sayesinde uygulamaların çakışmamasını sağlamaktadır. Her konteyner, tam olarak bağımsız bir sunucu gibi çalışır ve yürütülür; bir konteyner bağımsız olarak yeniden başlatılabilir ve kök erişimine, kullanıcılara, IP adreslerine, belleğe, işlemlere, dosyalara, uygulamalara, sistem kitaplıklarına ve yapılandırma dosyalarına sahiptirler.[175]

3.2.2. Ticari Sanallaştırma Yazılımları

Çeşitli ölçeklerde ücretli ve ücretsiz ticari sanallaştırma yazılımları bulunmaktadır. Ücretsiz ticari yazılımlar üzerinde birden fazla işletim sistemini çalıştırabilme, anlık görüntü alma gibi özellikler yer alırken kurumsal firmaların ihtiyaç duyacağı felaket kurtarma, yüksek kullanılabilirlik, canlı taşıma, depolama alanı taşıma gibi özellikler genelde bulunmamaktadır.

Ücretsiz ticari sanallaştırma yazılımlarının genel özellikleri şunlardır:

- Sanallaştırma platformu Windows vb. işletim sistemi üzerine kurulmaktadır.
- Windows, Linux vb. farklı işletim sistemlerini aynı anda çalıştırmaktadır.
- Anlık görüntü alabilme özelliği bulunmaktadır.

3.3.2.1. Ücretsiz Ticari Sanallaştırma Yazılımlarına Örnekler

- **VMware Player**

VMware Workstation Player, bir Windows, Sun Solaris veya Linux gibi işletim sistemlerinde tek bir sanal makine çalıştırmayı sağlayan bir yardımcı programdır.

[175] https://openvz.org/ Erişim Tarihi: 20.08.2020

Genellikle bu sanallaştırma çözümü öğrenciler ve eğitimciler tarafından eğitim amaçlı kullanılmaktadır.[176]

- **VMware ESXi Server**

Linux ve Microsoft Windows gibi birincil bir işletim sistemi aracılığıyla kullanılabilen ve ücretsiz olarak dağıtılan bir sanallaştırma platformudur.[177]

- **Microsoft Hyper-V**

Direk donanım üzerine kurulan bu yazılımda, canlı taşıma, anlık görüntü vb. özellikler bulunmaktadır.

3.3.2.2. Ücretli Ticari Sanallaştırma Yazılımlarına Örnekler

Ticari yazılımlar içerisinde giriş seviyesindeki ürünlerin yanı sıra, tüm sanal platformu yönetebilecek büyük kurumsal firmalara hitap eden tip 1 hiper yönetci ürünleri yer almaktadır.

Giriş seviyesindeki ticari yazılımlar şunlardır:

- VMware Workstation
- Vmware Fusion
- Parallels Desktop

Kurumsal firmalara hitap eden ticari yazılımlar şunlardır:

- Citrix Essentials for XenServer
- VMware vSphere
- Microsoft Windows Server 2008 R2 Hyper-V

[176] https://www.vmware.com/tr/products/workstation-player/workstation-player-evaluation.html Erişim tarihi 8.02.2021
[177] https://www.vmware.com/products/esxi-and-esx.html Erişim Tarihi: 20.08.2020

- Parallels Server

3.2.2.3. Ticari Sanallaştırma Yazılımlarının Sağladığı Özellikler

Ticari sanallaştırma yazılımlarının sağladığı birçok özellik vardır. Bu özellikler sayesinde sanallaştırma yazılımları verimlilik ve kullanılabilirliği yüksek seviyeye taşımıştır.

- **Donanım Üzerine Kurulabilme Özelliği**

Sanallaştırma yazılımı herhangi bir işletim sistemine gerek duyulmadan direkt donanım üzerine kurulabilmektedir.

- **Yönetim Yazılımları**

Yönetim yazılımları, sunucu üzerinde çalışan sanal makineleri ve kaynakları kolay bir şekilde yönetmeyi sağlar. Fiziksel sunucuların üzerinde çalışan sanal makinelerin ve tüm sanal platformun yönetimi için ayrı bir yönetim yazılımı kullanılmaktadır. VMware için vCenter Server, Citrix için Xen Center, Microsoft için System Center Virtual Machine Manager yazılımları kullanılmaktadır.

Yönetim yazılımlarının sağladığı kolaylıklar:

- Fiziksel sunucuların ve tüm sanal makinelerin durumlarının merkezi olarak denetlenmesi ve kaynak yönetimini basitleştirerek analizlerin yapılması,
- Fiziksel altyapılar, sanal ve hibrit bulutlar arasındaki tüm uygulamaların merkezi olarak yönetilmesi ve izlenmesi,
- Şablon özelliği sayesinde misafir işletim sistemlerinin çabuk bir şekilde oluşturulması,
- Veri kaybı yaşanmadan sanal makinelerin bir sunucudan diğerine hızlı bir şekilde taşınması,

- iSCSI, Fiber Channel SAN gibi farklı fiziksel depolama alanlarının yönetimi; ayrıca tüm depolama alanlarının vaziyetlerinin kontrol edilmesi,[178]
- Gerekli uyarı önlemlerinin, alarmlar tanımlanarak ayarlanması ve bu sayede güvenlik risklerinin minimum seviyeye indirilmesi,
- Muhtemel felaket senaryolarının, kolay bir şekilde test ortamı oluşturularak önceden tespit edilmesi,
- Felaket anlarında sanal makine kopyasını geri yükleyebilmek için fiziksel konumda depolanan bir sanal makinenin kopyasının oluşturulması,
- Sanal makinelerin anlık görüntülerinin alınması,
- Bir sanal makineye ve verilere kötü amaçlı yazılım ve diğer yetkisiz erişimlere karşı koruma sağlaması.[179]

- **Geniş Alanda İşletim Sistemini Destekleme**

Kurumsal sanallaştırma örneklerinde 32-bit ve 64-bit mimaride, Windows, Linux, Solaris gibi işletim sistemleri kullanılabilmektedir. Bu misafir işletim sistemleri eşzamanlı olarak çalıştırılabilmektedir.

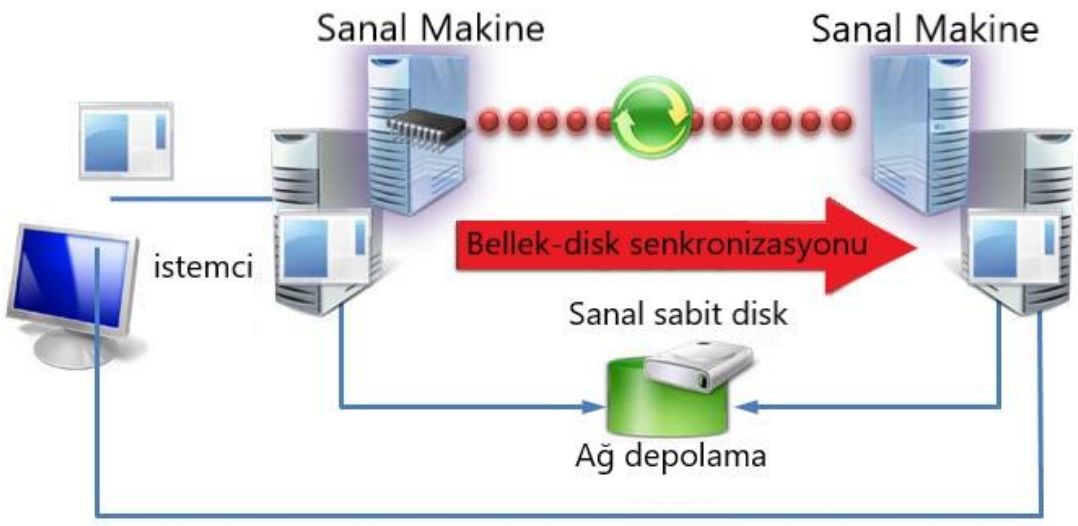
- **Canlı Göç**

Canlı göç, fiziksel sunucular üzerinde çalışan sanal makinalar çalışır durumdayken herhangi bir hizmet kesintisi olmadan farklı bir fiziksel sunucuya taşınmasını sağlayan teknolojidir. Bu teknoloji yük dengeleme, bakım ve güç yönetimi gibi çeşitli senaryolarda veri merkezleri için özel avantaj sağlar.[180]

[178] A. Öklü, 2013, s.45
[179] T.Merdan,2010,s.27
[180] Anja Strunk, *"Costs of Virtual Machine Live Migration: A Survey" Chair of Computer Networks Faculty of Computer Science* ,Technical University of Dresden, Germany, 2015, s.1-4.

Canlı göç teknolojisi sunucu göçü dışında depolama alanında yeterli alan kalmaması durumunda sanal makine dosyalarını farklı bir LUN ya da datastore üzerine aktarılabilme olanağı tanımaktadır.

Canlı göç, iki ana bilgisayar arasında gerçekleşmektedir. Burada, VM belleği iki ana bilgisayar arasında kopyalanır. Bellek kopyalandıktan sonra, yeni ana bilgisayardaki VM, sanal sabit disk (VHD) dosyalarına erişebilir ve çalışmaya devam edebilir. Her iki ana bilgisayar da sanal makinenin VHD dosyalarının depolandığı paylaşılan depolamaya erişir. Şekil 3.2'de gösterildiği gibi dinamik geçiş başlatıldığında, aşağıdaki adımlar gerçekleşir:



Şekil 3.25 : İki ana makine arasında canlı geçiş[181]

1. Hedef sunucuda yeni bir VM yapılandırma dosyası oluşturulur.

2. Kaynak sanal makinenin başlangıç bellek durumu hedefe kopyalanır.

3. Kaynak VM'de değiştirilen bellek sayfaları etiketlenir ve hedefe kopyalanır.

4. Bu işlem, değiştirilen sayfa sayısı azalana kadar devam eder.

[181]http://activedirectoryservice.blogspot.com/2011/06/hyper-v-live-migration-step-by-step.html Erişim Tarihi 24.03.2021

5. VM, kaynak düğümde (source node) duraklatılır.

6. Son bellek durumu, kaynak sanal makineden hedefe kopyalanır.

7. VM hedefte devam ettirilir.

8. Ağ yönlendirme tablolarını güncellemek için bir ARP [182] yayınlanır ve migration işlemi tamamlanır.

- **Sistem Çalışırken Backup Alma İşlemi**

Bu teknoloji ile sanal makinelerde herhangi bir ajan kurulumuna gerek duyulmaksızın hizmet kesintisinde bir aksaklık yaşanmadan yedeklenme sağlanmaktadır. Yedekleme sırasında veriler sıkıştırılarak depolama alanından tasarruf edilmektedir. Ayrıca yüksek performans ile kurumsal düzeyde kısa sürede yedekleme ve yedekten geri dönme işlemi yapılmaktadır. Kısa aralıklarla alınan yedekleme sayesinde olası bir felaket senaryosunda ek avantajlar sağlamaktadır.[183]

- **Anlık Görüntü Kullanma**

Anlık görüntü özelliği kısa süreli çalışmalar öncesinde ya da sunucu üzerinde riskli bir güncelleme yapılması gerektiğinde yedek almak yerine anlık görüntü özelliği kullanılabilir. Anlık görüntü, anlık görüntü alındığı anda sanal makinenin tüm disklerin durumu, bellek durumu ve sanal makine ayarları kısaca sanal makinenin tüm durumunu yakalar. Anlık görüntüye geri dönüldüğünde, tüm bu öğeleri anlık görüntüyü aldığı sırada bulundukları duruma döndürülebilir. [184]

Anlık görüntü özelliği en çok sanal makinenin durumu korunmak istendiğinde kullanışlıdır; böylece kısa sürede tekrar tekrar aynı duruma dönüş sağlanabilir. Anlık görüntü, sanal makina açık veya kapalı durumdayken alınabilir.[185]

---

[182] ARP: Adres Çözümleme Protokolü: Internet Protokolü adresinin (IP adresi) yerel ağda tanınan fiziksel makine adresine eşlenmesi için kullanılan bir protokoldür.
[183] Peter Chi-Hsiung Liu, Soubir Acharya, *System and Method For Virtualizing Backup Images*, Jan 1 2013, US Patent : 8,346,726 B2
[184]https://www.vmware.com/support/ws4/doc/preserve_anlık görüntü_ws.html Erişim Tarihi 21.02.2021
[185] David Marshall vd., 2006, s.513-517

- **Kaynak Havuzları**

Farklı seviyelerde kaynak havuzları oluşturularak kaynaklar ihtiyaçlar doğrultusunda ilgili sunuculara aktarılabilmektedir. Fiziksel makinelerdeki kullanım yoğunluğuna göre sanal makineler otomatik olarak kaynakları daha iyi olan sunucular üzerine aktarılabilmektedir. [186]

- **Çeşitli Fiziksel Depolama Alanlarını Yönetebilmesi**

SAN büyük miktarda depolama ortamını (TeraByte) işleyebilir, depolama kaynaklarının bir paylaşımını sağlayabilir ve gerçek zamanlı, hızlı ve kolay veri erişimi sağlar. iSCSI, depolama ortamını ve ağ hizmeti aracılığıyla veri aktarımını bağlamak için bir ortam olarak internet protokolünü kullanan bir depolama ortamı konseptidir.[187] Bu fiziksel depolama birimleri fiziksel sunucunun depolama alanlarına bağlı kalmadan kullanılabilmektedir. Depolama alanlarının kullanım durumu kontrol edilebilmekte ve ihtiyaç halinde depolama alanları eklenerek mevcuttaki depolama alanlarının boyutu arttırılabilmeklerdir. Kümeleme (cluster)[188] özelliği sayesinde birden fazla fiziksel sunucu tarafından depolama alanı ortaklaşa kullanılabilmektedir.[189]

- **Kendini Yöneten Sistem**

Sanallaştırma yazılımları genel olarak kullanıcı tarafından yapılandırılabilen bir olay ve alarm alt sistemi içerir. Bu alt sistem, altyapıda meydana gelen olayları izler ve verileri günlük dosyalarında depolar. Bu alt sistem ayrıca alarmların hangi koşullar altında tetikleneceğinin belirlenmesini sağlar. Sistem koşulları değiştikçe alarmlar, durumu hafif uyarılardan daha ciddi uyarılara değiştirebilir ve otomatik alarm eylemlerini tetikleyebilir. Bu işlevsellik, operasyonel yanıt verebilirlik hızı sunarak, dinamik bir BT ortamı oluşturulmasını sağlamaktadır. [190]

---

[186] A. Öklü, 2013,s.49.
[187] M. T. Abdullah , S. Qidri , W. Nuryadi , S. R. Widianto, 2020, s. 89-96.
[188] Cluster mimarisi ya da cluster yapısı: Belirli konfigürasyonlar ile yapılandırılarak aynı amaç için birlikte ya da yedekli çalışan sunucu kümeleridir.
[189] A. Öklü, 2013,s.49.
[190] https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-9272E3B2-6A7F-427B-994C-B15FF8CADC25.html Erişim Tarihi: 22.02.2021

Sanallaştırma yazılımları, makinenin fiziksel durumu, üzerinde çalışan sanal makinelerin işlemci, bellek durumları, hostlar arasındaki cluster yapısı gibi birçok objeyi kontrol edip tanımlanan alarmların gerçekleşmesi durumunda uyarı mesajı gönderme, mail atma, sunucuyu kapatma, açma gibi fonksiyonları yerine getirerek kendi kendini yönetebilir.

Örneğin, belirli bir ana bilgisayar kümelerindeki tüm sanal makinelerin CPU kullanım oranları alarmlar ile yönetilebilir. Sanal makinenin CPU kullanım oranı 5 dakika boyunca %75 'ten yüksek bir değere ulaşırsa uyarı durumuna düşmesi, %90 değerine ulaşması durumunda hata durumuna düşmesi tanımlanabilmektedir. [191]

- **Yüksek Kullanılabilirlik Özelliği**

Fiziksel sunucular arasındaki cluster yapısı sayesinde sunuculardan herhangi birinde sorun oluşması durumunda, sorunlu makine üzerinde çalışan misafir işletim sistemleri diğer sunucular üzerinde çalıştırılabilmektedir.

- **Felaket Kurtarma Özelliği**

Yüksek kullanılabilirlik sadece cluster yapısında meydana gelen bir sorunu çözmeye yardımcı olurken, potansiyel olarak kritik iş verilerini bir fidye yazılımı saldırısından veya verilerin bir son kullanıcı tarafından yanlışlıkla veya kasıtlı olarak silinmesinden koruyamaz. Bu tür bir saldırı veya bir felaket senaryosunda felaket kurtarma özelliği devreye girer. Felaket ya da olağanüstü durum kurtarma, kuruluşların başka şekilde yok edilen verileri yeniden oluşturma olanağına sahip olmalarına olanak tanır. Bu, yalnızca sanal makinelerde bulunan verilerin yeniden oluşturulmasını değil, aynı zamanda sanal makinenin kendisini tamamen yeniden oluşturabilmeyi de içerebilir.

[191] A. Öklü, 2013, s.49.

DÖRDÜNCÜ BÖLÜM

SANALLAŞTIRMADA BİLGİ GÜVENLİĞİ VE SANAL SİSTEMLERE YÖNELİK TEHDİTLER

4.1. SANALLAŞTIRMANIN BİLGİ GÜVENLİĞİ ÜZERİNDEKİ ETKİLERİ

4.1.1. Bilgi Güvenliği ve Bilgi Güvenliği Yönetimi

Bilgi güvenliği, bilgi ve bilgi altyapısı varlıklarının kayıp, kötüye kullanım, ifşa veya hasar risklerine karşı korunmasıyla ilgili faaliyetleri tanımlar.[192] Bilgi güvenliği yönetimi, bir kuruluşun varlıkların gizliliğini, kullanılabilirliğini ve bütünlüğünü tehditlerden ve güvenlik açıklarından makul bir şekilde koruduğundan emin olmak için uygulaması gereken kontrolleri tanımlar. BGY'nin hedefi, bir kuruluşun varlıkların yönetimi ve korunmasında gereken risklerin değerlendirilmesini ve risklerin tüm uygun paydaşlara yayılmasını içeren bir süreç olan bilgi riski yönetimini içerir.[193]

Bilgi Güvenliği Yönetimi, bir sistem için yaşam döngüsü süreçlerinin önemli bir parçasıdır ve bu süreçler:

- Sistem konsepti ve tasarımı,
- Sistem geliştirme,
- Konuşlandırılmış sistemlerin çalışması,
- Sistemin devre dışı bırakılması (aktif bir sistemin kaldırılması),
- Sistem konseptinin ve tasarımının başlangıcından itibaren güvenlik hususlarının dahil edilmesi,
- Güvenlik teknolojisinin kullanımı (güvenlik duvarları (FW), kripto, SIEM, yama, vb.)

---

[192] Ercan Buğra Tokdemir, *An Information Security Management System Approach And Technical Security Best Practices For The Enterprise Companies*, Bahçeşehir Üniversitesi, 2019, s.6

[193] Tony Campbell, *Practical Information Security Management: A Complete Guide to Planning and Implementation,*2016,Australia,Apress, Chapter 1: Evolution of a Profession,s.1-14, ISBN 9781484216859.

- Güvenlik sürecinin aktif olarak yönetilmesi,
- Kişiler (geliştiriciler, kullanıcılar, bilgisayar korsanları) olarak tanımlanabilir.[194]

4.1.2. Bilgi Güvenliği Yönetim Sistemi

Bir bilgi güvenliği yönetim sistemi (BGYS), bir kuruluşun genel bilgilerini güvende tutmak amacıyla gerekli politikaların ve prosedürlerin oluşturulmasını ve uygulanmasını sağlamak için benimsenen sistematik bir yaklaşımdır.[195] Bu sistem tipik olarak kuruluşun ihtiyaçları, hedefleri, güvenlik gereksinimleri, boyutu ve süreçlerinden etkilenir. Bir BGYS, etkili risk yönetimi ve azaltma stratejilerini içerir. Ek olarak, kuruluşun BGYS'yi benimsemesi, büyük ölçüde bilgi güvenliği risklerini sistematik olarak tanımladığını, değerlendirdiğini, yönettiğini, bilgi gizliliği ve bütünlüğü ile kullanılabilirlik gereksinimlerini başarılı bir şekilde ele alabileceğini gösterir. Bununla birlikte, ilgili insan faktörleri BGYS geliştirme, uygulama ile BGYS'nin nihai başarısını en iyi şekilde sağlamak için de dikkate alınmalıdır.[196]

BGYS'nin temel konsepti, bilgi erişilebilirliğini etkin bir şekilde yönetmek için tutarlı bir süreç ve sistem tasarlamak, uygulamak ve sürdürmektir. Ayrıca bilgi varlıklarının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak ve bilgi güvenliği risklerini en aza indirmektir. BGYS'nin kapsamı, şirket üst yönetiminin katılımıyla gerçekleştirilen Bilgi Güvenliği Komitesi (ISC) tarafından şirketin bilgi güvenliği gereksinimleri ve yasal gereklilikler doğrultusunda belirlenmektedir. [197] Bilgi güvenliğinin sağlanmasında ilk adım gizliliğin, bütünlüğün, kullanılabilirliğin ve varlıkların değiştirilmesinin değerlendirilmesi dahil olmak üzere uygun varlık tanımlama ve değerleme adımlarını gerektirir.[198] Kuruluşlar bilgi güvenliği ile ilgili

[194] E. B. Tokdemir, 2019, s.7.
[195] Arhnel Klyde S. Terroza, *"Information Security Management System (ISMS) Overview"*, The Institute of Internal Auditors, 12 Mayıs 2015, https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information Security Management System (ISMS) Overview.pdf Erişim Tarihi 24.03.2021
[196] https://en.wikipedia.org/wiki/Information_security_management#cite_note HumphreysImplement16-3 Erişim Tarihi:24.03.2021
[197] E. B. Tokdemir, 2019, s.8.
[198] Harold F Tipton, Micki Krause, *Information Security Management Handbook*, 5th edition,(ISC)[2] press, 2006, s.183-189 ISBN 0-8493-9561-5

ISO / IEC 27001, ISO / IEC 27002 ve ISO / IEC 27035 standartlarında bulunan bir bilgi güvenliği yönetim sistemini ve diğer ilgili standartları uygulayabilir.[199]

4.1.3. İlgili Standartlar

Kuruluşların tehditleri ve güvenlik zafiyetlerini azaltmak amacıyla Türkiye'de ve Dünyada kabul görmüş ve yaygın bir şekilde uygulanan standartlar arasında ISO / IEC 27000 standartlar ailesi, ITIL çerçevesi, COBIT çerçevesi ve O-ISM3 2.0, PCI-DSS bulunur. Bu standartlar en iyi bilgi güvenliği yönetim sistemlerini kurmak, uygulamak, dağıtmak, izlemek, gözden geçirmek, sürdürmek, güncellemek ve iyileştirmek için gereksinimleri ortaya koyarlar.[200]

ISO / IEC 27001, bilgi güvenliği yönetim sistemleri için gereksinimleri sağlar. ISO / IEC 27001'in odak noktası, ağırlıklı olarak belirli bir kuruluşun kontrolü altındaki ortamlarda bilgi güvenliği ve ilişkili risklerdir. Siber güvenlik, kurumsal sınırların ötesine geçebilen ve varlıkların bilgi paylaştığı, dijital olarak etkileşime girdiği ve siber güvenlik olaylarına yanıt verme sorumluluğuna sahip olduğu birbiriyle bağlantılı bir dijital ortam olan siber uzaydaki risklere odaklanır.[201]

IEC, toplu olarak "elektroteknoloji" olarak bilinen tüm elektrik, elektronik ve ilgili teknolojiler için uluslararası standartları hazırlayan ve yayınlayan uluslararası bir standartlar kuruluşudur. [202]

ITIL, yalnızca birkaç yönden ISO / IEC 27001'den farklı olarak, bilgi teknolojisi altyapısının, hizmetinin ve güvenliğinin etkin yönetimi için kavramlar, politikalar ve en iyi uygulamalardan derlenerek oluşturulmuş bir kütüphane olarak ifade edilmektedir.[203]

---

[199] Edward Humphreys, *Implementing the ISO/IEC 27001:2013 ISMS Standard*, 2016, Artech House. s. 11–26, ISBN 13: 978-1-60807-930-8

[200] https://en.wikipedia.org/wiki/Information_security_management#cite_note-HumphreysImplement16-3 Erişim Tarihi:24.03.2021

[201] https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en Erişim tarihi 17.12.2020

[202] https://www.iec.ch/what-we-do/how-iec-funded Erişim tarihi 17.12.2020

[203] Mehmet Tuygun, *ISO27001 Bilgi Güvenliği Yönetim sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği*, Yüksek Lisans Tezi, Gazi Üniveristesi,2019

ISACA tarafından geliştirilen COBIT, bilgi güvenliği personelinin olumsuz etkileri en aza indiririp bilgi güvenliği ve risk yönetimini kontrol ederken bilgi yönetimi ve yönetişim için stratejiler geliştirmesine ve uygulamasına yardımcı olan bir çerçevedir. O-ISM3 2.0, Open Group'un kurumlar için teknolojiden bağımsız bilgi güvenliği modelidir.[204]

4.2. SANALLAŞTIRMADA BİLGİ GÜVENLİĞİ SORUNUNUN İNCELENMESİ

Sanallaştırma, ilk olarak BT kaynaklarını merkezileştirmeye ve bütünleştirmeye yardımcı olur, merkezi veri depolama, verilerin yedeklenmesini kolaylaştırır, fazlalıkları önler ve kontrolü iyileştirir. Ayrıca BT düzenlemelerine ve yönetimine uyumu kolaylaştırır. İkinci olarak, sanallaştırma, sunucuların sayısını azaltmaya yardımcı olur ve bunu yaparak, güç ve soğutma altyapısının kullanımını azaltma eğilimindedir. Azalan sunucu sayısı ve güç kullanımı, yalnızca BT yönetiminin verimliliğinin baskısını hafifletmekle kalmaz, aynı zamanda küresel yeşil enerjiye yönelik yaygın eğilime de uygundur.

Bahsedilen bu faydalarla, sanallaştırmanın uygulanması veya benimsenmesi ile ilgili olarak ele alınması ve çözülmesi gereken birçok sorun vardır. Ele alınması gereken en önemli konulardan biri sanal makineler ve sanallaştırılmış ortamlarla ilgili güvenlik zafiyetleridir. [205] Bu zafiyetlerin önlenmesi amacıyla sanallaştırılmış ortamlarda uygun güvenlik düzeylerine ulaşmak gerekmektedir. Bunun için de aşağıda belirtilen kapsamdaki maddelerin tümü güvence altına alınmalıdır.

1. Sanal makine işletim sistemi: Bilgi güvenliği organizasyonun VM işletim sistemi için belirlediği en iyi uygulamalar kullanılarak güvenli hale getirilmelidir. Sanal makine işletim sisteminin güvenliğinin sağlanamaması, aynı zamanda bir ağ tehlikesi olasılığını da önemli ölçüde artırabilir. Bunun nedeni, bir kez güvenliği ihlal

[204] https://en.wikipedia.org/wiki/Information_security_management#cite_note-HumphreysImplement16-3 Erişim Tarihi : 24.03.2021
[205] Steven J. Vaughan-Nichols, *Virtualization sparks security concerns*, Computer 41 (8), 2008, 13–15, doi:10.1109/mc.2008.276

edildiğinde, VM işletim sistemi ağa yönelik saldırılar için kolayca bir sıçrama tahtası görevi görebilmesidir.

2. VM ağları: Harici olarak başlatılan tüm VM ağ bağlantıları, uygun şekilde yapılandırılmış, bakımlı bir güvenlik duvarı ile korunmalıdır. Ek olarak, daha önce de belirtildiği gibi, VM'deki işletim sistemi uygun şekilde güvenli hale getirilmelidir.

3. VMkernel'in güvenliğini sağlama: VMkernel, doğası gereği son derece güvenlidir. VMkernel'in herkese açık uygulama programlama arayüzleri (API) olmadığından, bu önemli yazılımın bir saldırgan tarafından ele geçirilme ihtimali çok düşüktür; ancak imkânsız değildir. VMKernel'in güvenliğini sağlamak için düzenli bir şekilde kurumun bilgi güvenliği politikasına uygun olarak güncellemelerinin ve yamalarının yapılması gerekmektedir.[206]

4. VM sunucusunu VM sunucusu trafiğine ve VMkernel trafiğine karşı koruma: Sunucular arasındaki iletişim, her bir VM ana bilgisayarını yönetmeye yardımcı olmak ve performans dengelemesini kolaylaştırmak için VM sunucuları arasında bellek verilerinin geçmesini sağlar. VMkernel ağı ayrıca NFS bağlantıları ve iSCSI erişimini gerçekleştirmek için de kullanılır. Veriler şifrelenmemiş olarak aktarılır ve bundan dolayı bu verileri geçiren ağa erişim her zaman kontrol edilmelidir.

5. Konsol işletim sistemi: COS, VMkernel'in donanıma ve VM disk dosyaları için veri depolarına erişime sahiptir. COS bu nedenle bir başka önemli güvenlik meselesidir. En azından, yönetici olmayan sanal makinelerin COS ağına erişimi olmamalıdır. Bu, olası saldırı başlangıç noktalarını sınırlayacaktır.[207]

6. VM Dağıtımı: COS ağ bağlantısını kullanan VM'leri dağıtmak için birçok farklı araç vardır. Tipik olarak bu araçlar, şifrelenmemiş bilgileri hedef VM

[206] Edward Ray, Eugene Schultz, - *Virtualization security, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies*- CSIIRW '09, 2009, s.1–5, doi:10.1145/1558607.1558655
[207] E. Ray, E. Schultz, 2009, s.5.

sunucusuna gönderir. Bu tür trafiğin AES[208] gibi güçlü şifreleme standardı ile şifrelenmesi sağlanarak dağıtım ağının güvenliği sağlanmalıdır.

7. VM yedekleme: Tipik olarak VM'ler iki yoldan biriyle yedeklenir. Birincisi, VM'nin ağ bağlantılarını kullanan VM içinden yedekleme yapmaktır. İkinci yöntem VMware Consolidated Backup gibi harici olarak COS aracılığıyla yapılır. Her iki durumda da, ağ üzerinden geçen yedekleme verileri güçlü şifreleme ile şifrelenmeli; yedekleme sunucusu erişim kimlik doğrulaması ve dosya koruması açısından yeterince güvenli olmalıdır.[209]

8. Veriler: Sanallaştırılmış ortamlardaki veriler, bir veri merkezinin korunması gerektiği şekilde korunmalıdır. Her bir VM birbirinden ayrı ve farklı olmasına rağmen, COS servisi, VM Sunucusunun bir parçasıdır ve kritik verilerin erişimine sahiptir. Düzgün yapılandırılmış ACL'ler[210] ve en az ayrıcalık ilkesinin uygulanması, veri güvenliği ihlalleri olasılığını en aza indirecektir.[211]

Ayrıca, hizmet konsolunu bir kurumun ağına uygun şekilde yerleştirmek de bir zorunluluktur. Hizmet konsolu, dışarıdan başlatılan saldırılara daha kolay bir şekilde saldırabileceği bir DMZ[212] ağının dışında tutulmalıdır. Bir güvenlik duvarının onu bu tür saldırılardan koruduğu bir ağ içindeki bir noktaya yerleştirmek, güvenlik açısından çok daha iyidir. Birleştirilmiş denetim günlüğü çıktısının düzenli ve sistematik olarak incelenmesini gerektiren prosedürlerle yeterli denetimin sağlanması da önemlidir. Ayrıca güvenliğin sağlanması için gerekli önemli bir diğer konu ağın izlenmesidir. Bu nedenle nihai hedef, ihtiyaç duyulduğu kadar önleyici koruma sağlamak ve aynı zamanda sistem uygulamalarının çalışması üzerinde minimum etkiyle işletim sisteminin denetlenmesine ve izlenmesine izin vermek olmalıdır.

---

[208] AES (Advanced Encryption Standard; Gelişmiş Şifreleme Standardı): Uluslararası alanda defacto şifreleme (kripto) standardı olarak kullanılmakta olan elektronik verinin şifrelenmesi için sunulan bir standarttır.

[209] E. Ray, E. Schultz, 2009, s.5-6.

[210] ACL(Access Control List; Erişim Kontrol Listesi): Bir sistem kaynağı ile ilişkili izinlerin bir listesidir. ACL, hangi kullanıcılara veya sistem işlemlerine nesnelere erişim izni verildiğini ve belirli nesnelerde hangi işlemlere izin verildiğini belirtir.

[211] E. Ray, E. Schultz, 2009, s.6.

[212] DMZ(Demilitarized Zone): Bir kuruluşun dışarıya bakan hizmetlerini içeren ve internet gibi güvenilmeyen, genellikle daha büyük bir ağa maruz bırakan fiziksel veya mantıksal bir alt ağdır. Bir DMZ'nin amacı, bir kuruluşun yerel alan ağına (LAN) ek bir güvenlik katmanı eklemektir.

Güvenliğin sağlanmasında ağ güvenlik duvarları, uygulama güvenlik duvarları, güçlü kimlik doğrulama, anti-virüs ve casus yazılım önleme araçları, hata toleransı veya diğer mekanizmalar, DoS koruması, adli araçlar, uzaktan günlük kaydı, periyodik güvenlik açığı taramaları ve yama yönetimi gibi araçlar da etkilidir. [213] Son araştırmalar ve çalışmalar, bilgi güvenliği ile ilgili olarak sanallaştırmanın hem zorlu hem de faydalı yönlerini ortaya çıkarmıştır.[214] Bilgi güvenliği sorununun incelenmesi ve öneriler Tablo 4.1'de özetlenmiştir.

Tablo 4.1 : Bilgi güvenliği sorunu incelemesi[215]

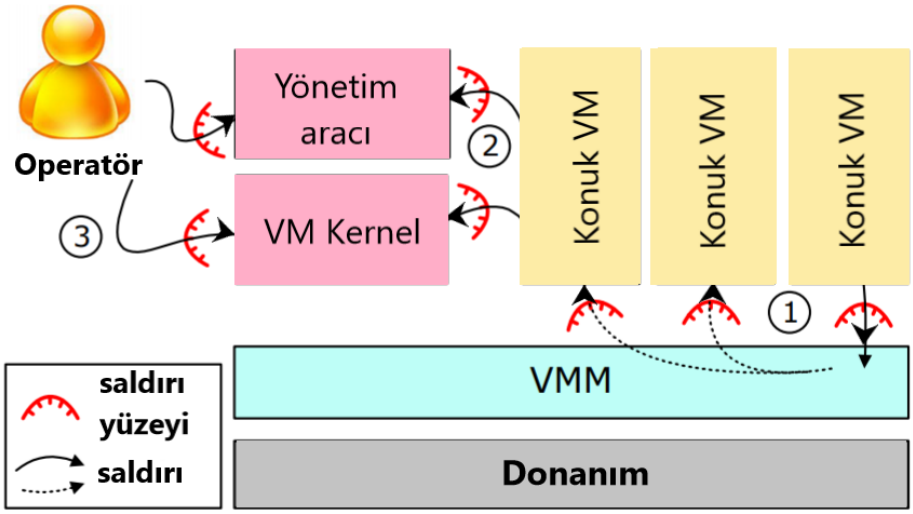
Bilgi güvenliği sorunu	Öneriler
İş ağı güvenliği	Ağ güvenliği araçları, yazılımları ve ürünleri: İnternet ve intranet güvenliğini artırmak için güvenlik araçları, ürünleri veya yazılımları kullanılabilir. Sanal Özel Ağ (VPN): Çevrimiçi kaynaklara VPN aracılığıyla uzaktan erişilebilir.
İşletme verilerini koruma	Sabit disk ve dosya düzeyinde şifreleme: Diskleri veya dosyaları şifrelemek için şifreleme araçları veya yazılım kullanmak, bir sızıntı durumunda verileri yetkisiz erişimden koruyabilir. Bilgi sızıntısının önlenmesi: Bir bilgi sızıntısı izleme sistemi kurmak, düşmanca gizli dinlemeyi ortaya çıkarabilir ve / veya önleyebilir. Veri tabanı güvenlik kontrolü: Verilerin şifrelenmesi ve veri tabanı erişiminin denetlenmesi, güvenlik ihlali olasılığını azaltabilir.
Kurumsal personel tanımlama ve erişim kontrolü	Personel tanımlama yönetimi: Kimlik tanımlama ve şifre yönetimi politikası oluşturulması önerilmektedir.

[213] E. Ray, E. Schultz, 2009, s.5-6.
[214] S. J. Vaughan-Nichols, 2008, s.13–15.
[215] S. Li, D. C. Yen, S. Chen, P. S. Chen, W. Lu, C. Cho, 2015, s.2-5.

	Kullanıcı kimlik doğrulama hizmeti: Çoklu oturum açma veya akıllı kart kimlik doğrulaması gibi yöntemler uygulanabilir. Web sitesi kullanıcı kimlik doğrulaması: Sistemlerin yalnızca yetkili kullanıcının içeriğe erişmesine izin vermesi ve bilgisayar korsanlığı kaynaklı tehditleri önlemek için tek oturum açma kullanması önerilir.
Güvenlik denetimi, uygulaması ve standartları	Bir bilgi sızıntısı izleme sistemi kurmak, düşmanca gizli dinlemeyi ortaya çıkarabilir veya önleyebilir. Verilerin şifrelenmesi ve veri tabanı erişiminin denetlenmesi, güvenlik ihlali olasılığını azaltabilir.
Uygulama ve platformların güvenliği	Personel tanımlama yönetimi: Kimlik tanımlama ve şifre yönetimi politikası oluşturulması önerilmektedir. Kullanıcı kimlik doğrulama hizmeti: Çoklu oturum açma veya akıllı kart kimlik doğrulaması gibi yöntemler uygulanabilir. Web sitesi kullanıcı kimlik doğrulaması: Sistemlerin yalnızca yetkili kullanıcının içeriğe erişmesine izin vermesi ve bilgisayar korsanlığı kaynaklı tehditleri önlemek için tek oturum açma kullanması önerilir.
Bilgi güvenliğine yönelik tehditler	Kötü amaçlı yazılım, virüsleri, Truva atlarını, casus yazılımları, bilgisayar solucanlarını, rootkit'leri ve reklam yazılımlarını içerir. Korsanlık araçları ve püf noktaları: Bilgisayar korsanları her zaman yeni saldırı araçları, yolları ve teknolojileri geliştirmektedir. Uygulama düzeyinde saldırılar: Artık pek çok bilgisayar korsanı, OS düzeyindeki saldırılardan arabellek taşması ve siteler arası komut dosyası saldırılarına yönelmiştir.

4.3. SANAL SİSTEMLERE YÖNELİK GÜVENLİK TEHDİTLERİ

Birçok faydasının yanında sanallaştırma teknolojilerinin getirdiği bazı güvenlik zafiyetleri vardır. Sanallaştırma sisteminde kullanılan yazılım katmanı ya da donanımlar güvenlik tehditlerine maruz kalabilir veya saldırılara uğrayabilir. [216] Teknik olarak sanallaştırma, yeni saldırı senaryolarının ortaya çıkmasını sağlamıştır. Birincisi, sanal bir makine fiziksel bir makineye eşdeğerdir ve kontrolü ele geçirmeye istekli bir saldırgan her iki durumda da aynı araçları kullanabilir. Öte yandan, bir sanallaştırma katmanının eklenmesi, bir saldırgana hedefini altüst etmenin yeni yollarını sağlayabilir. Aslında, Şekil 4.1'de gösterildiği gibi, tip 2 hiper yönetici için, sanallaştırma katmanındaki güvenlik açıkları, bir sanal makineden başka bir VM'ye, VMM'ye veya ana bilgisayar işletim sistemine yönelik saldırıların gerçekleştirilmesine izin verebilmektedir.[217]



Şekil 4.26 : Sanal makine yüzeyine saldırı[218]

Tip 1 hiper yönetici için de bu durum benzerdir, ancak hiper yöneticinin altında ana bilgisayar işletim sistemi yoktur, bu nedenle karşılık gelen saldırı yüzeyi de

[216] Mert Doğukan SOYER, Sanallaştırmada Güvenlik Açıkları, Tehditleri ve Bunların Çözümleri, 2021, Proje Raporu, s.8

[217] Ivan Studnia, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Vincent Nicomette, *Survey of Security Problems in Cloud Computing Virtual Machines*, Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012), Cloud and security:threat or opportunity, 2012, Rennes, France, s. 61-74. ffhal-00761206f

[218] Fengzhe Zhang, Jin Chen, Haibo Chen and Binyu Zangfeng, *"CloudVisor : Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization,"* in Proc. SOSP, 2011, pp. 203–216.

kaldırılır. Herhangi bir sistem yönetim aracı varsa, bunlar da potansiyel bir saldırı vektörü olarak kabul edilir.[219]

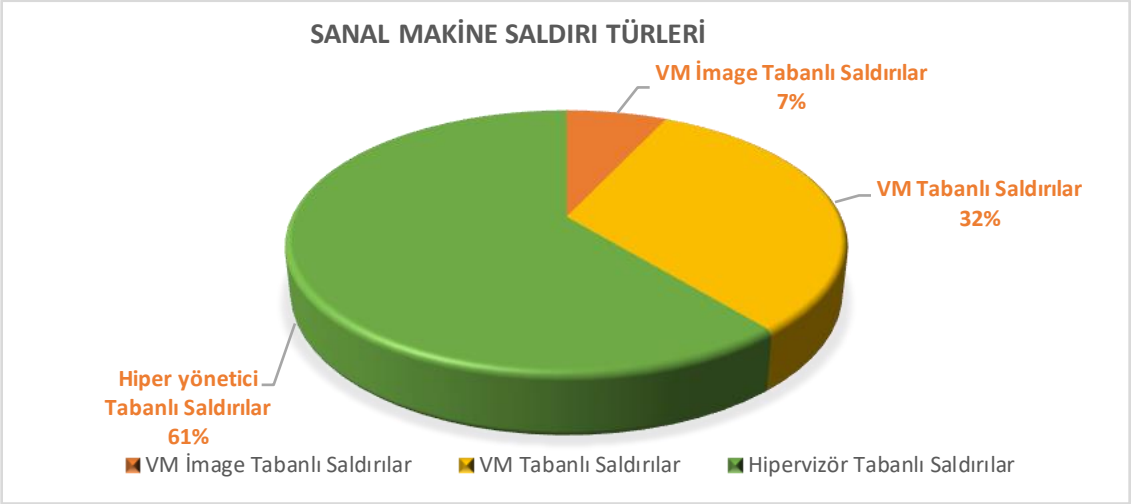
Sanallaştırma teknolojisi ile birlikte güvenlik altına alınması gereken yeni bir katman eklenmiştir ve saldırganlar bu katmanı kullanarak sistemlere sızabilmektedir. Fiziksel ana makine güvenliği tehlikeye girerse, söz konusu ana makinede bulunan tüm VM'ler ve uygulamalar etkilenir. Ayrıca, güvenliği ihlal edilmiş bir sanal makine, fiziksel sunucuda hasara yol açabilir ve bu, aynı makinede çalışan diğer tüm VM'ler üzerinde olumsuz bir etkiye sahip olabilir. Dolayısıyla, sanal makine güvenliği, fiziksel makine güvenliği kadar önemlidir. Sanallaştırılmış ortamlar da normal altyapılara yönelik her türlü saldırıya karşı savunmasızdır. Bununla birlikte, sanallaştırma ile daha fazla giriş noktası ve daha fazla ara bağlantı karmaşıklığı oluşturulduğundan dolayı güvenliği sağlamak büyük bir sorun haline gelmiştir.[220]

Güvenliği sağlamak için güvenlik tehditlerinin bilinmesi ve gereken önemlerin alınması gereklidir. Sanallaştırma üzerine son zamanlarda birçok tehdit unsuru vardır. Bunlar 'hiper yönetici tabanlı saldırılar' , 'VM tabanlı saldırılar' ve 'VM image saldırıları' olarak kategorize edilebilir. Bunların arasında en çok saldırı yüzdesine sahip saldırı hiper yönetici tabanlı saldırılardır. İkinci olarak 'VM tabanlı saldırılar' ve daha sonra 'VM Imaj tabanlı saldırılar' olarak sıralanmaktadır.[221] Şekil 4.2'de bu saldırıların yüzdelik halleri gösterilmektedir.

[219] Ivan Studnia, Eric Alata, Yves Deswarte, Mohamed Kaâniche, Vincent Nicomette, *Survey of Security Problems in Cloud Computing Virtual Machines*, Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012), Cloud and security:threat or opportunity, 2012, Rennes, France, s. 61-74. ffhal-00761206f

[220] Işıl Karabey Aksakallı, "Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler Ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2019, Cilt:5, No:1, s:8-34

[221] M.Soyer, 2021, s.8



Şekil 4.27 : Sanal makinelerde en çok görülen saldırı türleri[222]

Sanallaştırmanın tasarım aşamasında güvenlik ön planda tutulsa da, sanallaştırma teknolojileri hala birkaç yaygın yazılım saldırısına karşı potansiyel olarak savunmasız olabilmektedir. Sanal makine üzerindeki saldırılar, hizmet kalitesine zarar vererek ve veri korumasını ihlal ederek sanallaştırmanın her katmanında çeşitli bileşenleri istismar etmektedir. Bu bölümde sanal makinede meydana gelen saldırılar ve saldırı yöntemleri incelenmiştir.

4.3.1. Sanal Makine Yayılımı (VM Sprawl)

Sanal makine yayılımı, ağa bağlı sanal makinelerin sayısının ağın yeteneklerini aştığında ortaya çıkan olgudur.[223] Kullanılmayan birçok VM kaynakları (enerji, CPU, bellek, depolama, lisanslar) tüketmeye devam ettiğinde ortaya çıkar. Bu durum çok fazla sunucuya sahip olmakla birlikte, bir yöneticinin bir ağdaki tüm sanal makineleri etkili bir şekilde kontrol edemediğinde veya yönetemediğinde gerçekleşir.[224] Meydana gelen bu durum, sunucularda gereksiz karmaşıklığa ve verimsizliğe neden olur.[225] Sanal makine yayılımı, sanallaştırma mantığına ve prensibine aykırıdır ve bu durumla

[222] Darshan Tank, Akshai Aggarwal, Nirbhay Chaubey, *Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison, Bharati Vidyapeeth's Institute of Computer Applications and Management*, 2019, https://doi.org/10.1007/s41870-019-00294-x, 'deki verilere göre hazırlanmıştır.

[223] https://www.techopedia.com/definition/30475/vm-sprawl Erişim Tarihi: 9.02.2021

[224] Maik Lindner, Fiona McDonald, Barry McLamon and Philip Robinson, Towards Automated *Business-driven Indication and Mitigation of VM Sprawl in Cloud Supply Chains, 12th IFIP/IEEE International Symposium on Integrated Network Management and Workshops Dublin*, Ireland, 2011, s. 1062–1065, doi:10.1109/inm.2011.5990505

[225] https://www.dnsstuff.com/what-is-virtual-machine-server-vm-sprawl Erişim Tarihi: 10.02.2021

karşılaşmamak için kontrol mekanizması kurulması gereklidir. VM yayılımın olması durumunda, sanal makinelerin kontrol edilmesi ve güvenliğinin sağlanması mümkün olmayacaktır. [226]

4.3.1.1. Sanal Makine Yayılımına Karşı Önlemler:

- **Sanal makine denetimi yapmak**

Sanal makine yayılmasının birçok olumsuz etkisinden kaçınmak için, sanal makine yayılma kontrolü sağlayan yönetim uygulamalarının uygulanması önemlidir. Yine de farklı nedenlerle VM'ler oluşturmak gerekeceğinden, yayılma tamamen ortadan kaldırılamaz, ancak VM yönetimi ile, yayılmadan olumsuz etkilenmeden VM'ler kullanılabilir. Bunun için ilk adım, VM'lerin denetimini yapmaktır. Bu, hangi makinelerin bir hiper yönetici kümesi veya ana bilgisayar ile ilişkili olduğunu belirlenmesine olanak tanır. Bunu, envanteri diskteki içeriklerle karşılaştırmak için komut dosyaları çalıştırarak yapılabilir. Bir hiper yönetici ile eşlenmemiş herhangi bir makine varsa, bunların aktif kullanımda olmadığını anlaşılır ve daha sonra yer açmak için bu sanal makineler silinebilir. Bununla birlikte boştaki sanal makineleri kontrol etmek de önemlidir Herhangi bir görev gerçekleştirmedikleri halde çalışan sanal makineler kaynakları tüketmektedir. Bu makineler bir kullanım için yeniden tasarlanıp kullanılmayacağına, kapatılmalarına veya kaynaklarının azaltılmasına karar verilebilir.

- **Sanal makineyi doğru boyutlandırmak**

Yayılmayı kontrol etmenin diğer temel unsurlarından biri, sanal makineleri doğru boyutlandırmaktır. VM'ler yeterli kaynağa sahip değilse veya ihtiyaç duyduklarından daha fazlasına sahipse, yapılandırmalarını ayarlamak performansı arttırmaktadır. Bu, manuel olarak veya bir sanallaştırma izleme aracı aracılığıyla yapılabilir.

[226] M.Soyer, 2021, s.8.

- **Gereksiz anlık görüntülüleri silmek**

Sanal makine yönetiminin bir parçası olarak, belirli bir zamanda sanal makine disk dosyasının bir kopyasını oluşturmak için anlık görüntü almak önemlidir. Bu anlık görüntüler bir değişiklik günlüğü sağlar ve sanal makineyi geri yüklemek için kullanılabilir. Ancak anlık görüntü alınırken artık dosya oluşabilir ve orijinal VM silindikten sonra bile bu dosyalar kalabilir. Artık dosyalar önemli miktarda kaynak kullanır ve bunları temizlemek, diğer kullanımlar için disk alanında yer açabilir.

Bu durumun oluşmasında en büyük etken, artık ihtiyaç kalmayan sanal makinenin çalışmasına devam ettirilmesidir. Sanal makineler için bir yaşam döngüsü planı oluşturulmalıdır. Gereksiz ve süresi geçen bir sanal makinenin kaynakları tüketmesini engellemek sistem kaynaklarının hem verimsiz yere harcanmamasına hem de takip edilemeyen sanal makinelerin ortada kalıp güvenlik riskleri oluşturmasına sebep olur. Sanal makine görüntülerinin oluşturulmasını, depolanmasını ve kullanımı kontrol altına alınmalıdır. Yeni yapılacak eklemeler yalnızca gerektiği durumlarda uygulanmalıdır. Her bir sanal makine ile ilişkili ağ bağlantıları için en uygun güvenlik kontrollerinin sınıflandırması ve oluşturulan yol haritasının uygulanması riski azaltacaktır.

- **İyi bir adlandırma kuralı kullanmak**

Sunucuları takip etmekte yardımcı olan adlandırma standartları oluşturulabilir ya da mevcut olan adlandırma kuralları iyileştirilebilir. Örneğin, oluşturma bilgilerine ek olarak sanal makinenin adına veya açıklamasına, sunucunun oluşturulma amacı, kullanılan departmanının adı gibi bilgiler dahil etmek sanal makinenin sahibini bulmayı kolaylaştırır.

- **Arşivlemek**

Sanal makineleri silmek kaynakları serbest bırakır, ancak bu her zaman en iyi yaklaşım değildir. Bazı durumlarda, bir sanal makine şu anda kullanılmayabilir, ancak bir veya iki ay içinde yeniden ihtiyaç duyulabilir. Bu durumlarda, en iyi yaklaşım, genellikle yedekleme ürünleriyle sağlanan arşiv işlevini kullanmaktır. Bu, ihtiyaç duyulana kadar sanal makinenin başka bir yerde arşivlenmesine olanak tanır. Bu süreç,

sanal makinenin nerede depolandığını takip etmeyi, böylece daha sonra ihtiyaç halinde sanal makinenin dosyalarına erişilmesini ve bu dosyalar artık gerekli değilse arşivi temizlemeyi içermektedir.

- **Gereksiz yedeklemeleri sonlandırmak**

Yedeklemeler önemlidir, ancak yedekleme havuzlarında da alan kalmayabilir. Bu durumda, herhangi bir VM' nin birden fazla yedekleme işinin parçası olup olmadığını görmek için yedeklemeler kontrol edilmelidir. Bu durumları belirlemek ve fazlalıkları kaldırmak, yayılmayı azaltmanın başka bir yoludur.[227]

- **Önemsiz öğeleri temizlemek**

Sanal makinelerin günlük kullanımı birçok kurum için çok önemlidir, ancak bu sürekli kullanım aynı zamanda çok sayıda çöp dosyası da üretir. Örneğin, silinmiş veya artık kullanılmayan VM'ler için geçici dosyaları ve VM yapılandırma verileri bir şekilde hala depolanıyor olabilmektedir. Bu gereksiz dosyaların belirlenmesi ve kaldırılması, daha iyi kullanım için kaynakları serbest bırakır.

- **Kategorileri verimli kullanmak**

Sanal makine yönetimiyle ilgili en büyük zorluklardan biri, sanal altyapıdaki tüm nesneleri takip etmektir. Her sanal makineye belirli bir kategori atanırsa, onları gruplamak ve yönetmek çok daha kolay hale gelir.

- **Süreçler ve standartlar oluşturmak**

Belirli süreçler ve standartlar kullanılarak sanal makine yayılımı önlenebilmektedir. Bunun için ilk adım, farklı kullanıcılar için rolleri ve izinleri tanımlamak için rol tabanlı erişim denetimi uygulamaktır. Bu politikalar, doğru kişilerin sanal makineler ve anlık görüntüler oluşturabilmesini sağlar ve bu da hileli sanal makinelere sahip olma olasılığını azaltır.

[227] https://www.dnsstuff.com/what-is-virtual-machine-server-vm-sprawl Erişim Tarihi:10.02.2021

Bu süreçler şunları da içerebilir:

- Herhangi bir sanal makine isteğinin gerekçesini sorma
- Kaynak tahsisini gerçek kullanıma göre ayarlama
- Belirli bir sanal makine için kaç anlık görüntünün tutulacağına ilişkin yönergeler ekleme

Bu standartların yürürlükte olması, sanal makinelerin yönetimini kolaylaştırır ve yayılmayı azaltmaktadır.

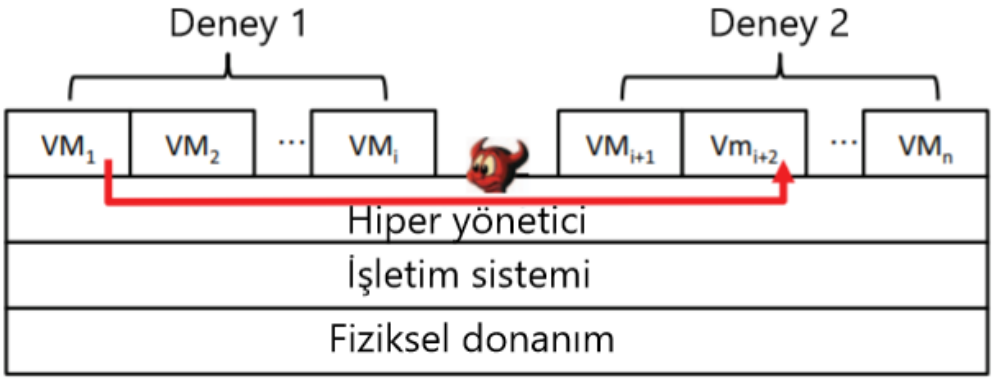
- **Sanal makine yönetim aracı kullanmak**

Son olarak, sanallaştırma dağınıklığını gidermek için bir VM yönetim aracı kullanmak VM yayılma saldırısını önlemede yardımcı olabilir. Bu araçlar, belirli görevleri otomatikleştirerek ve yöneticilere sanal makinelerin çalışmasıyla ilgili net bir görünürlük sağlayarak yığın sanal makineden ve tüm VM ağından en iyi şekilde yararlanılmasına yardımcı olmaktadır.[228]

4.3.2. Sanal Makine Kaçışı (VM Escape)

Sanal makine kaçışı, bir bilgisayar korsanının sanal bir makineden ana işletim sistemine veya sanal makine yöneticisine erişmesini sağlayan bir istismar sürecidir. Bu saldırılar, ana işletim sisteminin güvenlik açığından veya yanlış yapılandırılmasından yararlanır ve sanallaştırma katmanına nüfuz eder. Ana makine kök ayrıcalığına sahip olduğundan, sanal makineden kaçan bir saldırgan, ana işletim sistemi üzerinden erişim elde edebilir ve diğer sanal makinelere saldırabilir veya yapılandırmalarını değiştirebilir. Şekil 4.3'te sanal makine kaçışı gösterilmiştir.[229]

[228] https://www.dnsstuff.com/what-is-virtual-machine-server-vm-sprawl Erişim Tarihi:10.02.2021
[229] Yu-Lun Huang, Borting Chen, Ming-Wei Shih, Chien-Yu Lai, *Security Impacts of Virtualization on a Network Testbed*, IEEE Sixth International Conference on Software Security and Reliability, 2012,s.71-77



Şekil 4.28 : Sanal makine kaçışı[230]

Sanal makinelerin ana makinenin kaynaklarını paylaşmasına izin verilir, ancak yine de bir VM kendisi ile, diğer VM'ler ve ana bilgisayar arasında izolasyon sağlayabilir. Yani, sanal makineler, bir sanal makinede çalışan bir programın diğer VM'lerde çalışan programlarla veya ana bilgisayarda çalışan programlarla izleyemeyeceği veya iletişim kuramayacağı şekilde tasarlanmıştır.[231] Ancak sanal makinenin içinde çalışan işletim sistemindeki güvenlik açıkları, izolasyondan ödün vererek saldırganların VM'e kötü amaçlı bir program eklemesine yardımcı olabilir. Bu program çalıştırıldığında, VM izole edilmiş sınırları aşar ve işletim sistemi ile doğrudan VM katmanını atlayarak iletişim kurmaya başlar.[232] Böyle bir istismar, saldırganların ana makineye erişim elde etmesine ve daha fazla saldırı başlatmasına kapı açar.[233] Bu, ortamın tam bir çöküşüyle sonuçlanabilir. Bu sorun, ana bilgisayar / konuk etkileşimini uygun şekilde yapılandırarak çözülebilir.

4.3.2.1. Sanal Makine Kaçışına Karşı Önlemler

Sanal makine kaçış tehdidini engellemek için literatürde belirlenen başlıca üç metod vardır. Bunlar HyperSafe metodu, güvenilir bulut bilişim platformu ve güvenilir sanal veri merkezidir.[234]

[230] a.g.m., s.75
[231] Jenni Susan Reuben, *A Survey on Virtual Machine Security*, Helsinki University of Technology, 2007-10-11/12, TKK T-110.5290 Seminar on Network Security
[232] D.Tank, A. Aggarwal, N. Chaubey, 2019, s.5.
[233] I. Aksakallı, 2019, s.16
[234] a.g.m., s.16

- **HyperSafe metodu**

HyperSafe, mevcut tip 1 hiper yöneticilere ömür boyu kontrol akışı bütünlüğü sağlamak için kendini koruma özelliği sunan bir yaklaşımdır. Spesifik olarak, iki temel teknik ile tip 1 hiper yöneticilerin korunması amaçlanmıştır. [235]

İlki, devre dışı bırakılamayan (non-bypassable) bellek kilididir. Bu kilit arabellek taşması gibi istismar edilebilir bellek bozulması hatalarının varlığında bile hiper yöneticinin kodunu ve statik verilerini tehlikeye atmaya karşı güvenilir bir şekilde korur, böylece hiper yönetici kod bütünlüğünü başarılı bir şekilde sağlar.

İkincisi, kısıtlı işaretçi indekslemedir. Kontrol verilerini işaretçi indekslerine dönüştürmek için bir dolaylama (indirection) katmanı sunar. Bu işaretçi indeksleri, karşılık gelen çağrı / geri dönüş hedeflerinin hiper yönetici kontrol akış grafiğini sıkı bir şekilde takip eder ve dolayısıyla hiper yöneticilerin korunması sağlanır.[236]

- **Güvenilir bulut bilişim platformu (Trusted cloud computing platform)**

Güvenilir bulut bilişim platformu, güvenilir VM monitörü ve güvenilir bir koordinatörden meydana gelmektedir. Sağlayıcılara kapalı kutu çalışma çevresi sağlar ve kullanıcılara VM'lerini başlatmadan önce ortamın güvenliğini belirlemeye izin verir.[237]

- **Güvenilir sanal veri merkezi (Trusted virtual datacenter)**

Güvenilir sanal veri merkezi, sanallaştırılmış ortamlarda güvenlik ve sistem yönetimi yeteneklerini önemli ölçüde geliştirir, sistemin bütünlüğünü sağlar. VM'ler arasında kaynakların paylaşımını ve ayrıca VM'ler arası iletişimi denetler. VM'leri iş yüklerine göre gruplandırır; hiper yönetici tabanlı izolasyon ve VLAN'lar gibi korunmuş iletişim kanallarını zorlayarak iş yükleri arasında izolasyonu sağlar. Hiper

[235] Zhi Wang, Xuxian Jiang, *HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity*, Department of Computer Science North Carolina State University, 2010, IEEE Computer, Society, Washington DC, USA, s. 380-385.
[236] a.g.m., s.390-395
[237] I. Aksakallı, 2019, s.16

yönetici ile yönetim sanal makinesi için bir aracı görevi görür ve etkin güvenlik politikasına göre sanal makineler arası iletişim ve kaynaklara erişimi kontrol eder.[238]

4.3.3. Çapraz Sanal Makine Yan Kanal Atakları

Sanal makine yan kanal saldırısı, saldırgan şifreleme algoritmasının uygulanma şeklini öğrenmekten ziyade uygulanan algoritmadaki zayıflıklara odaklandığı erişim odaklı bir saldırıdır. Bu saldırılar, saldırganın kurbanın sanal makinesiyle aynı fiziksel donanım üzerinde farklı bir sanal makinede bulunmasını gerektirir.[239]

Yan kanal saldırılarının bir çeşidi, çeşitli hesaplamaların gerçekleştirilmesinin ne kadar zaman aldığını ölçmeye dayanan zamanlama yan kanal saldırısıdır. Ölçülen bu sürenin başarılı bir şekilde değiştirilmesi, hesaplamanın sahibi veya hatta bulut sağlayıcısı hakkında hassas bilgilerin sızmasına neden olabilir. Zamanlama kanallarının kontrolü özellikle zordur ve büyük paralellik nedeniyle bulut teknolojisinde yaygın olarak kullanılır. Dahası, zamanlama yan kanal saldırılarının tespit edilmesi, iz bırakmadıkları veya herhangi bir uyarı vermedikleri için zordur.

Yan kanal saldırılarının bir başka olayı da enerji tüketimi yan kanal saldırısıdır. Hiper yönetici sanallaştırma katmanına doğrudan saldırmak yerine saldırganlar, enerji tüketimi günlüklerini kullanarak bulut hakkında dolaylı olarak hassas bilgiler toplayabilir. Bu tür veriler altyapı durumunu izlemek ve enerji verimli iş yükü haritalaması sağlamak için tutulur.[240] Bulut bilişim ortamında düzinelerce hiper yönetici bulunabilir ve bunların her biri hedeflenen VM'nin ana bilgisayarı olabilir. Bu nedenle, saldırganın hedeflenen VM'yi hangi hiper yöneticinin barındırdığını belirlemesi biraz zaman alabilir. Bir saldırganın ana makineyi belirlemesi ne kadar uzun sürerse, saldırı algılama olasılığı o kadar yüksek olur. Bununla birlikte, saldırgan bir şekilde güç tüketimi verilerini alabilirse, hedeflenen VM'yi çalıştırabilecek olası

[238] Stefan Berger, Ramón Cáceres, Dimitrios Pendarakis, Reiner Sailer, Enriquillo Valdez, *TVDc: Managing Security in the Trusted Virtual Datacenter,* 2007, IBM T. J. Watson Research Center, 19 Skyline Drive, Hawthorne, NY 10532, USA,
[239] Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem, *Cloud Computing Security: A Survey, Computers*, 2014, 3, 1-35; doi:10.3390/computers3010001
[240] I. M. Khalil, A. Khreishah , M. Azeem, 2014, s.16

sunucu kümesini daraltması mümkün olabilir. Bu, saldırganlara tespit edilmeden önce doğru sunucuyu belirleme şansı verir.[241]

4.3.3.1. Çapraz Sanal Makine Yan Kanal Ataklarına Karşı Önlemler

VM yan kanal saldırıları ile ilgili son dönemde yapılan çalışmalar saldırıların ciddiyetini net bir şekilde ortaya koymaktadır. Bu tür saldırıları ele almaya yönelik yaklaşımlar, genellikle donanımda, istemci sanal makinelerinde veya hiper yöneticilerde önemli değişiklikler gerektiren bu saldırıların, belirli varyantları için özelleştirilmiş çözümler sunmaktadır.[242]

Bu sorunu minimize etmek ve saldırganın hedeflerini bulmasını zorlaştırmak için gerçek zamanlı hareketli hedef savunmasını kullanan MIGRATE isimli bir konteyner yönetim çerçevesi geliştirilmiştir. Bu yönetim çerçevesi yan kanal saldırılarına karşı genel savunma sağlar. Ayrıca farklı ana bilgisayarlar arasında, Linux konteynerlarında bulunan bulut kiracılarının uygulamalarının verimli gerçek zamanlı olasılığa dayalı rastgele göçlerini kullanır. MIGRATE, çalışan konteynerları birden çok fiziksel ana bilgisayar arasında taşır. Aynı ana bilgisayarda saldırgan-kurban birlikte kalma olasılığını en aza indirmek için yapılan bu eylem, böyle bir platformla karşılaşan yan kanal saldırılarının çoğunu ortadan kaldırır.

VMware V-Sphere bulut üzerinde test edilen MIGRATE uygulaması göz önüne alındığında, uygulamalar üzerinde neredeyse hiçbir etkiye yol açmadan yüksek frekanslı geçişleri tetikleyebildiğini, bu da onu kritik görev uygulamaları için uygun hale getirdiğini ve hızlı yan kanal saldırılarına karşı bir azaltıcı olduğunu göstermiştir.[243]

4.3.4. Güvensiz Sanal Makine Göçü

Kuruluma bağlı olarak, bir etki alanında birkaç VM çalıştıran bir fiziksel makine aşırı yüklenebilir. Bu gibi durumlarda yük dengesini sağlamak için bazı VM'lerin başka bir fiziksel makineye taşınması gerekebilir. Bu süreç VM Göçü olarak

[241] I. M. Khalil, A. Khreishah , M. Azeem, 2014, s.17
[242] Mohamed Azab, Mohamed Eltoweissy, *MIGRATE: Towards a Lightweight Moving-target Defense against Cloud SideChannels*, 2016, IEEE Symposium on Security and Privacy Workshops,s.96-103
[243] M.Azab, M. Eltoweissy, 2016, s.96-103

adlandırılır. [244] Göç sırasında bir fiziksel makineden hedef konumdaki diğer fiziksel makineye aktarılırken VM dosyalarının içeriği çeşitli saldırılara karşı savunmasız kalabilmektedir.[245] Bunun sebebi sanal makine göçü sırasında VM durum dosyalarının içeriğinin erişilebilir bir hale gelmesidir. Bu zaaftan faydalanmak isteyen bir saldırgan şunları yapabilir:

- Taşıma sırasında verilere yasa dışı olarak erişim sağlayabilir.
- Bir sanal makineyi güvenli olmayan bir ana makineye aktarabilir.
- Kesintilere veya DoS ataklarına neden olan birkaç sanal makine oluşturabilir.[246]

Sanal makine göçü saldırısında, saldırgan ağdan başka bir konuma geçen bir sanal makineden değerli bilgileri gizlice dinlemeye odaklanır. Böylece saldırgan bulut ağını izler ve VM'in bir kez geçişini tespit ettiğinde, taşınan VM'in paketlerini toplar. Ve bu paketler sayesinde taşınan sanal makineye erişmek için kullanabileceği şifreleme anahtarları, sertifikalar, kimlik bilgileri gibi bilgilere erişebilir.[247]

4.3.4.1. Güvensiz Sanal Makine Göçüne Karşı Önlemler

Zhang ve arkadaşları[248] yaptığı çalışmada VMM tarafından uygulanan işlem koruma sistemlerindeki VM'lere canlı göç yeteneği sağlayan, güvenliği koruyan bir VM canlı göç çerçevesi sunmuşlardır. Göç süreci sırasında bu çerçevede, hassas verilerin, meta verilerin ve canlı göç sürecinin gizliliğinin ve bütünlüğünün korunması için güvenlik açıklarını belirleyerek bunlara uygun çözümler sağlamışlardır. Tasarım çerçevesini değerlendirmek için PALM adlı bir çalışma prototipi uygulamışlardır.

---

[244] Aaron Zimba and Victoria Chama, *Cyber Attacks in Cloud Computing: Modelling Multi-stage Attacks using Probability Density Curves*, I. J. Computer Network and Information Security, 2018, 3, 25-36, doi: 10.5815/ijcnis.2018.03.04

[245] I. Aksakallı, 2019, s.14-15.

[246] Keiko Hashizume, David G Rosado , Eduardo Fernández-Medina, Eduardo B Fernandez, *An analysis of security issues for cloud computing*, Journal of Internet Services and Applications 2013, 4:5, s.1-21.

[247] A. Zimba, V. Chama, 2018, s.25-36

[248] Fengzhe Zhang, Yijian Huang, Huihong Wang, Haibo Chen, Binyu Zang, *PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection*, Third Asia-Pacific Trusted Infrastructure Technologies Conference, 2008, s.9-18

Önerilen sistem:

- Göç işlemi yapıldığı sırada korunan işlemleri veya sayfaları şifrelemek, şifre çözmek ve engellemek için kullanılan göç verilerini koruma modülü ,
- Göç işlemi sonrasında şifreleme anahtarları, işlem kimlikleri gibi meta verileri yönetmek için kullanılan meta veri yönetim modülü,
- Canlı göç işlemi sırasında güvenlik koruması olmak üzere üç modülden oluşmaktadır.

Bu prototip Xen ve Gnu Linux platformları üzerinde başarılı bir şekilde uygulanmış ve değerlendirme sonucunda bu şemanın yalnızca şifreleme ve deşifreleme nedeniyle hafif kesinti ve geçiş süresi eklediği görülmüştür.

Gao ve arkadaşlarının yaptığı çalışmada[249] her VM için güvenlik politikalarını özelleştiren bir güvenlik çerçevesi önerilmiştir. Bu çerçeve sanal makineye canlı göç sırasında sürekli koruma sağlamaktadır. Gao ve arkadaşları, kapsamlı güvenlik duvarı teknolojileri ve ip tabloları, xml komutları kullanarak Xen hiper yönetici tabanlı VNSS isimli bir prototip sistemi uygulamışlardır. Yapılan çalışmalar neticesinde yapılan bu güvenlik politikalarının canlı göç boyunca etkili olduğu gözlemlenmiştir.

Diğer bir çözümde ise kimlik doğrulama, onaylama ve veri aktarma işlemlerini kapsayan VM-vTPM (Virtual Trusted Platform Module) isimli bir göç protokolü önerilmektedir. [250] vTPM, tek bir donanım platformunda birkaç sanal makine tarafından kullanılmak üzere fiziksel bir TPM'yi sanallaştıran sistemdir.[251]Bu protokol her iki tarafın birbirlerini doğrulamasıyla başlamaktadır. Ardından iletişim için güvenli oturum oluşturularak kimlik doğrulama yapılmaktadır. Bu işlemler başarıyla yapıldığında sistemi doğrulamak ve kontrol etmek için kaynak tarafından uzaktan onaylama ile VM - vTPM aktarımı gerçekleşmektedir. Kaynak ana bilgisayar önce VM' i vTPM boyunca askıya alarak şifrelemekte ve sonra hedef makineye aktarma

[249] Gao Xiaopeng, Wang Sumei,Chen Xianqin, Vnss: *A Network Security Sandbox For Virtual Computing Environment,2010 IEEE Youth Conference on Information*, Computing and Telecommunications , s. 395–398. doi:10.1109/ycict.2010.5713128

[250] Dongxi Liu, Jack Lee, Julian Jang, Surya Nepal, John Zic, *A Cloud Architecture of Virtual Trusted Platform Modules*, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, s.804-811

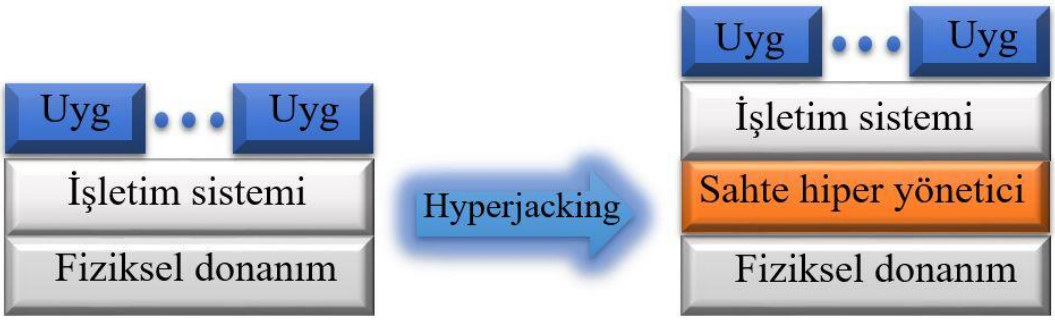
[251] S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer and L. van Doorn, *vTPM: virtualizing the trusted platform modüle*, Proceedings of the 15th conference on USENIX Security Symposium, 2006

işlemi gerçekleşmektedir. Ayrıca, kaynak ana makine vTPM'si boyunca VM'yi de silmektedir.[252]

4.3.5. Hyperjacking Saldırısı

Bir hiperjacking saldırısı, bir sahte modülü alt etmek veya sisteme enjekte etmek için bir sistemi dışarıdan istismar etmeyi hedeflemektedir. Sisteme sahte modül enjekte edildiğinde, bir saldırgan aynı ana bilgisayarın üzerinde çalışan sanal makineleri kontrol edebilir ve ağ trafiğini izleyebilir. Dahası, kötü amaçlı kodlar diğer sistemleri bozabilir ve izolasyon gereksinimine zarar verebilir.[253]

Bu riskin kendisini nasıl gösterebileceğine dair güzel bir örnek, güvenlik araştırmacısı Joanna Rutkowska tarafından geliştirilen Blue Pill rootkit'tir. Rootkit, varlığının tüm kanıtlarını sistem yöneticilerinden ve sistemlerde anormallikler ve güvenlik ihlalleri arayan diğer kişilerden gizlemek için tasarlanmış bir Truva atı programıdır. Blue Pill rootkit, Vista işletim sisteminin çekirdeğine imzasız kod yüklemek için Vista bütünlük denetimi sürecini atlar. Bu kod, AMD'nin güvenliği artırmak, kendisini algılamadan gizlemek için tasarlanmış güvenli sanal makinesini kullanır ve Şekil 4.4'de gösterildiği üzere, sistem yöneticileri ve diğerlerinin varlığını algılamadan işletim sisteminin kontrolünü ele geçiren bir hiper yönetici haline gelir.[254]



Şekil 4.29 : VM hyperjacking saldırısında kodun hiper yönetici hâline gelmesi[255]

[252] I. Aksakallı,2019, s.25
[253] Y. Huang, B. Chen, M.Shih, C. Lai, 2012, s.71-77
[254] M. Lindner, F. McDonald, B. McLamon, P. Robinson,2011,s.1062-1065
[255] Y.Huang, B. Chen, M. Shih, C. Lai, 2012, s.71.77

Sanal makine hyperjacking saldırıları hem konteyner tabanlı hem de hiper yönetici tabanlı sanallaştırma sistemlerine saldırmak için başlatılabilir. Bu tür saldırılar, genel bir işletim sisteminin herhangi bir güvenlik açığından yararlanabilir ve bir ağ test yatağının izolasyonuna zarar vermek için ana işletim sistemini kullanabilir.[256]

Bilgisayar korsanı hiper yöneticiye erişim sağlarsa, bu sunucuya bağlı olan her şeyin değiştirilebileceği ve saldırılara açık olduğu anlamına gelmektedir. Bir hiperjacking saldırısının başarılı olması için, bir saldırganın aşağıdaki yöntemlerle hiper yönetici kontrolünü ele geçirmesi gerekir:

- Orijinal hiper yöneticinin altına sahte bir hiper yönetici enjekte etmek
- Doğrudan orijinal hiper yöneticinin kontrolünü elde etmek
- Mevcut bir hiper yönetici üzerinde hileli bir hiper yönetici çalıştırmak[257]

4.3.5.1. Hyperjacking Saldırısına Karşı Önlemler

Hyperjacking ciddi bir sorun olmasına rağmen alınacak basit önlemlerle bu durum önlenebilir. Öncelikle hiper yöneticinin güvenlik yönetimi normal trafikten ayrılmalıdır. Konuk işletim sistemleri bu aşamada en çok dikkat edilmesi gereken hususların başında gelmektedir. Konuk işletim sistemlerinin hiper yöneticiye erişimi tamamen kesilmelidir. Yönetimsel araçlar konuk işletim sisteminden asla yüklenilmemeli ve kullanılmamalıdır. Hiper yöneticide düzenli olarak patch işlemleri yapılmalıdır. [258]

4.3.6. Sanal Makine Atlama Saldırısı (VM Hopping)

Sanal makine atlama saldırısı, bir sanal makinedeki bir saldırganın aynı ana bilgisayarda oturan diğer bir sanal makineye atladığı bir saldırıdır. Sanallaştırma güvenlik saldırılarında yaygın bir saldırı modu olan atlama saldırısının ilk hedefi,

[256] Y.Huang, B. Chen, M. Shih, C. Lai, 2012, s.71-77
[257] M. Soyer, 2021, s.13
[258] a.g.m., s.14

kurban sanal makinelerinin IP adreslerini elde etmektir. Böylece saldırgan, dahili ağ köprüsü üzerinden izolasyon kontrolünü kırabilmektedir.[259]

Sanallaştırmanın uygulanmasına göre, aynı hiper yönetici üzerindeki sanal makineler ağ bağlantıları, paylaşılan bellek veya diğer paylaşılan kaynaklar aracılığıyla birbirleriyle iletişim kurabilir. Ancak, sanal makinenin atlamasına neden olan şey sanallaştırmanın uygulanmasıdır.

Atlama saldırısı iki duruma ayrılabilir. Birinci durumda, saldırgan, sanal makineler arasındaki bu iletişim yoluyla hiper yönetici üzerindeki diğer sanal makinelere sessizce erişmek veya bunları kontrol etmek için kötü amaçlı bir sanal makine kullanabilir. Diğer bir durum da sanal makinedeki bir saldırgan, hiper yönetici katmanını yasa dışı bir şekilde aşarsa ve ana bilgisayar işletim sistemine erişim kazanırsa, aynı fiziksel sunucu üzerindeki diğer sanal makineleri bile yok edebilir. Her iki durum da sanallaştırma katmanı ve hatta tüm bulut platformu için farklı yönlerden büyük bir tehdit oluşturmaktadır.

Sanal makine atlama saldırısı başarılı olduğunda, saldırgan hiper yönetici katmanını aşarak doğrudan ana bilgisayara iner. Kaçınılmaz olarak, saldırgan bu ana makinedeki diğer sanal makinelerin G/Ç veri akışını engelleyebilir, diğer kullanıcıların ilgili verilerini analiz edip elde edebilir ve ardından hassas bilgilere yönelik başka saldırılar gerçekleştirebilir.

Varsayılan kullanıcı veya hatta yöneticinin temel bilgileri değiştirildiğinde, ana makine de korumasız olacaktır. Dahası, ana bilgisayardaki bir sanal makine temel bir hizmet olarak çalışıyorsa, saldırgan sanal makineyi zorla kapatabilir veya silebilir.

4.3.6.1. Sanal Makine Atlama Saldırısına Karşı Önlemler

Sanal makine atlama saldırı savunması, temel olarak daha sağlıklı ve basit hiper yöneticiler oluşturarak ve daha sağlam erişim kontrol politikaları tasarlayarak çözülmektedir.[260]

[259] Y. Huang, B. Chen, M. Shih, C. Lai, 2012, s.71-77
[260] a.g.m., s.78

Güvenilir Bilgi İşlem Tabanı (Trusted Computing Base), sistem genelinde bilgi güvenliği politikalarının uygulanmasından sorumlu olan sistemin parçasıdır.[261] Tüm sistem için güvenlik sağlayan TCB, son derece güvenilirdir ve üst düzey uygulama işlemlerinin güvenliğini sağlamanın temelini oluşturur. Bununla birlikte, TCB ne kadar büyükse, o kadar fazla kod, güvenlik açığı olasılığı ortaya çıkar.

Erişim kontrolü, sistem güvenliği ve bilgi güvenliği için ortak bir teknik araçtır ve her yönden verilerin gizliliğini ve bütünlüğünü sağlar. Sanallaştırma alanında, güvenlik riskleri esas olarak yasadışı kaynak erişiminden kaynaklanmaktadır ve erişim kontrolünün tasarımı, özne ile nesne arasındaki kaynakların erişim haklarını hedeflemektedir. Bu nedenle, erişim kontrol politikası, sanallaştırılmış etki alanındaki ilgili sorunları çözmek için kullanılır. Daha karmaşık durum geçişleri ve sanal makine atlama saldırılarının tehlikeleri nedeniyle, özel olarak bir dizi erişim kontrol politikası tasarlanmalıdır.[262]

4.3.7. Kötücül Sanal Makine Saldırısı (Malicious VM Attack)

Bir sanal makine imajı, sanal makine oluşturmak için kullanılan bir sanal aygıt şeklidir. Bu imajlar başlangıç dosya sistemi durumunu ve yazılımı içermektedir. Sanal makineye erişen bir saldırgan, içerisinde sistemi etkileyebilecek Trojan atı gibi kötü amaçlı kod içeren yazılımlarla sanal makine imajı oluşturabilir. Diğer kullanıcılar bu imajı kullandıkları zaman, saldırganın oluşturduğu kötü amaçlı kod bu makinelere de bulaşma riski oluşmaktadır. Oluşan bu durum karşısında saldırganın sunucuda tutulan gizli verilere de erişim sağlaması kaçınılmaz olacaktır. [263]

4.3.7.1. Kötücül Sanal Makine Saldırılarına Karşı Önlemler

Anlık ve güncel durumlarını gösteren sanal makine izleme sistemi kurmak kötü niyetli saldırıların hedefi olan sanal makineleri korumaya yardımcı olabilir. Bu sistem

[261] https://www.ibm.com/docs/en/aix/7.2?topic=configuration-trusted-computing-base Erişim Tarihi 04.04.2021
[262] Ying Dong and Zhou Lei, *An Access Control Model for Preventing Virtual Machine Hopping Attack, School of Computer Engineering and Science*, Shanghai University, Shanghai, China, 2019, s.4
[263] I. Aksakallı, 2019, s.16

birbirine saldıran sanal makinelerin tespitini yapmaktadır. Böylece kaynak kullanım durumların analizini sanal makine izleme aracıyla takip etmek mümkündür.[264]

4.3.8. Sanal Makine Geri Alma Saldırısı (VM Rollback)

Hiper yönetici, yürütme sırasında herhangi bir zamanda bir VM'yi askıya alabilir, mevcut CPU durumlarının, diskin ve belleğin anlık görüntüsünü alabilir ve daha sonra konuk VM farkındalığı olmadan bir anlık görüntüyü devam ettirebilir. Bu özellik, hata toleransı ve VM bakımı için yaygın olarak kullanılmaktadır; ancak, aynı zamanda bir saldırgana VM geri alma saldırılarını başlatması için açık bir pencere sağlamaktadır.[265]

Geri alma saldırısında saldırgan önceki anlık görüntülerden yararlanabilir, bunları kullanıcının farkında olmadan çalıştırabilir, ardından geçmişi temizleyebilir. Saldırgan geçmişi temizleyerek şüpheli faaliyetlerinden dolayı yakalanma ihtimalini azaltır.[266] Örneğin, bir saldırgan, konuk giriş yapsa bile sanal makinenin oturum açma parolasını tahmin etmek için kaba kuvvet (brute-force) saldırısı başlatabilir.[267]

İşletim sisteminin, kullanıcıyı üç başarısız denemeden sonra engelleme veya 10 denemeden sonra hesabı silme gibi kısıtlaması vardır. Ancak saldırgan yine de her denemeden sonra sanal makineyi başlangıç durumuna geri alabilir. Saldırgan, sanal makinenin içindeki sayacı temizleyerek ve kısıtlamayı atlayarak kaba kuvvet saldırısını yeniden çalıştırabilir.[268]

4.3.8.1. Sanal Makine Geri Alma Saldırılarına Karşı Önlemler

Sanallaştırmanın önemli bir parçası, fiziksel platformu yöneten ve konuk sanal makinelere atanan bellek dahil tüm kaynaklarına erişebilen hiper yöneticidir. Sanallaştırma yazılımındaki hata raporları hiper yöneticiyi saldırılara karşı korumanın

[264] M.Soyer, 2021, s.8
[265] I. M. Khalil, A. Khreishah and M. Azeem, 2014, s.19-20
[266] Y. Xia, Y. Liu, H. Chen, B. Zang, 2012, s.1-8.
[267] Nuno Antunes,Marco Vieira, *Defending against web application vulnerabilities*, Computer, 2012, 45, s.66–72.
[268] a.g.m., s.68.

çok zor olduğunu göstermektedir. Szefer ve Lee[269], hiper yönetici güvenlik açıklarını yönetmek için "Hyperwall" adlı bir mimari çözümü önermiştir. Sanal makine geri alma saldırısını önlemeye yönelik olan bu çözüm, hiper yöneticinin askıya alma ve sürdürme işlevlerini devre dışı bırakmaya dayanmaktadır. Askıya alma ve sürdürme özelliği sanallaştırma için önemli bir özellik olduğundan devre dışı bırakılması daha iyi bir çözüm sağlamaz.

Bu çözümün diğer bir sınırlaması, bulut sistemi ile aşırı kullanıcı etkileşimidir. Bu etkileşim son kullanıcıların VM önyükleme, askıya alma ve devam ettirme sırasında dahil olmasını gerektirir. Bu, sistemin bir VM'yi her yeniden başlattığında, taşıdığında veya askıya aldığında izin istemesi gerektirdiğinden çözümü elverişsiz ve kullanışsız hale getirir.

Xia ve arkadaşları[270] , Hyperwall çözümünün aksine hiper yöneticiün herhangi bir temel işlevini devre dışı bırakmadan çalışan bir çözüm sunmaktadırlar. Bu çözümde, VM etkinliklerinin günlüğünü denetleyerek bir geri dönüşün kötü amaçlı olup olmadığını tespit etmektedir. Bu çözüm, Hyperwall'a kıyasla kullanıcı katılımını en aza indirmiş olsa da bulut bilişimin değişen altyapısı, yine de bir miktar kullanıcı katılımıyla VM işleminin otonom çalışmasını gerektirmektedir.

4.3.9. Sanal Makine DoS ve DDoS Saldırıları

Uluslararası siber saldırılarda da sıklıkla kullanılan DoS ve DDoS saldırılarında amaç sistemin verdiği hizmetleri aksatmaktır. Saldırıya uğrayan kurum hizmet veremediği zaman maddi ve manevi olarak zarara uğramaktadır. Günümüzde basit araçlarla çok kolay bir şekilde saldırılar gerçekleştirilebilir. Bu yüzden bu saldırılar kurumlar ve sistemler için ciddi bir tehdit unsurudur. Bu saldırılar hizmet aksatmaya neden olduğu için suç teşkil etmektedir.[271]

[269] J. Szefer,R. B. Lee, 2012 s.437-439
[270] Y. Xia, Y. Liu, H. Chen, B. Zang, 2012, s.1-8.
[271] https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html Erişim tarihi: 15.02.2021

4.3.9.1. Sanal Makine DoS ve DDoS Saldırılarına Karşı Önlemler

Bu saldırıların tamamen engellenmesi için kesin bir yöntem yoktur. Ancak saldırıların etkisini minimuma indirmek için önlemler alınmalı ve sistemin ağ altyapısının sağlam yapılandırılması gerekmektedir.[272] Saldırının engellemesinden ziyade saldırı öncesi önlemlerin alınması ve erken tespiti daha önemlidir. Bunun için alınması gereken başlıca önemler aşağıda sıralanmıştır.

- Güvenlik duvarı ve antivirüs yazılımı kullanılmalıdır.
- Sistem güncellemeleri zamanında ve eksiksiz yapılmalıdır.
- Ağ trafiği izlenilmelidir, olağandışı durumlar için ağ cihazları yapılandırılmalıdır.
- Bant genişliği kurumun ihtiyacı olandan fazla olmalıdır.
- Büyük ölçekli kurumlar için İçerik Dağıtım Ağı (CDN) verilerin dünyada birden çok sunucuda saklanması kullanımı uygulanabilir.[273]

4.3.10. Zararlı Yazılımlar

Zararlı yazılımların özellikle sanal sistemlere nasıl saldırabileceğini gösteren iki ana senaryo vardır. Kötü amaçlı yazılım ya ana sunucuda bulunur ve sanal makineye saldırır ya da tehdit sanal makinededir ve ana sunucuya saldırır. Diğer tüm saldırı vektörleri, geleneksel BT dünyasından zaten bildiğimiz bir bilgisayarın başka bir bilgisayara saldırdığı klasik senaryolara indirgenebilir.

4.3.10.1. Kötü amaçlı yazılıma bir örnek: Crisis

Bir ana sunucuyu başarıyla ihlal eden bir saldırganın, o sunucudaki sanal makinelere sızması veya kendi kötü amaçlı sanal makinelerini oluşturup onu başlatması mümkündür. Bu davranışı otomatikleştiren kötü amaçlı yazılımlar vardır. Bu tür kötü amaçlı yazılımlara bir örnek W32.Crisis'tir.

Bu özel tehdit, Windows, Mac OS X ve Microsoft'un önceki mobil işletim sistemi Windows Mobile dahil olmak üzere birden çok işletim sistemini

[272] Y. Huang, B. Chen, M. Shih, C. Lai, 2012, s.71-77
[273] https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html Erişim tarihi: 15.02.2021

hedeflemektedir.[274] Kötü amaçlı yazılım, sosyal mühendislik yoluyla bir Java dosyası olarak bırakılır ve çeşitli bilgi çalma etkinlikleri gerçekleştirir. Kötü amaçlı yazılım ayrıca, ana bilgisayardan konuklara bulaşan yerel sunucuda depolanan sanal makinelere de yayılmaya çalışır. Bunu başarmak için VMware yazılımındaki herhangi bir güvenlik açığından yararlanmaz. Bunun yerine, tüm sanal sistemlerin basitçe ana sunucunun diskindeki bir dizi dosyadan oluşması gerçeğinden yararlanır.

Bu dosyalar genellikle doğrudan kullanılabilir veya ücretsiz olarak kullanılabilen araçlarla monte edilebilir. W32.Crisis durumunda, kötü amaçlı yazılım, VMware kurulum dizinindeki tercihler.ini dosyasını ayrıştırır ve içindeki.vmx dosya yollarını arar. Tehdit daha sonra.vmx ayarlar dosyası içinde VMware Sanal Makine Disk dosyalarını (VMDK) arar.

Kötü amaçlı yazılım görüntü dosyasını bir sürücü olarak bağlamak ve değiştirmeye başlamak için mevcut bağlama hizmeti aracı olan vixDiskMountServer.exe'yi kullanmaktadır. Tehdit, görüntü dosyasını, sanal makinenin bir sonraki başlatılışında kendisini yürütmek ve sanal makineye bulaştırmak için sanal Windows bilgisayarlarının başlangıç klasörüne kopyalayarak değiştirir. W32.Crisis'in analiz edilen sürümlerinde, sanal makinelerin içindeki başka bir işletim sistemine bulaşmaya çalışmadığı ve VMware ESX sunucularını hedeflemediği görülmüştür, ancak bir saldırgan teorik olarak bunu yapabilmektedir.[275]

4.3.10.2. Zararlı Yazılımlara Karşı Önlemler

Sanal ortamlar, dinamik ve uygulama merkezli yaklaşımının farklı gereksinimlerini karşılamak için geleneksel korumaların ötesine geçen güvenlik çözümlerine ihtiyaç duymaktadır. Bu, bağımsız sanallaştırılmış sunucular ve modern SDDC'ler için de geçerlidir. Elbette farklı kurulumlar ve mimariler farklı uygulama yaklaşımları gerektirebilir. Her durumda, sanal makinelerin BT'nin güvenlik stratejisine entegre edilmesi gerekmektedir. Sanal ortamların güvenliğini sağlarken dikkate alınması gereken bazı en iyi uygulama yönergeleri burada verilmiştir.

[274] https://www.itpro.co.uk/642409/crisis-malware-infects-virtual-machines Erişim Tarihi: 17.02.2021
[275] https://vxug.fakedoma.in/archive/Symantec/threats-to-virtual-environments-14-en.pdf Erişim Tarihi : 19.02.2021

- **Sağlamlaştırma**: Birden çok sanal makineye erişim sağladığı için ana sunucunun iyi korunması gerekmektedir. Güncelleme ve yama uygulamasının yanı sıra sunucu, kilitleme çözümleri ve ana bilgisayar IDS[276] yardımıyla saldırılara karşı korunabilir. Yöneticiler, politikaları ve beyaz listeyi yalnızca güvenilir sistem uygulamalarının çalışmasına izin verecek şekilde ayarlayabilir.
- **Gelişmiş kötü amaçlı yazılım koruması:** Ana sunucu ve üzerinde çalışan herhangi bir sanal makinenin kötü amaçlı yazılımlara karşı korunması gerekmektedir. Bunu başarmak için, klasik statik antivirüs tarayıcısının ötesine geçen proaktif bileşenlere sahip gelişmiş kötü amaçlı yazılım korumasının olması gerekmektedir. Kuruluma bağlı olarak, yüksek bir performans seviyesini korumak için tehdit koruması her sanal makineye ayrı ayrı veya barındırma sunucusundan aracısız olarak dağıtılabilir.
- **Erişim denetimi:** Yöneticilerin, değişiklikleri yalnızca uygun kullanıcıların gerçekleştirebilmesini sağlamak için sanal makine barındırma sunucularına uygun erişim denetimi yönetimi uygulaması gerekir. Bunlar, iki faktörlü kimlik doğrulama gibi güçlü oturum açma işlemleri kullanması gereken çok önemli sunuculardır. Bu işlemler, hesap verebilirlik için başarılı ve başarısız oturum açma işlemlerinin uygun şekilde günlüğe kaydedilmelidir.
- **Olağanüstü durum kurtarma:** Sanal makinelerin olağanüstü durum kurtarma ve iş sürekliliği planına entegre edilmesi gerekir. Yöneticiler, veriler için yüksek kullanılabilirlik ve yedekleme stratejileri uygulamalıdır.
- **Sanal ağ koruması:** Yöneticiler, IPS[277] / IDS gibi ağ güvenliği araçlarının aynı ana sunucu üzerindeki birden çok sanal makine arasındaki sanal ağdaki trafiğe erişiminin olmasını sağlamalıdır.
- **Güncelleme**: Sanal makinelerin anlık görüntülerinin ve görüntülerinin, konuşlandırıldıklarında güncel olmaları için yama ve yükseltme döngüsüne dahil edilmesi gerekmektedir.

[276] Intrusion Detection Systems (IDS) : Saldırı Tespit Sistemleri, ağlara veya sistemlere karşı yapılan kötü niyetli aktiviteleri ya da politika ihlallerini izlemeye yarayan cihaz ya da yazılımlardır.
[277] Intrusion Prevention System (IPS) :Saldırı Önleme Sistemleri, ağ trafiği içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti ile birlikte önlenmesi için kullanılan güvenlik sistemleridir.

- **Günlük kaydı:** Sanal makinelerin, tıpkı diğer BT cihazları gibi güvenlik kaydı ve SIEM görselleştirme sistemlerine entegre edilmesi gerekir. Sanal makineler dinamik olarak sağlanabildiğinden ve ağ içinde taşınabildiğinden, bu faaliyetlerin de tutarlı bir şekilde günlüğe kaydedilmesi gerekmektedir.

BEŞİNCİ BÖLÜM

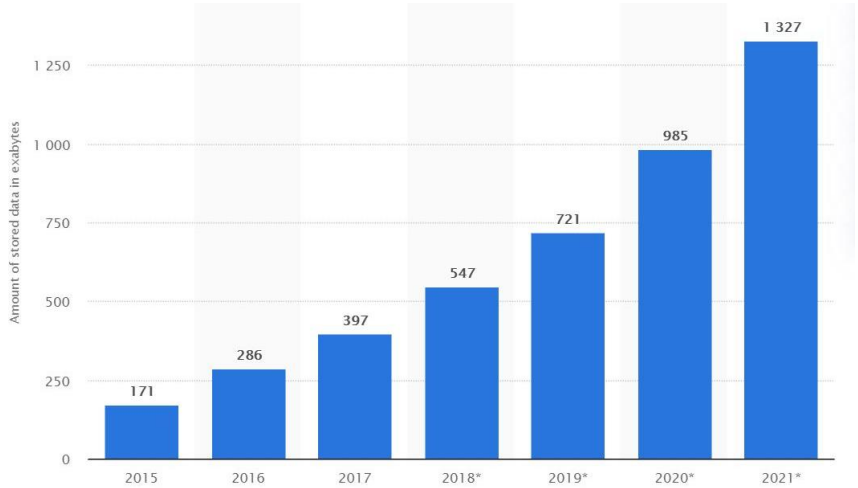
SANALLAŞTIRMADA YENİ YAKLAŞIMLAR VE SANALLAŞTIRMA TEKNOLOJİSİNİN YARARLARI

5.1. SANALLAŞTIRMADA YENİ YAKLAŞIMLAR

5.1.1. Veri Merkezi Mimarisi Evrimi

Günümüzde veri merkezleri, bilgi merkezli dünyanın önemli bir parçası haline gelmiştir. Bunun sonucunda dünya genelinde özellikle son yıllarda veri merkezlerinde depolanan veri miktarında ciddi bir artış gözlenmiştir. 2015 yılından 2021 yılına kadar depolanan veri miktarı ve artışı Şekil 5.1'de gösterilmiştir. Üretilen verilerdeki bu üstel artışla doğru orantılı olarak depolama ihtiyacı da artmıştır. İş sürekliliğinin sağlanması için bu ihtiyacın karşılanması zorunluluk halini almıştır.

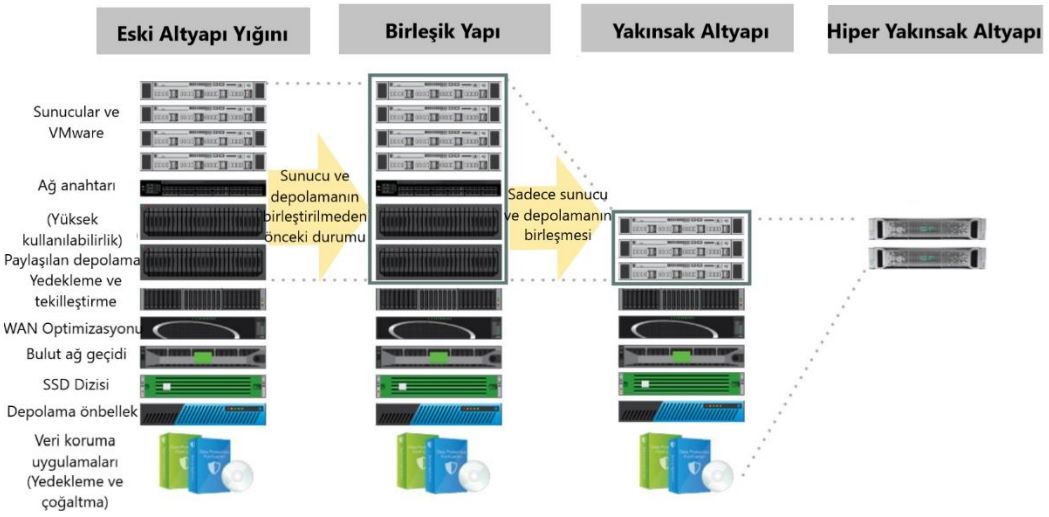
Veri merkezleri, altyapıyı çalışır durumda tutmak için yedekli bilgi işlem, depolama ve ağ bileşenlerini barındırmaktadır. Teknolojinin bu alanda gelişmesindeki amaç, veri merkezlerini daha güçlü ve verimli hale getirmek, genel sistem verimini iyileştirmek için daha iyi kaynak kullanımına olanak sağlamaktır.



Şekil 5.30 : 2015'ten 2021'e kadar dünya genelindeki veri merkezlerinde gerçekte depolanan veri miktarı[278]

[278] https://www.statista.com/statistics/638613/worldwide-data-center-storage-used-capacity/#statisticContainer Erişim Tarihi : 03.03.2021

Veri merkezleri zaman içerisinde gelişerek hantal ana bilgisayarlardan merkezi depolamaya sahip sunuculara, yakınsak ve hiper yakınsak altyapıya dönüşmüştür. Şekil 5.2'de veri merkezinin gelişim aşamaları gösterilmiştir. Bu gelişmedeki her aşama, önceki neslinin eksikliklerini gidermekte, ancak kendi içinde avantajlar ve dezavantajlar barındırmaktadır.



Şekil 5.31 : Veri merkezinin evrimi[279]

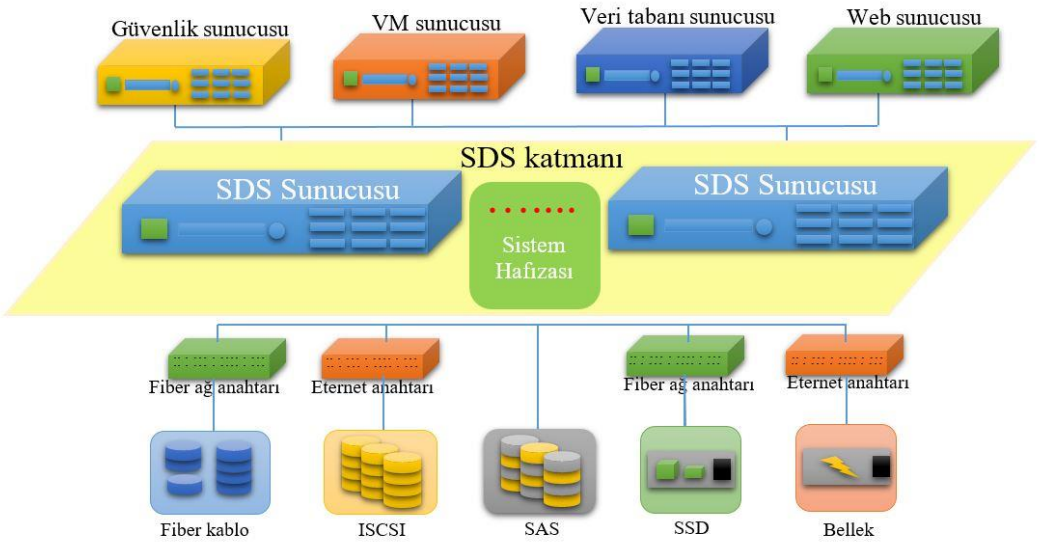
5.1.2. Yazılım Tanımlı Depolama (SDS)

SDS, farklı depolama donanımlarının havuzda toplanmasına izin vererek, kullanıcıların mevcut altyapılarını tam olarak kullanmalarına ve böylece gereksiz, daha maliyetli donanım revizyonlarından kaçınmalarına olanak tanıyan yazılım tanımlı depolamadır. Bu mimari ile tüm temel depolamayı sanallaştıran sanal bir yazılım katmanı oluşturulmaktadır. Altyapı sanallaştırıldıktan sonra, depolama düzenini optimize etmek ve yeniden tasarlamak kolaylaşmaktadır. Kullanıcılar tarafından depolama alanları bölünebilmekte ve en çok ihtiyaç duyulan yere dağıtılabilmektedir.

Yazılım tanımlı depolama, sabit disk, SSD, flash NVMe, bellek gibi tüm farklı depolama türlerini yönetmektedir. Şekil 5.3'te gösterildiği üzere, SDS tüm farklı

[279] https://www.sentia.sanca/Blog/ArtMID/1133/ArticleID/81/The-Top-10-Characteristics-and-Benefits-of-Hyper-convergence Erişim Tarihi: 03.03.2021

depolama türlerinden tüm G/Ç' yi kontrol eden bir yazılım katmanı ekleyerek depolamanın performansını artırmaktadır.



Şekil 5.32 : SDS ve yazılım katmanı

SDS bir dizi avantaj sağlamaktadır:

- SDS, farklı türlerdeki depolama cihazlarının birbirleriyle iletişim kurmasını sağlamaktadır.
- Tüm depolama cihazlarının merkezi yönetim altında bir araya getirilmesine olanak sağlamaktadır.
- Donanım yükseltmeleri ve bakımının yanı sıra veri geçişlerini ve teknoloji yenilemelerini basitleştirmektedir.
- Bulutta neredeyse sorunsuz ölçeklenebilirlik sağlamaktadır.
- Tüm uygulamalara uyacak şekilde hem blok hem de dosya depolama sağlamaktadır.
- Eski depolama sistemlerinin performansını arttırmaktadır.

5.1.3. Yazılım Tanımlı Veri Merkezi (SDDC)

SDDC'nin ilk ve ana katmanı sanallaştırma olarak ifade edilir. Geleneksel bir veri merkezi, kurumsal verilerin, uygulamaların, ağların ve altyapının merkezi olarak barındırıldığı ve erişildiği bir tesistir. Geleneksel veri merkezleri gibi, SDDC'ler de

sunucuları, depolama cihazlarını, ağ ekipmanlarını ve güvenlik cihazlarını barındırır. Geleneksel veri merkezlerinden farklı olarak, bir SDDC, geleneksel bir veri merkezinin işlevlerine programlı bir yaklaşım sunmak için sanallaştırılmış bir ortam kullanır.

Uzak API'leri ve ağ tarayıcısı arayüzlerini kullanarak SDDC'ler herhangi bir konumdan yönetilebilmektedir. Tüm BT altyapı öğelerinin yazılımla tanımlandığı ve devreye alındığı hiper yakınsak altyapının ortaya çıkmasıyla birlikte, ağ teknolojisi bulut SDDC ve ITaaS girişimlerini destekleme gücüne sahip olur. SDDC ana sunucuları, ağ ekipmanını fiziksel olarak yapılandırılmasına veya barındırılmasına gerek kalmadan veri merkezlerini ihtiyaçlara göre oluşturup yapılandırılma imkanı olan bulutta bulunur. SDDC'ler, veri merkezi işlevlerini soyutlamak, yönetmek ve dağıtmak için büyük ölçüde sanallaştırma teknolojilerine güvenir.[280]

Geçmişin yekpare veri merkezi sistemlerinden farklı olarak, SDDC tasarımı nasıl uygulanabileceği konusunda büyük esneklik sunar. SDDC, yakınsak altyapı (CI) ve hiper yakınsak altyapı (HCI) olmak üzere iki yoldan biriyle gerçekleştirilebilir.

5.1.4. Eski Altyapı Yığını (Legacy Infrastructure Stack)

Eski Altyapı, yığının her bir donanım öğesinin ayrı tutulduğu ve her birinin sonunda farklı bir üretici tarafından sağlanarak, birlikte çalışabilmesi için farklı olası teknolojilerden yararlanılarak yakınsak yapısının bir ön aşaması olarak kabul edilebilir. Bu altyapıyı oluşturan ögeler:

- Sunucular ve sanallaştırma hiper yöneticileri
- Depolama ağı
- Paylaşılan depolama dizisi (Yavaş, büyük diskler)
- SSD dizisi (Hızlı, küçük katı hal diskler)
- Yedekleme ve tekilleştirme dizisi ve yazılımı
- WAN optimizasyon cihazları
- Bulut ağ geçitleri

[280] https://www.delltechnologies.com/tr-tr/learn/data-storage/software-defined-data-center.htm Erişim Tarihi: 18.03.2021

- Depolama optimizasyon cihazları
- Veri koruma / Güvenlik Cihazları olarak sınıflandırılabilir ve bu ögelerin her biri, aralarında herhangi bir yazılım entegrasyonu olmaksızın ayrı öğeler olarak kabul edilmektedir. Bu sınıflandırma, bu ayrı sanallaştırma bileşenleri yığınını "eski" olarak ele alsa da bu model hala dünya çapında birden çok veri merkezinde yaygın olarak kullanılmaktadır.[281]

Bu yapı, kurumsal sanallaştırmaya yönelik ilk birleşik yaklaşımdır ve kararlı endüstri standartları ve protokollerine dayalı olarak birlikte çalışan farklı üreticilerin sağladığı donanımlardan yararlanılan güvenilir bir modeldir. Entegre Sistemler, yığının belirli bileşenlerinin belirli bir düzeyde entegrasyon elde ettiği bir modeldir. Bu bileşenler yine de ayrı ve fiziksel açıdan ayrılmış gibi görünse de, daha sıkı bir yazılım entegrasyonu ile birleşmiş altyapının temeli oluşturmaktadır. Bu yaklaşım ile farklı öğelerin yönetimi için birkaç yazılım parçası bir araya getirilerek genel olarak kolaylaştırılmış bir yönetim sağlamaya çalışılmıştır. Bu, konsolide edilmiş bir yazılım tanımlı Bilgi Teknolojisi yönetimi katmanına ulaşmaya yönelik ilk girişim olarak tanımlanabilir. Bu yaklaşım, dağıtım süreleri ve yönetim kolaylığı açısından bir gelişme ve yeniliği temsil etmektedir.

5.1.5. Yakınsak Altyapı Mimarisi (CI)

Sunucu sanallaştırma ile verimsiz bilgi işlem ve depolama kaynağı kullanımı sorunu çözülmüştür. Ancak altyapının uygulanabilir olmayan bir şekilde yükseltilmesi ve daha yavaş dağıtımlar sorunu devam etmiştir. CI çözümü bu sorunları gidermektedir. Ancak bir veri merkezindeki bilgi işlem, depolama ve ağ altyapılarını raf uygulamasında birleştirmektedir. Buradaki depolama doğrudan fiziksel sunucuya bağlıdır ve birden çok hesaplama düğümü arasında paylaşılmamaktadır. Burada bileşenler fiziksel olarak ayrıktır ancak tek bir kontrol düzlemine sahiptir.

5.1.5.1. Yakınsak Altyapı Mimarisinin Avantajları ve Dezavantajları

Bu altyapının avantajı, daha az kablolama, daha hızlı montaj ve daha kolay yönetim nedeniyle daha hızlı dağıtımdır. Ayrıca, kurucu bileşenler hala fiziksel olarak

[281] Alberto Perez Veiga, *Hyper Converged Infrastructures: Beyond virtualization*, University of Maryland University College, 2017, s.1-7.

ayrık olduğundan, bunları bağımsız olarak ölçeklendirmek mümkündür. Yatay ölçekleme ile bir rafa daha fazla bileşen eklenerek ve ek raf birimleri eklenerek dikey ölçeklendirme yapılabilir. Tekrarlayan kurulum görevleri ve sistem testi için saatler azaltılarak maliyetler düşürülebilir. Standartlaştırılmış bileşenler, altyapı silolarını azaltarak ve dolayısıyla altyapıyı konsolide ederek maliyetleri de düşürmektedir.[282]

Bu altyapının dezavantajı, üreticiye bağımlı olmaya yol açmasıdır; bu da daha az işlevsellik ve sınırlı özelleştirme seçenekleri ile sonuçlanabilir. Ayrıca, hali hazırda var olan yakınsak altyapıya yeni bileşenler eklemek karmaşık ve pahalı bir süreçtir. CI çözümleri, büyük ölçüde geleneksel 3 katmanlı veri merkezi mimarisinden hareket eden daha büyük kurumlar tarafından benimsenmektedir.

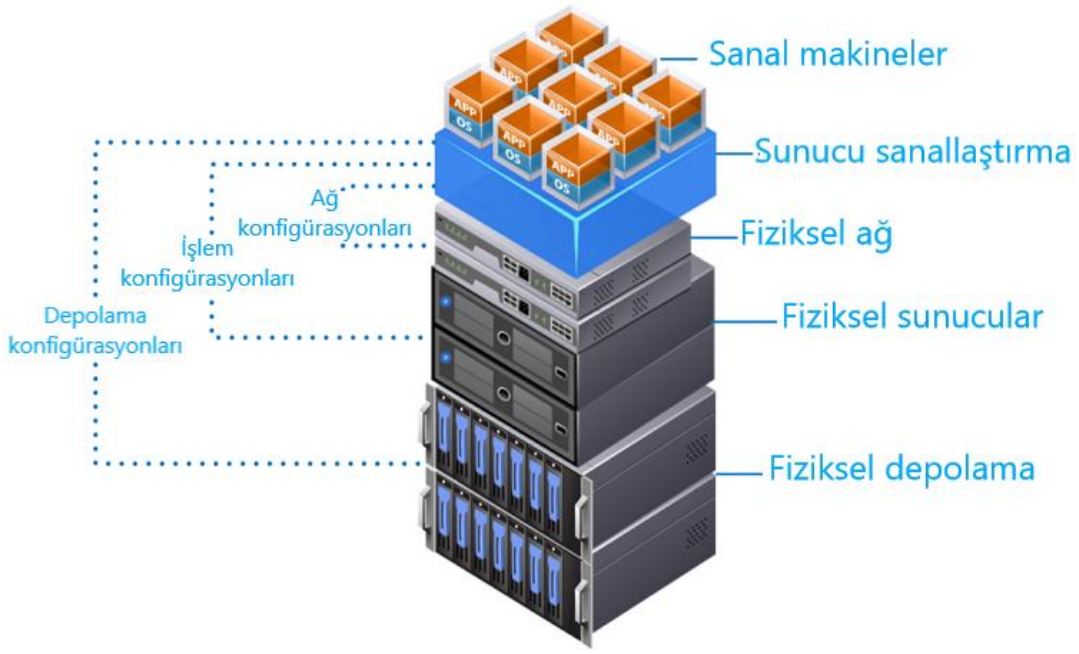
5.1.5.2. Yakınsak Altyapı Mimarisinin Sınırlamaları ve Dikkat Edilmesi Gereken Hususlar

- CI platformları, BT operasyonunda ve sistem yönetiminde daha fazla verimlilik sağlayabilir, ancak mevcut veri merkezleriyle tam olarak birlikte çalışmayabilir.
- CI dağıtımları, yatırım getirisi analizi ile açıkça gerekçelendirilmeli ve kapsamlı bir ilke kanıtı projesiyle incelenmelidir. Ayrıca kuruluşlar, CI tedarikçisinin ürün yol haritasını beklenen bilgi işlem ihtiyaçlarına göre değerlendirerek gelecekteki kesinti potansiyelini azaltabilir. CI durumu çok zayıfsa, kuruluşlar daha geleneksel bir veri merkezi modeliyle kalmalıdır.
- CI'ye yabancı bir cihaz bağlandığında, düşük performans, zayıf yönetim anlayışı veya diğer birlikte çalışabilirlik sorunlarına yol açabilen yeni bir heterojen durum ortaya çıkabilir.
- CI, özel bir bulut için bir platform olarak mevcut bir veri merkezi ortamına eklendiğinde, kendi benzersiz yönetim araçları ve performans standartlarına sahip bir altyapı adası olarak var olur.
- Mevcut herhangi bir altyapı, diğer yönetim araçlarıyla birlikte çalıştırılırsa iki farklı ortam meydana gelir. İki "farklı" ortamı bu şekilde desteklemek, BT personeli için çok fazla ek iş anlamına gelebilir.

[282] https://www.netapp.com/data-storage/flexpod/what-is-converged-infrastructure/ Erişim Tarihi: 12.03.2021

5.1.6. Hiper Yakınsak Altyapı Mimarisi (HCI)

Hiper yakınsama, genellikle x86 donanımından oluşan tek bir sistemde bilgi işlem, depolama ve sanallaştırma kaynaklarını sıkı bir şekilde bütünleştiren yazılım merkezli bir mimaridir. [283] HCI, ayrı sunucular, depolama ağları ve depolama dizilerinden oluşan eski altyapının yerini alan esnek yapı taşları oluşturmak için sunucuları ve depolamayı akıllı yazılımla dağıtılmış bir altyapı platformunda birleştirir. Daha spesifik olarak, veri merkezi sunucu donanımını yerel olarak bağlanmış depolama cihazlarıyla birleştirir ve eski altyapıyla ilişkili yaygın sorun noktalarını ortadan kaldırmak için dağıtılmış bir yazılım katmanı tarafından çalıştırılır.[284]Hiper yakınsak yapı şekil 5.4'te gösterilmiştir.



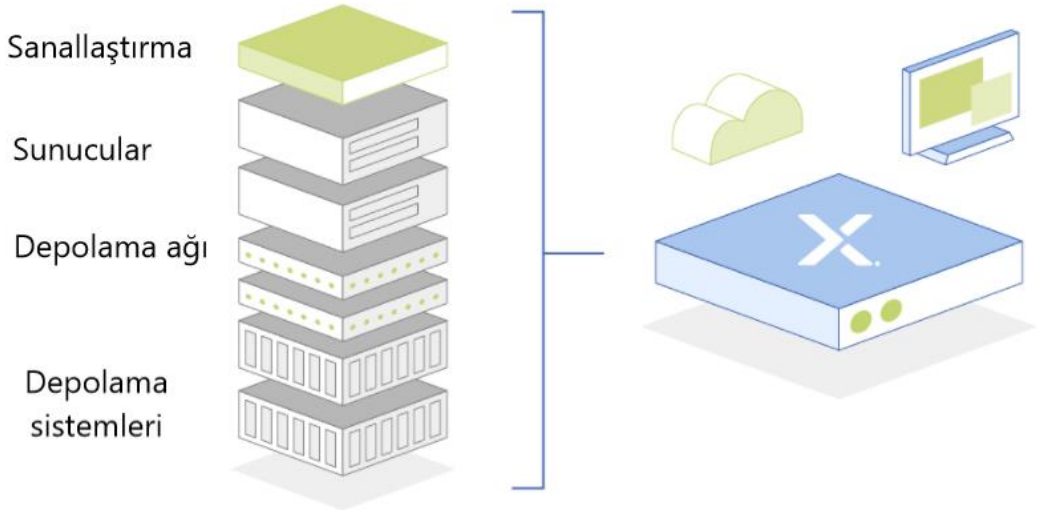
Şekil 5.33 : Hiper yakınsak altyapının fiziksel gösterimi[285]

HCI ve CI aynı hedefleri paylaşır ancak uygulamada farklılık göstermektedir. İki çözüm arasındaki en büyük fark, hiper yakınsak altyapının yazılım tanımlı bir çözüm olmasıdır ve fiziksel donanımdan ziyade yazılım yapı taşlarından yapılmıştır. HCI çözümde, hesaplama ve depolama tek bir çözümde birleştirilir ve tek bir kontrol

[283] http://www.americanacomputers.com/converged.html Erişim Tarihi: 17.03.2021
[284] https://www.nutanix.com/hyperconverged-infrastructure Erişim Tarihi: 17.03.2021
[285] https://www.cioandleader.com/article/2019/02/14/sublime-architecture-hyper-converged-infrastructure Erişim Tarihi 17.03.2021

düzlemine sahipken, ağ hâla fiziksel olarak ayrık kalır ve ayrı bir yönetim düzlemine sahiptir. Bir HCI'nin diğer önemli özelliği paylaşılan depolamadır. Diskler her bir hesaplama sunucusuna doğrudan bağlı olsalar bile, dağıtılmış bir şekilde birden çok sunucu arasında paylaşılır. Bazı çözümlerde yazılım denetleyicileri bir SAN'a bağlanır. Sistem, önceden yapılandırılmış bir çoğaltma faktörüne göre birden çok veri kopyasını koruduğundan, ham disk kapasitesi her zaman mevcut disk kapasitesi değildir. Bu, felaket kurtarma için yapılır ve herhangi bir düğüm veya disk arızası durumunda yüksek kullanılabilirliği sağlar. Kullanılabilir toplam depolama alanını artırmak için sıkıştırma ve tekilleştirme gibi yazılım tanımlı teknikler uygulanabilir. Yazılım tanımlı bir depolama çözümü olan depolama denetleyicisi, her bir düğümde bir hizmet olarak çalışır.

HCI, kolayca değiştirilebilen donanımın üzerine inşa edilmiştir ve yazılım tanımlı bir çözüm olarak, yakınsak altyapı çözümlerinde üreticiye bağlı kalma sorununu giderir. Depolamayı işlemin yakınında tutmak ve erişimini bilgi işlem sunucuları grubuna dağıtmak, yalnızca depolama I/O gecikmesini kontrol altında tutmakla kalmaz, aynı zamanda depolama kullanımını artırır. Herhangi bir donanımını ekleme esnekliği ve çok daha hızlı dağıtımla eklenen basit yönetim ile bu sistemin yakınsak yapıya göre daha elverişli hale getirir. Altyapı, yalnızca mevcut kümeye (düğüm grubu) yeni bir düğüm (bilgisayar ve depolama) ekleyerek doğrusal olarak ölçeklenir. Ancak yatay ölçekleme pahalıdır. Çünkü yalnızca bilgi işlem veya depolama kapasitesini yükseltmek isteseniz bile tamamen yeni bir düğüm eklenmesi gerekir. İşletim Sistemi lisansı CPU çekirdeği başına ise bu, yalnızca depolamaya ihtiyacı olan kurumlar için bir dezavantajdır. Birden çok yönetim yazılımı nedeniyle, HCI'da kaynak tüketimi ek yükü mevcuttur. Şekil 5.5'te örnek bir HCI küme gösterilmektedir.



Şekil 5.34 : Hiper yakınsak altyapı, sanallaştırmanın geleneksel bileşenlerini tek bir birleşik platformda birleştirir.[286]

5.1.6.1. Hiper Yakınsak Altyapı Mimarisinin Kullanım Durumları

- **Kurumsal Veri Merkezi Altyapısı:** HCI, raf sistemi kullandığı için merkezi depolama gerektiren geleneksel veri merkezi uygulamalarıyla iyi çalışmaktadır. Bu uygulamaların sanallaştırmaya ihtiyacı olmasa bile, HCI yine de çalışacak ve bu uygulamaları destekleyecektir.
- **Kurumsal VDI (Sanal Masaüstü Altyapısı):** Bu, Hewlett Packard Enterprise'a göre, HCI'nin arkasındaki asıl amaçtır.[287] HCI, her ikisi de "bir VDI ortamında kalıcı masaüstlerinin kullanılmasını sağlayan anahtar teknoloji" olarak görev yapan tekilleştirme ve depolama sıkıştırmasını ortaya çıkarır.
- **Özel Bulut:** HCI, esneklik ve erişilebilirlik avantajları dahil olmak üzere genel bulutun avantajlarıyla yerinde bulutu sunar. HCI, özel bulutu yerinde dağıttığından, ağ yöneticileri ağlarını izleme ve kontrol etme yeteneğine sahipken, BT dışı çalışanlar özel buluta kolayca erişebilir.
- **Uç Bilişim (Edge computing) ve Nesnelerin İnterneti (IoT):** Mikro veri merkezlerinde HCI dağıtımı, ağın ölçeklenebilirliğini ve esnekliğini artırdığından, IoT teknolojinin bağlanmasını sağlar.

[286] https://www.nutanix.com/hyperconverged-infrastructure Erişim Tarihi: 17.03.2021
[287] https://www.hpe.com/us/en/newsroom/press-release/2020/05/hewlett-packard-enterprise-advances-hci-solutions-for-expanding-remote-workforce-initiatives-in-wake-of-covid-19.html Erişim Tarihi : 24.03.2021

- **Uzak Ofisler ve Şube Ofisleri:** HCI, ofis konumlarında sunucuları kullanarak ve aynı zamanda tüm tesisler için birleşik performans yönetimi aşılayarak bir kuruluşun uzaktaki veya şube ofis konumlarından BT yönetimini basitleştirir.[288]

5.1.6.2. Yakınsak ve Hiper Yakınsak Altyapı Mimarilerinin Karşılaştırması

- Cl, bir veri merkezi bilgi işlem, depolama, ağ iletişimi ve sunucu sanallaştırmanın dört temel özelliğini tek bir kasaya getirir; kısacası CI donanıma dayanır ve yapı taşlarını kullanır. HCI ise yazılım tanımlıdır, yazılım aracılığıyla daha fazla bileşen arasında daha sıkı entegrasyon sağlar.[289]
- Depolama, hesaplama ve ağın bağımsız bileşenleri tek yazılım mimarisi tarafından kontrol edilirken, CI'da ayrı bileşenlerin kendi kontrol yazılımları vardır.
- CI temel olarak donanım odaklıdır ve yazılım tanımlı veri merkezi (SDDC) genellikle donanımdan bağımsızdır; HCI bu iki yönü birleştirir.
- HCI, CI'dan daha fazla iş yükü için uygundur.[290]
- HCI, depolamayı tüm bilgi işlem ve sanal makinelerle paylaşırken, CI paylaşmaz.
- HCI, CI'dan daha esnek, manevra kabiliyeti yüksek ve ölçeklenebilirdir.
- CI ve HCI arasındaki diğer bir temel ayrım, raf sistemidir. CI, hesaplama, depolama ve ağ iletişimini anahtar teslimi bir üründe birleştiren büyük, raf ölçekli bir platformdur. HCI ise normalde bir veya daha fazla çok çekirdekli sunucuyu yerel bir depolama dizisiyle birleştiren 1U veya 2U (raf ünitesi) sistemlerinden oluşur.
- Mimaride iki yaklaşım arasında farklılık gösterir. Yakınsak mimari depolama doğrudan fiziksel sunucuya eklenir. HCI mimarisi, kümedeki her düğümde bir hizmet olarak çalışan bir depolama denetleyicisi işlevine sahiptir.

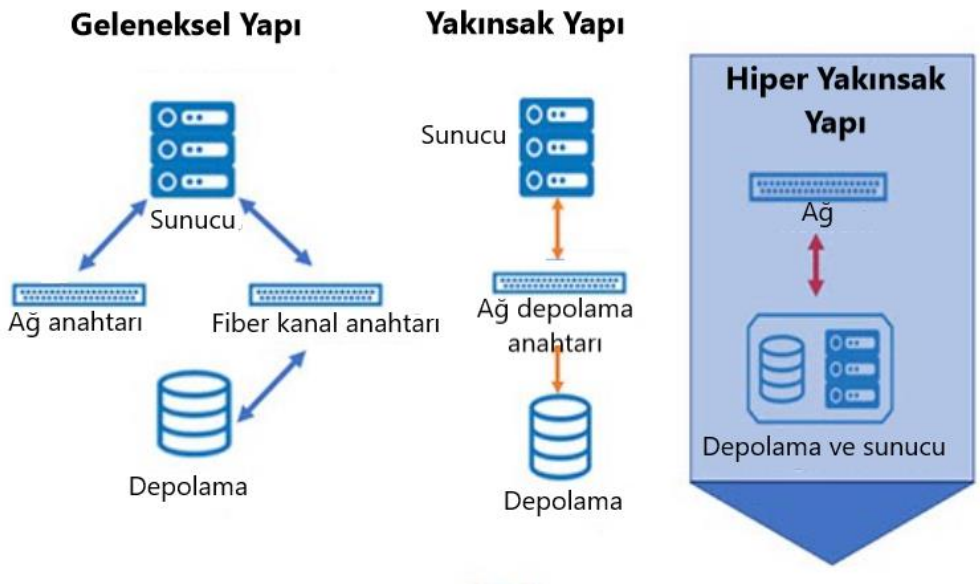
---

[288] https://www.sdxcentral.com/data-center/hyperconverged/definitions/hci-use-cases/ Erişim Tarihi: 26.03.2021

[289] http://www.americanacomputers.com/converged.html Erişim Tarihi: 18.03.2021

[290] Shaikh Abdul Azeem, Satyendra Kumar Sharma, *Study of Converged Infrastructure & Hyper Converge Infrastructre As Future of Data Centre*, International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017,900-903 doi: 10.26483/ijarcs.v8i5.3476

HCI'nin CI'e göre daha avantaj sağladığı olduğu durumlar olsa da, HCI CI'nın yerini almaz. Çünkü bu teknolojilerin her biri benzersiz faydalar içerir. Şekil 5.6'da geleneksel, yakınsak ve hiper yakınsak yapılar gösterilmiştir.



Şekil 5.35 : Geleneksel, yakınsak ve hiper yakınsak altyapıları

5.2. SANALLAŞTIRMANIN YARARLARI

Sanallaştırma, işletmeler için pek çok avantaj sunar, bu faydalar aşağıda kısaca açıklanmıştır.

- **Sunucu konsolidasyonu**

Sanallaştırma somut faydalar göstermeye devam ederek değerini artırmaktadır. Sunucu konsolidasyonu sanallaştırmanın en çok kullanıldığı alandır. Bunun nedeni, kuruluşların iş uygulamalarını destekleyen sunucuların sayısını ve türlerini azaltarak, önemli maliyet tasarrufları sağlamalarıdır.

- **Daha kolay yönetilebilirlik**

Yöneticiler, sanallaştırmayı kullanarak tek bir fiziksel makineden tüm sunucu / iş istasyonu gruplarını hem izleyebilir hem de yönetebilir. Bu da yönetilebilirliğin daha kolay yapılmasını sağlar. [291]

- **Uyumluluk sorunlarının ortadan kaldırılması**

Geçmişte MAC OS X, Linux veya Windows gibi farklı işletim sistemine sahip bilgisayarları aynı makinede çalıştırmak birçok uyumluluk sorunu yaratmaktaydı. Günümüzde sanal makineler kullanılarak birçok farklı işletim sistemi ve uygulama birbirini etkilemeden tek bir fiziksel makinede çalışabilmektedir.

- **Birden çok eşzamanlı işletim sistemi**

Birçok farklı türde uygulamayı çalıştırabilen birden çok eşzamanlı işletim sistemine sahip olma olanağı sağlayabilir.

- **Hata ayıklama**

Bir işletim sistemi veya bir aygıt sürücüsü gibi karmaşık yazılımların hatalarının ayıklanmasına, kullanıcının bunları yazılım kontrollerine sahip bir bilgisayarda çalıştırmasına izin vererek sorun gidermeye yardımcı olabilir.

- **Hata tespiti ve izolasyonu**

Bir sanal makinedeki herhangi bir hata, diğer sanal makineleri etkilememekte ve diğer tüm sistemler ve hizmetler çalışmaya devam ederken sorunlar otomatik olarak izole edilmektedir. Bu sorun bir yönetici tarafından düzeltilebilir veya incelenebilirken, diğer sanal makineler sorundan etkilenmeden çalışmaya devam etmektedir.

[291] S. U. Eren, 2020, s.10-11.

- **Yüksek güvenlik**

Yöneticiler, tek bir fiziksel makinedeki bilgileri ve uygulamaları farklı sanal makinelere ayırabilir. Bu, kullanıcıların erişim izinlerinin yönetilmesine olanak sağlar.

- **Bilgi güvenliğini sağlaması**

Sanallaştırma bilgi güvenliği için de çok şey sunmaktadır. VM'ler, süreçleri saldırganlardan ve kötü amaçlı yazılımlardan izole etmek için kullanılabilir, bu da sistemlerin ve uygulamaların başarılı bir şekilde saldırıya uğramasını veya bulaşmasını zorlaştırır. Uygulamalara kullanıcı erişimi sıkı bir şekilde kontrol edilebilir. Çünkü sanallaştırma özel uygulamaların son kullanıcı uygulamalarından izole edilmesine izin verir ve bu da ilkine yetkisiz erişimi çok zor hale getirir. Sanallaştırılmış bir ortamda çalışan bir sistem veya uygulama başarılı bir şekilde saldırıya uğramış olsa bile, saldırıdan kaynaklanan herhangi bir etki neredeyse her zaman zayıflatılır. Saldırganların ve kötü niyetli kodların saldırıları (özellikle kötü amaçlı yazılım tabanlı saldırılar) yayma yeteneği böylece azalır.

- **Kaynakların daha verimli kullanımı**

Birçok sanal makine, tek bir fiziksel makinede çalışabilir ve bu fiziksel makinelerin kaynaklarını, tek bir hizmet veya uygulama çalıştırmaya kıyasla çok daha verimli bir şekilde kullanabilir.

- **Taşınabilirlik**

Yine, sanal makine verileri fiziksel bir makinedeki dosyalarda saklanır. Bu, sanal makinelerin bir fiziksel makineden diğerine, işlevsellikte herhangi bir değişiklik olmaksızın zahmetsizce aktarılabileceği anlamına gelir.

- **Sorunsuz test edebilme imkânı**

Bir veya daha fazla sanal makine, test makinesi olarak kurulabilir. Bunlar daha sonra, günlük iş operasyonlarının işlevselliğini etkilemeden belirli uygulamaların veya programların kararlılığını test etmek için kullanılabilir.[292]

- **Hızlı dağıtım**

Bir sanal makinenin sabit diskleri genellikle fiziksel bir makinede tek bir dosya olarak temsil edilir. Bu durum sabit diskin kolayca kopyalanabileceği veya başka fiziksel makinelere aktarılabileceği anlamına gelir. Bir sanal makineyi "şablon" makine olarak kullanılıp kopyalar oluşturularak sanal sabit disk dosyası hızla yeni sanal makine klonları oluşturmak için kullanılabilir.

- **Daha az maliyet**

Sanallaştırmanın bir başka yararı da düşük güç tüketimidir. Mevcut, bilgi işlem kaynaklarının yoğun kullanımı, veri merkezi için daha uzun bir ömür ve daha geniş bir kâr anlamına gelir. Ek olarak, daha küçük bir sunucu ayak izini yönetmek daha kolaydır. Sanallaştırma sayesinde daha az fiziksel donanım gereksinimi, daha az güç ve soğutma gereksinimi, daha az fiziksel alan ve daha az personel gereksinimi gibi maliyetler azalmaktadır.

- **Uygulamaları ayırma yeteneği**

Birbiriyle çakışabilecek hizmetler ve uygulamalar, ayrı sanal makinelere yüklenebilir ve çalıştırılabilir. Bu hizmetler ve uygulamalar hala aynı fiziksel makinede çalıştığı için kaynaklar ve işlem gücü boşa gitmemektedir.[293]

- **Yük dengeleme**

Sanallaştırmanın bir diğer önemli yararı, birden çok dosya sistemi ve makine arasında dinamik yük dengeleme kapasitesidir. Geleneksel makinelerde işleme

[292] Ivanka Menken, Gerard Blokdijk, *Virtualization- The Complete Cornerstone Guide to Virtualization Best Practices_ Concepts, Terms, and Techniques*, Emereo Pty Ltd, 2010,2.ed
[293] a.g.m s.201

darboğazları oluştuğunda uygulamalar yavaşlar veya hatta durur. Dinamik yük dengeleme, bu tür darboğazların oluşmamasını sağlamaya yardımcı olarak uygulamaların kesinti olmadan çalışmasını sağlar. Bu, özellikle iş açısından kritik uygulamalar için önemlidir.

- **Test**

Sanallaştırma üretilmesi zor olan test senaryolarının oluşturulmasına yardımcı olur ve böylece yazılımın test edilmesini kolaylaştırır.

- **Zaman tasarrufu**

Sanallaştırma, yazılım teslim döngüsünün harcadığı süreyi büyük ölçüde azaltabilir. Geliştirme sürecini hızlandırarak ve sürecin güvenilirliğini artırarak, yazılım teslim döngüsü ile eğitim arasındaki boşluk büyük ölçüde azaltılır. Eğitim, yeni veya yükseltilmiş bir yazılım uygulamasının yayınlanmasının hemen ardından başlayabilir.[294]

- **Yeşil bilişim**

Sanallaştırma teknolojileri sürekli artan kaynak taleplerini karşılamak için kullanılabilir. Bu da yeşil bilişim için makul bir çözümdür. Kaynak sayısındaki üstel artışla birlikte enerji tüketiminin artması, fosil yakıt kullanımında artışa sebep olmaktadır. Karbondioksit emisyonundaki artış, dünyanın ısı dengesini düzenleyen sera gazı miktarını arttırmaktadır. Bu da küresel ısınma dediğimiz olguyu doğurmaktadır. Sanallaştırma teknolojileri kullanılan fiziksel sunucu ve diğer ekipman sayıları azaltılarak veri merkezlerinin oluşturduğu elektronik çöp miktarındaki artışın önüne geçilebilir. [295]

Sanallaştırmanın diğer önemli avantajları arasında yük devretme işlevselliği, sistemleri devre dışı bırakmadan sürdürme yeteneği, bilgi işlem kaynaklarını bir araya

[294] David Marshall vd., Advanced Server Virtualization, s.68
[295] Fatih ÖZTÜRK, *Sanallaştırma Teknolojilerinin Bilişim Sektörüne Sağladığı Faydalar ve Bazı Uygulama Örnekleri*, Uzmanlık Tezi, 2011, s.84

getirme yeteneği, her biri uygulama teslimi için bir konteyner görevi gören özel sanal makinelere (VM'ler) sahip olma yeteneği ve diğerleri yer almaktadır. [296]

[296] Edward Ray, Eugene Schultz, - *Virtualization security, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies*- CSIIRW '09, 2009, s.1–5, doi:10.1145/1558607.1558655

SONUÇ VE ÖNERİLER

Bu çalışmada öncelikle sanallaştırma teknolojisinin tanımı, tarihçesi ve sanal makine yöntemi açıklanmıştır. Sanallaştırma teknolojisinin yöntemi, kullanımı ve faydaları üzerine çalışılmış, sanallaştırma teknolojisinin getirdiği özellikler incelenmiştir. Sanallaştırma teknolojisi ile birlikte, geleneksel sistemlere göre daha ucuz maliyetlerle daha fazla uygulama ve servisin çalıştırılabileceği konularına değinilmiştir.

Sanallaştırma, günümüzün BT dünyasında muazzam bir etkiye sahip olan bir teknolojidir. Fiziksel bir bilgisayarı, genellikle sanal makineler veya konuk makineler olarak bilinen, kısmen veya tamamen izole edilmiş birkaç makineye bölen bir tekniktir. Sanallaştırma hayatımızın her alanında kullanılan bir teknolojidir ve çok fazla yöntemi vardır. Sunucu sanallaştırma başta olmak üzere; masaüstü sanallaştırma, ağ sanallaştırma, depolama sanallaştırma ve konteyner tabanlı sanallaştırma gibi yöntemleri ile sanallaştırma teknolojisi sürekli gelişmekte ve değişmektedir. Kendi avantajları ve dezavantajları olan çeşitli sanallaştırma teknolojileri bulunmaktadır.

Son yıllarda BT'nin gelişmesiyle birlikte güç kaynağı için daha yüksek gereksinimler ortaya çıkmaktadır. Bunun için kurumlarda atılan ilk adım sunucu sanallaştırmadır. Sunucu sanallaştırma teknolojisinin verimini anlamak için geleneksel fiziksel makine ile sanallaştırılmış ortamdaki makinelerin performans farkı araştırılmıştır. Bu kapsamda geleneksel fiziksel sunucunun kurumsal bilgi yapısında birçok eksikliğe sahip olduğu, sanal sunucunun yüksek bilgi güvenliği, düşük enerji tüketimi, yüksek kullanım oranı ve düşük bakım maliyeti gibi bariz avantajlara sahip olduğu görülmüştür.

Ayrıca sunucu sanallaştırma stratejisinin kullanımının kurumsal bilgilerin güvenliğini artırabileceğine ve sunucu kullanımının da önemli ölçü iyileştirildiğine inanılmaktadır. Sanal sunucu ağ mimarisini benimsediğinden, özellikle sunucu CPU ve bellek kullanımında kaynakların kullanımını en üst düzeye çıkarmak için sanal sunucuların sayısı kuruluşlarının gerçek zamanlı talebine göre artırılabilir veya azaltılabilir.

Veri işlemleri aksiyonların yer aldığı tüm işlemler depolama sanallaştırma teknolojisi ile ağ işlemleri ağ sanallaştırma teknolojisi ile daha hızlı ve verimli gerçekleştirilmektedir. Uygulama sanallaştırma ise kullanıcıların bir uygulamaya herhangi bir bilgisayardan erişmesine ve onu kullanmasına olanak tanıyan bir teknolojidir. Bununla birlikte, korona virüs salgınının büyümesiyle masaüstü sanallaştırma ayrı bir önem kazanmıştır. Günlük operasyonlara ve temel iş faaliyetlerine devam etmek için, uzaktan çalışma ve gelişmiş iletişim ve çalışma altyapısının mevcudiyeti çok gereklidir. Kısacası sanallaştırma ağ işlemleri, depolama, uygulama, 5G, mikro işlemler, uzaktan erişim gibi hayatın her alanında kullanılan bir teknoloji hâline gelmiştir. Sanallaştırma teknolojilerinin her birinin farklı işlevleri vardır. Her birinin kendine özgü avantajları ve dezavantajları vardır. Değişen iş ihtiyaçlarına göre geçilecek yöntemin belirlenmesi faydalı olacaktır. İyi bir sanallaştırma ortamı oluşturmanın anahtarı, sanallaştırılacak ortamı, kuruluşun ihtiyaçlarını ve hedeflerini dikkate alarak ayrıntılı bir şekilde incelemek ve uygun yöntemi belirlemek, bu yöntemi uygularken süreci iyi yönetmek ve sanal sistemlerin güvenliğini sağlamaktır.

Veri tüketiminin sürekli değişen manzarası ve kaynakları daha iyi optimize etmek ve düzenlemek için, her veri merkezi mimarisi önceki nesline göre gelişmektedir. Sunucu sanallaştırma, veri merkezinin çalışma şeklini tamamen değiştirdi; verimli kaynak kullanımına yol açtı ve maliyet etkinliğini artırdı. Yakınsak ve hiper yakınsak altyapılar daha fazla iyileştirmesini, kuruluşların dağıtım sürelerini kısaltmasını ve veri merkezinin bakımını kolaylaştırmasını sağladı. Bu tezde, tüm bu mimarilerin avantaj ve dezavantajları önceki mimarilere getirdiği iyileştirmelerle birlikte ele alındı.

Veri merkezi mimarisi zaman içinde gelişmiş olsa da, eski mimariler güncelliğini yitirmiş değildir. Bir mimarinin seçimi, kuruluşların ihtiyaç duyduğu şeye bağlıdır. Anabilgisayarlar sistemin en eski biçimi olsalar da modası geçmiş değildir. Bankacılık işlemlerinde, havayolu rezervasyon sistemlerinde büyük ölçekli birçok kurumda hâla yaygın olarak kullanılmaktadır. Çözümlerini düşük maliyetle hızlı bir şekilde uygulamak isteyen ve verilerinin gizliliğine değer veren kuruluşlar, geleneksel 3 katmanlı mimari yerine yakınsak veya hiper yakınsak bir altyapı çözümü

seçmektedir. Genellikle merkezi bir yönetimle verilere yüksek kullanılabilirlik ve güvenlik sağlamak için bu altyapı seçilir.

HCI, sanallaştırma ve BT stratejilerini yeni bir seviyeye taşıyan bir altyapıdır. Veri merkezleri, donanım merkezli bir yaklaşımdan, yazılım tanımlı mimarilerden yararlanan uygulama merkezli bir yaklaşıma geçmektedir. İlk yakınsak yapı girişimlerinden bu yana gelişen farklı aşamalar boyunca, nihayetinde tüm bir veri merkezinin tüm donanım katmanını soyutlamasını sağlamıştır. HCI, daha az zamanda, daha az fiziksel alan kullanarak, daha düşük güç tüketimi ve minimum yönetim ihtiyaçları ile daha ucuz hizmetler sunmayı vaat sağlamaktadır.

Radyo Ve Televizyon Üst Kuruluna İlişkin Öneriler

Sanallaştırmaya geçiş süreci için öneriler: Sanallaştırma projesi uygulama süreci sanallaştırma teknolojisine geçiş sürecinin önemli bir parçasıdır. Doğru planlanmamış ve uygulanmamış bir süreç başarısızlığa yol açmaktadır. Bu sebeple öncelikle Radyo ve Televizyon Kurulunda ve diğer kurumlarda sanallaştırma projesi uygularken yapılması gerekli görülen işlemler aşağıda önerilmiştir.

- Öncelikle işletim sistemi, CPU, bellek yükü, ağ bant genişliği, disk kullanımı dâhil olmak üzere her uygulamanın fiziksel sunucu yükü ayrıntılı bir şekilde araştırılmalıdır.
- Projeye başlanmadan önce bütün hatlarıyla planlanmalı, projenin genel tasarım planı düzenlenmeli ve formüle edilmelidir.
- Bu konuda uzman bir grubunun değerlendirmesinden sonra, proje ekibi projeyi eksik gördüğü noktalarda düzenleme yapmalıdır.
- Kurumsal sunucu sanallaştırma sürecinde oluşabilecek sistem sorunları ve güvenlik riskleri tahmin edilmeli ve güvenlik geri dönüş çözümü, bulut iş yönetim sisteminin güvenliği ve yüksek kullanılabilirliği sağlamak için formüle edilmelidir.

- Sanal makine ve fiziksel makine hizmet ekipmanları, veri merkezi sisteminde birbirlerinden izole edilmeli, böylece sunucuların karşılıklı etkileşimi önlenmelidir.

- Sanallaştırma yazılımın üzerinde çalışacak sunucu ve bileşenlerinin mutlaka sanallaştırma teknolojisini desteklemesi gerekir. Kurumun yedekleme alt yapısı değerlendirilmeli, eğer yetersiz ise bu husus proje kapsamında çözülmelidir.

- Sanallaştırma platformu ve yedekleme alt yapısında lisanslama mutlaka yapılmalıdır. Sanallaştırma projesinin en önemli parametrelerden birisi olan harici disk sisteminde de lisanslamanın unutulmaması önem arz etmektedir.

- Sanallaştırma projesi başından sonuna kadar mutlaka belgelendirilmeli ve sistem odasında kullanılan tüm donanımlara etiketlenme yapılmalıdır.

- Sanal ortamın güvenliğini sağlamak için proje kapsamında mutlaka çözüm sağlanmalıdır.

- Projenin genel uygulama planlama hedeflerine göre, ilgili donanım destek ekipmanlarının genel yerleştirme alanı, ilgili ekipmanın enerji tasarrufu ve gelecekteki ekipmanın sürdürülebilir genişlemesi dikkate alınarak planlanmalıdır.

- Sanallaştırma projesi uygulandıktan sonra bakım ve desteği sürdürülmeli; güvenlik zafiyetinin olmaması için gereken güncellemeler ve yamalar yapılmalıdır.

Sanal makine güvenliğini sağlamak için öneriler: Her biri kendi işletim sistemine ve uygulamalarına sahip sanal makinelerin birçoğu bir ana makinede çalışabilir. Bu, sanal makinelerdeki işlemlere sanki fiziksel bir bilgisayarda çalışıyorlarmış gibi bir yanılsama verir, ancak gerçekte ana makinenin fiziksel donanımını paylaşmaktadırlar. Birden çok işletim sisteminin fiziksel makinenin donanımını kullanmasına izin veren

yazılıma hiper yönetici denir. Hiper yöneticiler, ana makinenin işletim sistemi ile sanal ortam arasında bulunur.

Sanal olmayan ortamda, makinede çalışan uygulamalar birbirlerini görebilir ve hatta bazı durumlarda birbirleriyle iletişim kurabilirken, sanal ortamda bir konuk makinede çalışan programlar başka bir konuk makinede çalışan programlardan izole edilir, diğer bir deyişle konuk makineler, çalışan programlarına birlikte var olan bağımsız bilgisayarlar gibi görünmeleri sağlar. Bu yüzden,

- VM'nin güvenliği, işletim sistemine bağlıdır ve bu işletim sistemleri için bilgi güvenliği uygulaması tarafından zaten geliştirilen süreçlerin aynısını, sanki her VM fiziksel bir ana bilgisayarmış gibi izlenmelidir.

- Güvenlik açısından bakıldığında, bir VM ve bir fiziksel sunucu farklı değildir. Hizmet konsolunun VMFS erişimini kullanmanın yanı sıra, başka bir VM'ye erişmenin diğer tek yolu ağ bağlantılarıdır. Bu nedenle, ağın güvenliğini sağlamak birincil derecede önemlidir.

- COS hiper yöneticisinin VM disk dosyalarına erişebilmesi nedeniyle, servis konsolunun güvenliğini sağlamak da önemlidir.

- İzolasyon derecesi, bir sanal makinedeki güvenlik açıklarının ne sanal makineleri ne de temeldeki ana makineyi etkilememesi için yeterince güçlü olmalıdır.

Sanallaştırılan bilgisayarın sanallaştırılmayan bilgisayardan hiçbir farkı yoktur. Sanallaştırılmış ortam, normal ortamda ortak olan tüm geleneksel saldırılara açıktır. Durum, birden çok sanal makineye sahip sanallaştırılmış ortamda daha da kötüdür. Bu gibi ortamda güvenlik beklentileri daha yüksektir çünkü korunacak daha fazla sistem, daha fazla olası giriş noktası ve sanallaştırılmışta daha fazla ara bağlantı noktası vardır.

Saldırganlar, sanal makine ortamı için aktif olarak yeni kötü amaçlı yazılım programları geliştirmektedir. Root kit enfeksiyonları ve sanal ortamı algılayan ve kendisini buna göre değiştiren kötü amaçlı yazılımlar bunlardan bazılarıdır. Düşük

seviyeli hiper yönetici saldırıları ve kötü niyetli sanal sistemlerin konuşlandırılması bu ortama özgü birkaç olası saldırıdır. Hiper yönetici, ana bilgisayarın işletim sistemi ile sanal ortamı arasında yeni bir katman olduğundan, kötü amaçlı programlar için yeni fırsatlar yaratır. Hiper yönetici saldırıları, sanal makinelerde %61 oranıyla en fazla görülen saldırı çeşididir. Çünkü hiper yönetici temelde bir yazılım programıdır, dolayısıyla tüm geleneksel yazılım hatalarını ve güvenlik açıklarını barındırır.

Sanal sistemlere yönelik güvenlik tehditlerine alınacak önlem önerileri: Sanal sistemler Radyo ve Televizyon Üst Kurulunda BT alanında en çok kullanılan sistemlerin başında gelmektedir. Bu yüzden sanal sistemlerin güvenliği önem arz etmektedir. Sanal sistemlerin güvenliği için gerekli önlemler için öneriler aşağıda belirtilmiştir.

- Güvenlik duvarı ve antivirüs yazılımı kullanılmalıdır.
- Sistem güncellemeleri zamanında ve eksiksiz yapılmalıdır.
- Ağ trafiği izlenilmeli ve bant genişliği kurumun ihtiyacı olandan fazla olmalıdır.
- Göç işlemi yapıldığı sırada şifrelemek, verileri yönetmek ve güvenliği sağlamak için koruma modülü, meta veri yönetim modülü, güvenlik koruması modülü kullanılmalıdır.
- Sanal makinelerin, tıpkı diğer BT cihazları gibi güvenlik kaydı sistemlerine entegre edilmeli ve kayıtları eksiksiz tutulmalıdır.
- VM denetimi düzenli bir şekilde yapılmalı, VM üzerindeki gereksiz anlık görüntüler silinmelidir.

Masaüstü sanallaştırmanın hayata geçirilmesi önerisi: Masaüstü sanallaştırma koranavirüs salgınıyla beraber daha da önem kazanmış bir uygulama haline gelmiştir. Masaüstü sanallaştırma teknolojisi ile masaüstü sanal hâle getirilmiştir. Masaüstü sanallaştırmanın sağlayacağı avantajlar aşağıda belirtilmiştir.

- Kullanıcılar herhangi bir zaman diliminde herhangi bir yerde istedikleri cihaz ile kişisel masaüstlerine giriş yapabilirler.
- Masaüstü bilgi işlem uç nokta cihazlar yerine ana sunucuda gerçekleşir. Bu sayede uç nokta donanım gereksinimleri daha düşük olacaktır. Bu da maliyet açısından avantaj sağlayacaktır.
- Merkezi yönetim sayesinde sanallaştırılmış masaüstleri tek seferde yamalanma, güncelleme ve değiştirilmesine olanak sağlar. Aynı zamanda eksiksiz bir felaket kurtarma stratejisine olanak sağlar.
- Uygulamalar istemci cihaz yerine veri merkezindeki ana sunucuda çalıştığı için kurumların gizliliklerinin tam olarak korunmasını sağlamaktadır.

Masaüstü sanallaştırmanın sağladığı yararlar neticesine bu teknolojinin uygulanmasının birçok avantaj getirdiği söylenebilir.

KAYNAKÇA

Eren, S. U. (2020). Vmware Ve Hyper-V Sanallaştırma Sistemlerinin Performans Ve Yüksek Kullanılabilirliğinin Deneysel Olarak Karşılaştırılması. Yayınlanmış Yüksek Lisans Tezi, T.C. Maltepe Üniversitesi, İstanbul,s.7.

Abdullah, M., Qidri, S., & Nuryadi , W. (2020). Failover Cluster Nodes and ISCSI Storage Area Network on Virtualization Windows Server 2016. *Jurnal Online Informatika, 5*, 89-96. doi:10.15575/join. v5i1.5

Academia. (2021, 02 23).

https://www.academia.edu/31096053/Cloud_Computing_Types_Architecture_Applications_Concerns_Virtualization_and_Role_of_IT_Governance_in_Cloud adresinden alındı

Acharya, S., & Liu, P.-H. (2013). *US Patent No. US Patent : 8,346,726 B2.*

Activedirectoryservice. (2021, 03 24).

http://activedirectoryservice.blogspot.com/2011/06/hyper-v-live-migration-step-by-step.html adresinden alındı

Aksakallı, I. (2019). Bulut Bilişimde Güvenlik Zafiyetleri, Tehditler Ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi . *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, s:8-34.

Amazon. (2021, 02 08). https://aws.amazon.com/tr/autoscaling/ adresinden alındı

Americanacomputers. (2021, 03 17).

http://www.americanacomputers.com/converged.html adresinden alındı

Antunes, N., & Vieira, M. (2012). *Defending against web application vulnerabilities.* Computer.

Azab, M., & Eltoweissy, M. (2016). MIGRATE: Towards a Lightweight Moving-target Defense against Cloud SideChannels. *IEEE Symposium on Security and Privacy Workshops*, (s. 96-103).

Azeem, S., & Sharma, S. (May-June 2017). Study of Converged Infrastructure & Hyper Converge Infrastructre As Future of Data Centre. *International Journal of Advanced Research in Computer Science*, s.900-903. doi:10.26483/ijarcs.v8i5.

Bakhan, T. (2020). Virtualization mechanisms and its tools: A comprehensive survey. , Vol. 9 No. 4,s.346-355. doi:10.21817/ijcsenet/2020/v9i4/200904022

Barham, P., Fraser, K., Hand, S., Harris, T., Dragovic, B., Ho, A., . . . Warfield, A. (2004). Xen and the Art of Virtualization, University of Cambridge Computer Laboratory, Cambridge, 2004.

Barrett, D., & Kipper, G. (2010). *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments.* Burlington: Syngress.

Berger, S., Caceres, R., Goldman, K., Perez, R., Sailer, R., & Van Doorn, L. (2006). vTPM: virtualizing the trusted platform modüle. *Proceedings of the 15th conference on USENIX Security Symposium.*

Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., & Valdez, E. (2007). *TVDc: Managing Security in the Trusted Virtual Datacenter*. Hawthorne, NY, USA: IBM T. J. Watson Research Center.

Beyaz. (2021, 02 15).

https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html adresinden alındı

Bochs. (2021, 01 25). https://bochs.sourceforge.io/ adresinden alındı
Boettiger, C. (2014). An introduction to Docker for reproducible research, with examples from the R environment. s.3-8.
Bui, T. (2015). Analysis of Docker Security. *Aalto University School of Science*. arXiv preprint arXiv:1501.02967.
Büyükgöze, S. (2016). Kırklareli University Kayalı Campus' Desktop Virtualization. *Research Journal of Business and Management, 3*(4), 306-313.
Büyükyılmaz, E. (2016). Sunucu Sanallaştırma Teknolojili Veri Merkezi Ve Bir Uygulaması, Yayınlanmış Yüksek Lisans Tezi,Haliç Üniversitesi,İstanbul.
Campbell, T. (2016). *Practical Information Security Management: A Complete Guide to Planning and Implementation.* Australia: Apress, Chapter 1: Evolution of a Profession,s.1-14, .
Chae, M., Lee, H., & Lee, K. (2017). A performance comparison of linux containers and virtual machines using Docker and KVM. South Korea: Springer Science. doi:https://doi.org/10.1007/s10586-017-1511-2
Chaganti, P. (2007). *Xen Virtualization: A fast and practical guide to supporting multiple operating systems with the Xen hypervisor*. Birmingham: Packt Publishing.
Chi-Hsiung Liu, P. &. (2013). *US Patent No. 8,346,726 B2*.
Chirammal, H. D., Mukhedkar, P., & Vettathu , A. (2016). *Mastering KVM Virtualization.* Birmingham: Packt Publishing.
Cioandleader. (2021, 02 17). https://www.cioandleader.com/article/2019/02/14/sublime-architecture-hyper-converged-infrastructure adresinden alındı
Citrix. (2020, 10 02). https://www.citrix.com/tr-tr/glossary/what-is-application-virtualization.html adresinden alındı
Citrix. (2021, 01 28). https://www.citrix.com/tr-tr/glossary/what-is-application-virtualization.html adresinden alındı
Citrix. (2021, 02 22). https://www.citrix.com/tr-tr/glossary/vdi.html adresinden alındı
Citrix. (2021, 02 08). https://www.citrix.com/ adresinden alındı
Colinux. (2021, 01 25). http://www.colinux.org/ adresinden alındı
Data-storage. (2021, 03 29). https://www.data-storage.uk/software/software-defined-storage/ adresinden alındı
Delltechnologies. (2021, 03 18). https://www.delltechnologies.com/tr-tr/learn/data-storage/software-defined-data-center.html adresinden alındı
Dnsstuff. (2021, 02 10). https://www.dnsstuff.com/what-is-virtual-machine-server-vm-sprawl adresinden alındı
Docker. (2021, 01 14). https://www.docker.com/ adresinden alındı
Dong, Y., & Lei, Z. (2019). *An Access Control Model for Preventing Virtual Machine Hopping Attack.* Shanghai, China: School of Computer Engineering and Science, Shanghai University.
Dua, R., Raja, R. A., & Kakadia, D. (2014). Virtualization vs Containerization to support PaaS. *IEEE International Conference on Cloud Engineering, ,* (s. s.610-614). doi:10.1109/ic2e.2014.41
Ekiz, A. (2019). Informatıon Securıty Management System And Informatıon Securıty Risk Management Methodology Development,. Yayınlanmış Yüksek Lisans Tezi, Yeditepe Üniversitesi,s.6.

Erdoğan, S. E. (2020). Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ ISO 27001 Standartının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi. İstanbul Kültür Üniversitesi, Yayınlanmış Yüksek Lisans Tezi, s.41.

Fries, R., Hunt, G., & Balakrishnan, S. (2016). *United States Patent No. 9.286,182 B2.*

Gavanda, M., Mauro, A., Valsecchi, P., & Novak, K. (2019). *Mastering VMware vSphere 6.7* (2. b.). Birmingham: Packt Publishing.

Gökhan, C. (2017). Scalability Issues In Big Data On Cloud: A Comparison of Virtual Machines and Linux Containers. Atılım Üniversitesi, Yayınlanmış Yüksek Lisans Tezi,Ankara.

Harji , A. S., Buhr, P. A., & Brecht, T. (2013). Our Troubles with Linux Kernel Upgrades and Why You Should Care. *ACM SIGOPS Operating Systems Review, 47*(2), s. 66-72.

Hashizume, K., G Rosado, D., Fernández-Medina, E., & Fernandez, E. (2013). *An analysis of security issues for cloud computing, Journal of Internet Services and Applications* .

Hess, K., & Newman, A. (2010). *Practical Virtualization Solutions Virtualization from the Trenches* (1st ed b.). Pearson Education.

Hpe. (2021, 03 24). https://www.hpe.com/us/en/newsroom/press-release/2020/05/hewlett-packard-enterprise-advances-hci-solutions-for-expanding-remote-workforce-initiatives-in-wake-of-covid-19.html adresinden alındı

Huang, Y.-L., Chen, B., Shih, M.-W., & Lai, C.-Y. (2012). Security Impacts of Virtualization on a Network Testbed. IEEE Sixth International Conference on Software Security and Reliability, s.71-77.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard.* Artech House. , ISBN 13: 978-1-60807-930-8.

Ibm. (2020, 09 19). https://www.ibm.com/cloud/learn/desktop-virtualization adresinden alındı

Ibm. (2020, 11 28). https://www.ibm.com/cloud/learn/virtual-machines#toc-how-virtua--B5v9urC adresinden alındı

Ibm. (2020, 11 28). https://www.ibm.com/cloud/learn/virtual-machines#toc-how-virtua--B5v9urC adresinden alındı

Ibm. (2021, 02 19). https://www.ibm.com/cloud/blog/what-is-virtual-desktop-infrastructure adresinden alındı

Ibm. (2021, 04 04). https://www.ibm.com/docs/en/aix/7.2?topic=configuration-trusted-computing-base adresinden alındı

Iec. (2020, 12 17). https://www.iec.ch/what-we-do/how-iec-funded adresinden alındı

Intraway. (2021, 11 29). https://www.intraway.com/blog/nfv-benefits adresinden alındı

Iso. (2020, 12 17). https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en adresinden alındı

Itpro. (2021, 02 17). https://www.itpro.co.uk/642409/crisis-malware-infects-virtual-machines adresinden alındı

Jain, S. M. (28.11.2019). Linux Containers and Virtualization : A Kernel Perspective. doi:https://doi.org/10.1007/978-1-4842-6283-2

Jmeter. (2021, 02 07). http://jmeter.apache.org/ adresinden alındı

Kaneda, S., Matsumura, N., İkegami, F., Shimizu, K., & Ikuta, Y. (Feb. 20, 1980,). *US Patent No. 4,400,769.*

Karpoff, W., & Lake, B. (2002). *US Patent No. 6,857,059 B2*.

Kusnetzky, D. (2011). *Virtualization: A Manager's Guide, O'relly.*

L, M., D, A., & A, J. (2014). Virtualization in Cloud Computing. *Journal of Information Technology & Software Engineering, 4*(2), 1-3. doi:10.4172/2165-7866.1000136

Li, C., Ding, L., Needle, B., City, F., & Rawat, M. (17.11.2016). *US Patent No. US010802927B2*.

Li, S.-H. Y.-C.-H.-C. (2015). Effects of virtualization on information security. . Computer Standards & Interface,s.1-8.

Li, Z., Kihl, M., Lu, Q., & Andressan, J. (2017). Performance Overhead Comparison between Hypervisor and Container based Virtualization,College of Computer and Communication Engineering, China University of Petroleum, s.1-8.

Lindner, M., McDonald, F., McLamon, B., & Robinson, P. (2011). Towards Automated Business-driven Indication and Mitigation of VM Sprawl in Cloud Supply Chains. 12th IFIP/IEEE International Symposium on Integrated Network Management and Workshops Dublin , Ireland. doi:10.1109/inm.2011.5990505

Linux. (2021, 01 11). http://www.linux-vserver.org/Welcome_to_Linux-VServer.org adresinden alındı

Linuxcontainers. (2021, 01 11). https://linuxcontainers.org/lxc/documentation/ adresinden alındı

Linuxcontainers. (2021, 01 18). https://linuxcontainers.org/lxd/ adresinden alındı

Linux-kvm. (2021, 02 25). https://www.linux-kvm.org/page/Main_Page Erişim Tarihi 25.02.2021 adresinden alındı

Liu, D., Lee, J., Jang, J., Nepal, S., & Zic, J. (2010). A Cloud Architecture of Virtual Trusted Platform Modules. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, (s. s.804-811).

Lwn. (2020, 12 14). https://lwn.net/Articles/705160/ adresinden alındı

M. Khalil, I., Khreishah, A., & Azeem, M. (2014). *Cloud Computing Security: A Survey, Computers.* doi:10.3390/computers3010001

Marshall, D., Reynolds, W. A., & McCrory, D. (2006). *Advanced Server Virtualization: VMware and Microsoft Platforms in the Virtual Data Center*. Boca Raton, USA: Taylor & Francis Group.

Marttin, V., & Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *, Mühendislik Bilimleri ve Tasarım Dergisi, 1*(1), s.49-56.

Menken, I., & Blokdijk, G. (2010). *Virtualization- The Complete Cornerstone Guide to Virtualization Best Practices_ Concepts, Terms, and Techniques* (2 b.). Emereo Pty Ltd.

Merdan, T. (2010). Sanallaştırmanın Bilgi Teknolojilerine Getirdiği Yenilikler ve Uygulamaları. İstanbul.

Microsoft. (2021, 01 13).

https://docs.microsoft.com/en-us/virtualization/windowscontainers/about/containers-vs-vm adresinden alındı

Miller, K., & Pegah, M. (2007). Virtualization, Virtually at the Desktop, Ringling College of Art and Design. *Proceedings of the 35th annual ACM SIGUCCS fall conference* (s. 255-260). SIGUCCS '07. doi:10.1145/1294046.1294107

Milli, O. (2016). Yayınlanmış Yüksek Lisans Tezi. *Server Virtualization For Enterprises and an Application*.

Monckton, R. D. (2012). *Patent No. O080993.91B1*. Aralık 20, 2019 tarihinde alındı

Nakivo. (2021, 02 14). https://www.nakivo.com/blog/key-differences-between-vmware-horizon-and-vdi/ adresinden alındı

Netapp. (2020, 09 17). https://www.netapp.com/virtual-desktop-infrastructure/what-is-virtual-desktop-infrastructure adresinden alındı

Netapp. (2021, 02 23). https://www.netapp.com/devops-solutions/what-are-containers/ adresinden alındı

Netapp. (2021, 03 12). https://www.netapp.com/data-storage/flexpod/what-is-converged-infrastructure/ adresinden alındı

Nutanix. (2020, 09 22). https://www.nutanix.com/info/desktop-as-a-service-daas adresinden alındı

Nutanix. (2021, 03 17). https://www.nutanix.com/hyperconverged-infrastructure Erişim Tarihi: 17.03.2021 adresinden alındı

Olzak, T., Boomer, J., Keefer, R. M., & Sabovik, J. (2010). *Microsoft Virtualization: Master Microsoft Server, Desktop, Application, and Presentation Virtualization.* Burlington, USA: Syngress.

Openvz. (2020, 08 20). https://openvz.org/ adresinden alındı

Openvz. (2021, 01 11). https://openvz.org/ adresinden alındı

Öklü, A. (2013). Yeşil Bilgi Teknolojisi, Özel Bulut ve Karma Bir Sanallaştırma Uygulaması:Orman Genel Müdürlüğü, Yayınlanmış Yüksek Lisans Tezi. Kırıkkale: Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü.

Öztürk, A. (2013). Bilgi Teknolojisi Altyapılarının Yönetiminde Yeni Nesil Yaklaşımlar;Bilgi Teknolojileri ve İletişim Kurumu Altyapısına Yönelik Bir Model Önerisi. Bilgi Teknolojileri İletişim Kurumu, Teknik Uzmanlık Tezi,Ankara.

Öztürk, F. (2011). Sanallaştırma Teknolojilerinin Bilişim Sektörüne Sağladığı Faydalar ve Bazı Uygulama Örnekleri, Uzmanlık Tezi. Ankara.

Pandora FMS. (2021, 02 22). https://pandorafms.com/tr/sanallastirma-izleme/ adresinden alındı

Parallells. (2020, 10 16).

https://www.parallels.com/blogs/ras/application-virtualization/ adresinden alındı

Patwardhan, K., & Dudala, K. (16.06.2020). *US Patent No. 2020/0019466 A1*.

Pershin, A., Langouev, I., R. Pidur, S., Shah, R., & Silver, J. (2011, Ekim 11). *US Patent No. US 8,037,032 B2*. Aralık 20, 2019 tarihinde alındı

Portnoy, M. (2016). *Virtualizations Essentials.* içinde Indiana: Sybex.

Prof. Joy, A. M. (2015). Performance comparison between Linux containers and virtual machines. *International Conference on Advances in Computer Engineering and Applications (ICACEA)* (s. s.342-346). Ghaziabad, India: IMS Engineering College.

Pujolle, G. (2020). *Software Networks: Virtualization, SDN, 5G and Securit.* USA: John Wiley & Sons.

Radek , S., Silhavy, P., & Prokopova, Z. (2016). *Software Engineering Perspectives and Application in Intelligent Systems,.* Advances in Intelligent Systems and Computing 465, Springer International Publishing, Switzerland, s.242-245.

Ray, E., & Schultz, E. (2009). Virtualization Security. (s. s.1-5). Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence

Research Cyber Security and Information Intelligence Challenges and Strategies- CSIIRW '09. doi:10.1145/1558607.1558655

Redhat. (2019). Aralık 26, 2019 tarihinde https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor adresinden alındı

Redhat. (2019, 12 26). https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor Erişim Tarihi :26.12.2019 adresinden alındı

Redhat. (2021, 01 29). https://www.redhat.com/en/topics/virtualization/what-is-nfv adresinden alındı

Resmi Gazete. (2021, 03 31). https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm adresinden alındı

Reuben, J. (2007). A Survey on Virtual Machine Security. . *Helsinki University of Technology, TKK T-110.5290 Seminar on Network Security.*

Sareen, P. (2013). Cloud Computing: Types, Architecture, Applications,Concerns, Virtualization and Role of IT Governance in Cloud. *International Journal of Advanced Research inComputer Science and Software Engineering*, *3*(3), s. 533-537.

Schaffrath, G., Werle, C., Papadimitriou, P., Feldmann, A., Bless, R., Greenhalgh, A., . . . Mathy, L. (2009). *Network Virtualization Architecture: Proposal and Initial Prototype,*. Barcelona.

Sdxcentral. (2021, 03 26). https://www.sdxcentral.com/data-center/hyperconverged/definitions/hci-use-cases/ Erişim adresinden alındı

Sentia. (2021, 02 03). https://www.sentia.ca/Blog/ArtMID/1133/ArticleID/81/The-Top-10-Characteristics-and-Benefits-of-Hyper-convergence adresinden alındı

Soyer, M. D. (2021). Sanallaştırmada Güvenlik Açıkları, Tehditleri ve Bunların Çözümleri,. Proje Raporu, s.8.

Starwindsoftware. (2021, 03 24). https://www.starwindsoftware.com/blog/virtual-workload-migration-with-vmware adresinden alındı

Statista. (2021, 03 14). https://www.statista.com/statistics/1139931/adoption-virtualization-technologies-north-america-europe adresinden alındı

Statista. (2021, 03 03). https://www.statista.com/statistics/638613/worldwide-data-center-storage-used-capacity/#statisticContainer adresinden alındı

Strunk, A. (2012). Costs of Virtual Machine Live Migration: A Survey. *2012 IEEE Eighth World Congress on Services*, (s. 323-329). Dresden. doi:10.1109/SERVICES.2012.23

Strunk, A. (2015). Costs of Virtual Machine Live Migration: A Survey. Chair of Computer Networks Faculty of Computer Science ,Technical University of Dresden, Germany.

Studnia, I. A. (2012). Survey of Security Problems in Cloud Computing Virtual Machines. . *Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012),*, s.61-74.

Szefer, J., & Lee, R. (2012). Architectural Support for Hypervisor-Secure Virtualization, Princeton University, ASPLOS.

Şeşen, E. (2017). *Masaüstü Sanallaştırma Teknolojilerinin Performanslarının Analizi,*. Düzce Üniversitesi, Yayınlanmış Yüksek Lisans Tezi, Düzce.

Tank, D., Aggarwal, A., & Chaubey, N. (2019). Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. Bharati Vidyapeeth's Institute of Computer Applications and Management. doi:10.1007/s41870-0

Techopedia. (2021, 02 09). https://www.techopedia.com/definition/30475/vm-sprawl adresinden alındı

Techtarget. (2021, 02 22). https://searchservervirtualization.techtarget.com/definition/service-virtualization adresinden alındı

Terroza, A. (2015). Information Security Management System (ISMS) Overview. The Institute of Internal Auditors. https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information Security Management System (ISMS) Overview.pdf adresinden alındı

Tipton, H., & Krause, M. (2006). *Information Security Management Handbook* (5. b.). (ISC)2 press,ISBN 0-8493-9561-5.

Tokdemir, E. (2019). An Information Security Management System Approach And Technical Security Best Practices For The Enterprise Companies,. Yayınlanmış yüksek lisans tezi, Bahçeşehir Üniversitesi, İstanbul.

Tuomas Vase. (2015). Advantages of Dockers. s.20-24. Information Systems Science,University of Jyväskylä.

Turnbull, J. (2019). *The Docker Book: Containerization is the new virtualization.*

Tuygun, M. (2019). ISO27001 Bilgi Güvenliği Yönetim sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. . Yayınlanmış Yüksek Lisans Tezi, Gazi Üniveristesi,Ankara.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2021, 03 31). https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf adresinden alındı

Vase, T. (2015). Advantages of Dockers.

Vasilyev, A., & Baranov, A. (2015). *Saint-Petersburg Patent No. US 9,116,846 B2.* Aralık 23, 2019 tarihinde alındı

Vaughan-Nichols, S. (2008). Virtualization sparks security concerns, Computer 41 (8). s.13-15. doi:10.1109/mc.2008.276

Vaughan-Nichols, S. J. (2008). Virtualization sparks security concerns. *Computer, 41*(8), s.13-15. doi:10.1109/mc.2008.276

Vcenter. (2020, 06 18). http://vcenter.com/ adresinden alındı

Veiga, A. (November 2017). Hyper Converged Infrastructures: Beyond virtualization.

Virtualbox. (2021, 02 07). https://www.virtualbox.org/ adresinden alındı

Virtualbox. (2021, 02 07). https://www.virtualbox.org/ adresinden alındı

Vmware. (2019, 9 2). https://www.vmware.com/topics/glossary/content/hypervisor adresinden alındı

Vmware. (2020, 12 19). https://www.vmware.com/topics/glossary/content/network-virtualization adresinden alındı

Vmware. (2020, 08 20). https://www.vmware.com/products/esxi-and-esx.html adresinden alındı

Vmware. (2021, 02 29). https://www.vmware.com/topics/glossary/content/application-virtualization adresinden alındı

Vmware. (2021, 02 08).

https://www.vmware.com/tr/products/workstation-player/workstation-player-evaluation.html adresinden alındı

Vojtesek, J., & Pipis, M. (2016). Virtualization of Operating System Using Type-2 Hypervisor. Software Engineering Perspectives and Application in Intelligent Systems, s. 239–247. . doi:10.1007/978-3-319-33622-0_22

Vsphere. (2021, 03 22). https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-9272E3B2-6A7F-427B-994C-B15FF8CADC25.html adresinden alındı

Vxug. (2021, 02 19). https://vxug.fakedoma.in/archive/Symantec/threats-to-virtual-environments-14-en.pdf Erişim Tarihi : 19.02.2021 adresinden alındı

Wang, Z., & Jiang, X. (2010). *HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity*. Washington, DC, USA: Department of Computer Science North Carolina State University, IEEE Computer, Society.

Wikipedia. (2020, 08 06). https://en.wikipedia.org/wiki/Fibre_Channel adresinden alındı

Wikipedia. (2020, 12 24). https://en.wikipedia.org/wiki/Hyperjacking#Known_attacks adresinden alındı

Wikipedia. (2021, 03 24). https://en.wikipedia.org/wiki/Information_security_management#cite_note-HumphreysImplement16-3 adresinden alındı

Xavier, M., V. Neves, M., Rossi, F. D., Ferreto, T. C., Lange, T., & Cesar A. F. De, R. (2013). Performance Evaluation of Container-based Virtualization for High Performance Computing Environments. *21st Euromicro International Conference on Parallel,Distributed, and Network-Based Processing*, (s. 233-240). doi:10.1109/PDP.2013.41

Xiaopeng, G., Sumei, W., & Xianqin, C. (2010). Vnss: A Network Security Sandbox For Virtual Computing Environment. *IEEE Youth Conference on Information, Computing and Telecommunications*, (s. s. 395–398.). doi:10.1109/ycict.2010.5713128

Xing , Y., & Zhan, Y. (2012). Virtualization and Cloud Computing. *Future Wireless Networks and Information Systems,Lecture Notes in Electrical Engineering Book Series, 143*, s. 305–312.

Yan, L. (2011). Development and Application of Desktop Virtualization Technology . *IEEE 3rd International Conference on Communication Software and Networks* , (s. 326-329). doi:10.1109/ICCSN.2011.6013725

Yu, H., Guo, J., Wu, L., Wu, S., & Peng, B. (2021). Application of Server Virtualization Technology in Power. O. C. Center (Dü.), *240th ECS Meeting*. içinde Orlando,Fl: Journal of Physics: Conference Series. doi:10.1088/1742-6596/1744/2/022008

Yubin, X., Liu, Y., Chen, H., & Zang, B. (2012). Defending against VM Rollback Attack", Konferans, 2012,. *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*. doi:10.1109/dsnw.2012.6264690

Zhang, F., Chen, J., Chen , H., & Zang, B. (2011). CloudVisor : Retrofitting Protection of Virtual Machines in Multi-tenant Cloud with Nested Virtualization. s. 203–216. Portugal: SOSP '11: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, s.203-216. doi:10.1145/2043556.2043576

Zhang, F., Huang, Y., Wang, H., Chen, H., & Zang, B. (2008). PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. *Third Asia-Pacific Trusted Infrastructure Technologies Conference*, (s. s.9-18).

Zimba, A., & Chama, V. (2018). Cyber Attacks in Cloud Computing: Modelling Multi-stage Attacks using Probability Density Curves. *I. J. Computer Network and Information Security*, s.25-36. doi:10.5815/ijcnis.2018.03.04

ÖZET

Sanallaştırma her alanda yaygın olarak kullanılan ve sürekli gelişen bir teknoloji haline gelmiştir. Sanallaştırmanın yönetilebilirlik, esneklik, ayırma, kesinti süresini azaltma, maliyet verimliliği ve ölçeklenebilirlik gibi çeşitli avantajları vardır. İş sürekliliğinin ve verimliliğinin sağlanması için sanallaştırma teknolojilerine geçiş yapmak ve gelişen sanallaştırma teknolojilerini yakından takip etmek elzem bir hal almıştır. Sanallaştırma teknolojilerinin sürekli gelişmesi ve yöntem çeşitliliğinin artması sebebiyle "Sanallaştırma Yöntemleri ve Kullanım Alanları" bu tezin konusu olarak seçilmiştir.

Bu kapsamda, tez çalışmasının birinci bölümünde sanallaştırma ile ilgili temel kavramlar ve sanal makinenin özellikleri anlatılmaktadır. İkinci bölümde ise sanallaştırma teknolojileri yöntemleri ve kullanım alanları incelenmiştir. Tezin üçüncü bölümünde ise sanallaştırmada süreç ve yöntemler anlatılmış ve sanallaştırmada kullanılan yazılımlar ele alınmıştır. Dördüncü bölümde ise sanallaştırmada bilgi güvenliği incelenmiştir. Ayrıca sanal sistemlere yönelik güvenlik tehditleri ve bu tehditlere karşı alınabilecek önlemler anlatılmıştır. Tezin beşinci bölümünde ise sanallaştırmada veri merkezi modelleri ele alınmış ve sanallaştırmanın yararlarından bahsedilmiştir.

Sonuç ve değerlendirme bölümünde ise toplanan veriler değerlendirilmiş, sanallaştırma teknolojilerini uygulama alanları için önerilerde bulunulmuştur. Sanal sistemlerin kullanımı ve bilgi güvenliğini sağlamak için tez çalışmasının ortaya çıkardığı neticeler sonucunda kurum içinde alınması önem arz eden önlemler değerlendirilmiştir.

Arşiv Kayıt Bilgileri

Tezin Adı: Sanallaştırma Teknolojisi Yöntemleri ve Kullanım Alanları

Tezin Yazarı: Tuğçe ÇİÇEK

Tezin Danışmanı: Fatih ÖZTÜRK

Tezin Konumu: Uzmanlık Tezi

Tezin Tarihi: Nisan / 2021

Tezin Alanı: Sanallaştırma Teknolojisi

Tezin Yeri: RTÜK / ANKARA

Anahtar Kelimeler: Sanallaştırma, Sanal Makine, Bilgi Güvenliği, Sanal Sistem Güvenliği, Veri Merkezi

ABSTRACT

Virtualization has become a widely used and constantly evolving technology in every field. Virtualization has several advantages such as manageability, flexibility, separation, reduction of downtime, cost efficiency, and scalability. In order to ensure business continuity and efficiency, it has become essential to switch to virtualization technologies and to closely follow the developing virtualization technologies. Due to the continuous development of virtualization technologies and increasing variety of methods, "Sanallaştırma Yöntemleri ve Kullanım Alanları" has been chosen as the subject of this thesis.

In this context, the basic concepts of virtualization and the features of the virtual machine are explained in the first part of the thesis. In the second part, methods of virtualization technologies and their usage areas are examined. In the third part of the thesis, the processes and methods in virtualization are explained and the software used in virtualization is discussed. In the fourth chapter, information security in virtualization is examined. In addition, security threats against virtual systems and measures to be taken against these threats are explained. In the fifth part of the thesis, data center models in virtualization are discussed and the benefits of virtualization are mentioned.

In the conclusion and evaluation part, the collected data were evaluated and suggestions were made for the application areas of virtualization technologies. In order to ensure the use of virtual systems and information security, the important measures to be taken within the institution as a result of the results of the thesis study were evaluated.

Key Words: Virtualization, Virtual Machine, Information Security, Virtual System Security, Data Center

ÖZGEÇMİŞ

Tuğçe ÇİÇEK 1990 yılında Eskişehir'de doğdu. Sırasıyla Telsizler İlköğretim Okulu, Yıldırım Beyazıt Anadolu Lisesi'nde okuduktan sonra 2016 yılında Eskişehir Anadolu Üniversitesi Elektrik-Elektronik Mühendisliği bölümünden mezun olup lisans derecesi aldı. 2018 yılından itibaren Radyo ve Televizyon Üst Kurulu'nda görev yapmaktadır. Evlidir. İyi derecede İngilizce bilmektedir.