TÜRKİYE BİLİŞİM DERNEĞİ

KAMU BİLGİ İŞLEM MERKEZLERİ YÖNETİCİLERİ BİRLİĞİ

Kamu Bilişim Platformu XII

SANALLAŞTIRMA

Sürüm 1.0

1. ÇALIŞMA GRUBU

Nisan 2010

TBD Kamu-BİB

Kamu Bilişim Platformu XII

SANALLAŞTIRMA

Sürüm 1.0

1. ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği (TBD Kamu-BİB)'nin ***on ikinci dönem*** çalışmaları kapsamında, **1. Çalışma Grubu (ÇG1)** tarafından hazırlanmıştır. Bilişim teknolojileri sektöründe sanallaştırmanın kullanılmasına yönelik bilgiler sunmaktadır.

Hedef Kitle

Çalışmanın içeriği, bilişim teknolojileri çalışanları, yöneticileri ve bilişime ilgisi olan herkese yöneliktir.

Yayını Hazırlayanlar

Cevat ŞENER (Çalışma Grubu Başkanı)
Cemil ULU (Çalışma Grubu Editörü)
Oğuz ERGİN (Çalışma Grubu Başkan Yardımcısı)

Belge No ..... : TBD/Kamu-BIB/2010-ÇG1

Tarihi ..... : 30 Nisan 2010

Durumu ..... : Nihai Rapor – Sürüm 1.0

1. Çalışma Grubu

Çalışma Grubu Başkanı	Cevat ŞENER	ODTÜ
Kamu-BİB YK Temsilcileri	Nihat YURT	
	Ziya KARAKAYA	
	Aslıhan TÜFEKÇİ	
Başkan Yrd.	Oğuz ERGİN	TOBB ETÜ
Editör	Cemil ULU	TCMB
Yazman	Ulaş CANATALI	ODTÜ BİDB
Grup Üyeleri	Tolga ÖZDEMİREL	Türkiye Noterler Birliği
	İrfan KESKİN	SGK
	Umut YEŞİLIRMAK	SDYGM
	Yelda YİĞİT	Türkiye Noterler Birliği
	İlhan AKÇAL	Milli Kütüphane
	Hürol TABAK	OYTEK
	Abdullah GENCELLER	SSM
	Çağlar ÜLKÜDERNER	Profelis
	Bora GÜNGÖREN	Portakal Teknoloji
	Aslı ARTUN	Teknopark Proje
	Jale AKYEL	IBM
	Mustafa ÖZLÜ	TPE
	Selda GÜRÇAY	Türkiye Noterler Birliği
	Onur T. ŞEHİTOĞLU	ODTÜ -KKK
	Erek GÖKTÜRK	Identra
	Tuncay TOKGÖZ	Türkiye Noterler Birliği
	Emin CEBE	SSM
	Kürşat DEMİRAY	CISCO
	Mustafa AFYONLUOĞLU	Türkiye Noterler Birliği

TEŞEKKÜR

Bu çalışmanın başlatılması, gerçekleşmesi ve sonucunda da okumakta olduğunuz bu raporun ortaya çıkmasını sağlamış olan, Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği'ne (TBD Kamu-BİB); çalışmalarımıza katılan ve çalışmalarımız sırasında her konuda bizlere destek olan TBD Kamu-BİB Yürütme Kurulu temsilcilerine; bizlere sıcak bir ortam sağlayarak çalışmalarımızı kolaylaştıran, toplantılarımızda bizlere ev sahipliği yapan Türkiye Noterler Birliği'ne; toplantılara katılarak bilgi ve deneyimlerini bizlerle paylaşan değerli arkadaşlarımıza; yapıcı eleştirilerini sunarak eksiklerimizi tamamlamamızı kolaylaştıran değerlendirme toplantılarının katılımcılarına ve bizlere destek olan ancak burada isimlerini sayamadığımız tüm kişi, kurum ve kuruluşlara teşekkürlerimizi sunarız.

TBD Kamu-BİB

Bilişim Platformu XII

İÇİNDEKİLER

ŞEKİLLER

TABLOLAR

KISALTMALAR VE TANIMLAR

API	"*Application Programming Interface*". Uygulama Programlama Arayüzü.
BİB	Bilgi İşlem Birimi.
BT	Bilişim Teknolojileri.
DNS	"*Domain Name System*". Alan Adı Sistemi. İnternet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan bir sistemdir.
IPSEC	"*Internet Protocol Security".* Internet protokolünü (IP) daha güvenli yapmak için geliştirilmiş, her bir IP paketine kimlik tanıma ve şifreleme özellikleri katan veri iletişim protokolüdür.
iSCSI	"*Internet Small Computer System Interface*". İnternet küçük bilgisayar sistem arayüzü. Veri depolama araçlarını birbirine bağlayan IP tabanlı veri deposu ağı standardı.
İSS	"*Internet Servis Provider (ISP)".* İnternet Servis Sağlayıcısı
KVM	"*Klavye, Video, Mouse*". Birden fazla bilgisayarın erişiminin tek bir klavye, video monitör ve fare vasıtası ile gerçekleştirilmesini sağlayan bir donanım cihazıdır.
LDAP	"*Lightweight Directory Access Protocol*". TCP/IP üzerinde çalışan dizin servislerini sorgulama ve değiştirme amacıyla kullanılan uygulama katmanı protokolü.
MAC adresi	"Media Access Control". Bir cihazın ağ donanımını tanımaya yarayan kendine özel numarası.
MBR	"*Memory Buffer Register".* Arabellek Yazmacı. Bir bilgisayar işlemcisinin içerisinde yer alan, hızlı erişim ihitiyacı olan veri için kullanılan yazmaç.

NAS	“*Network Attached Storage*”. Ağa Bağlı Veri Depolama. İletişim ağındaki farklı türde istemcilere veri erişimi sağlayan, bu ağa bağlanmış dosya seviyesinde veri depolama mimarisi.
NAT	“*Network Address Translation*”. Ağ Adres Dönüşümü.
NIC	*"Network Interface Card"*. Ağ Arayüz Kartı.
NUMA	“*Non-Uniform Memory Architecture*”. Düzensiz Bellek Mimarisi. Çok işlemcililerde bellek zamanının belleğin işlemci üzerindeki yerine bağlı olduğu bir bilgisayar belleği tasarımıdır.
RAID	“*Redundant Array of Inexpensive Disks”.* Veri bütünlüğünü, hata toleransını, iş çıkarma yeteneğini ve toplam disk kapasitesini artırmak için birden fazla sabit diski kullanarak yapılan veri depolama tasarısıdır.
RARP	“*Reverse Address Resolution Protocol*”. Ters Adres Çözümleme Protokolü. Bir TCP/IP ağında MAC adresleri ile IP adresleri arasındaki bağı yapmak için kullanılır.
SAN	“*Storage Area Network*”. Veri Depolama Alanı Ağı. Uzak veri depolama cihazlarını birbirine bağlayarak kendi içerisinde bir ağ oluşturan mimari.
SCSI	"*Small Computer System Interface*". Küçük Bilgisayar Sistemi Arabirimi. Sabit Disk, CD sürücü, tarayıcı, yazıcı gibi aygıtları paralel arabirim standartlarından daha uyumlu ve gelişmiş bir şekilde kontrol eden standarttır.
SSD	“*Solid State Disk*”. Katı Hal Sürücüsü. Veri depolamak için geliştirilmiş, katı hâl bellek teknolojisini kullanan veri depolama aygıtıdır

SMP	“*Symmetric Multi Processing”. Simetrik Çoklu İşlem.* İki veya daha fazla eşlenik işlemcinin tek ve ortak kullanılan bir ana bellek ile birbirine bağlı olduğu ve tek bir işletim sistemine sahip çok işlemcili bilgisayar mimarisidir.
TCO	“*Total Cost of Ownership”.* Toplam sahip olma maliyeti.
USB	"*Universal Serial Bus*". Evrensel Seri Veriyolu". USB dış donanımların bilgisayar ile bağlantı kurabilmesini sağlayan seri yapılı bir bağlantı biçimidir.
VDC	*“Virtual Data Center”*. Sanal Veri Merkezi, işletmeci dışında olan birden çok özel veya tüzel kullanıcıya ait sanallaştırılmış sistemlerin aynı sanal makine havuzu veya havuzları içinde barındığı ve farklı da olabilecek hizmet kalitesi sözleşmeleri kapsamında işletildiği veri merkezi kurulumudur.
VDS	*"Virtual Dedicated Server"*. Sanal Adanmış Sunucu, kullanım tasarrufunun tamamının kullanıcıya ait olduğu bir özel sanal sunucu hizmetidir ve kendi kullanımına özel ve tamamen adanmış (paylaşımsız) olarak ayrılmış belirli bir işlemci gücü, bellek kapasitesi ve sabit disk alanı gibi sistem kaynakları ile sağlanmaktadır.
VM	*"Virtual Machine"*. Sanal Makine, sunucu sanallaştırması yöntemleri kullanılarak elde edilen sanal sunucudur..
VNC	*"Virtual Network Computing".* Sanal Ağ Bilişimi, uzaktaki bir bilgisayara kurulan sunucu yardımı ile basit bir el bilgisayarından bile uzaktaki bilgisayarın masaüstüne erişim sağlama yöntemidir.
VPLS	*"Virtual Private LAN Service"*. Sanal Özel Yerel Ağ Hizmeti, IP tabanlı ağlar üzerinden, çok noktadan çok noktaya Ethernet tabanlı iletişim sağlama yöntemi.
VPS	*"Virtual Private Server"*. Sanal Özel Sunucu, küçük ölçekli sunucu ihtiyaçlarını karşılamak üzere üretilmiş, kişi ya da kuruluşlara özel sanal sunucu teknolojisidir.

VPN	*"Virtual Private Network"*. Sanal Özel Ağ, ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından, uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür.

ÖNSÖZ

TBD Kamu-BİB çalışma ve belge gruplarının bugüne kadarki tüm çalışmaları, Kamu BİB yönetici ve çalışanlarına, çeşitli açılardan yol gösterici çalışmalarda bulunmak ve raporlar hazırlamak olmuştur. TBD Kamu-BİB 12. dönem çalışma gruplarından olan bu grup da, giderek artan bir öneme kavuştuğu görülmekte olan Sanallaştırma konusunda aydınlatıcı ve yol gösterici bir çalışmada bulunmak ve sonucunda da bu raporu üretmek çabasında olmuştur.

Grup çalışmalarımız sırasında, "http://wiki.tbd.org.tr/index.php/2010-CG1" adresinde konumlandırılmış olan bilgi ve belge paylaşım ortamı kullanılmış ve çalışma yöntemimizde bu ortamın çevresinde ve bu ortamı kullanarak en geniş katılımı sağlayabilmeyi hedef edinerek şekillendirilmiş bulunmaktadır. Çalışmalarımızda izlemiş olduğumuz yöntem şu ana aşamaları içermiştir:

i. Yanıtlanması gereken soruların ve değinilmesi beklenen konuların ortaya çıkarılması;
ii. Bu soruların gruplanarak, rapor bölümlerinin oluşturulması;
iii. Bölüm sorumlularının ve bölümlere katkı vermek isteyen üyelerin belirlenmesi;
iv. Bölümlerde değinilmesi gereken noktalar konusunda açıklamaların ve detaylı tariflerin toplanması;
v. Tariflenen noktaların Akış-İskelet formatına dönüştürülerek, raporun çok detaylı ve tarifli yapısının ortaya çıkarılması;
vi. Akış-İskelet formatında yer alan maddelerin, bölüme katkı veren üyeler tarafından katkı verilerek Taslak Metin çalışmasının gerçekleştirilmesi;
vii. Bu şekilde oluşan Taslak Metnin, önce bölüm sorumluları, sonra da çalışma grubu başkanı, yardımcısı ve editörü tarafınca elden geçirilmesi ve eksiklerin tamamlanması.

Yukarıda erişim adresi verilmiş olan paylaşım ortamı, bu adımlar göz önünde tutularak incelenebilir ve böylece çalışmalarımız hakkında daha detaylı bilgi edinilebilir.

Çalışmalarımız sırasında, ikisi sanal olmak üzere ondan fazla toplantı düzenlenmiş ve bu toplantılar sırasında, sanallaştırma konusunda bilgi ve deneyim sahibi kişi ve uzmanların değerli görüşlerini alabileceğimiz, deneyimlerini

paylaşabileceğimiz bilgi aktarım ve paylaşım seansları da düzenlenmiştir. Böylece, hem çalışma grubumuza katılımı geniş ve aktif tutmak, hem de grubumuzun konu hakkındaki bilgi düzeyini yükseltmek hedeflenmiştir. Tüm bu çabalarımızın sonucu olarak hazırlamaya çalıştığımız bu dokümanın, Bilgi Teknolojileri sektörünce yol gösterici olarak kullanılabileceğini umarız.

Saygılarımızla,

TBD Kamu-BİB 12. Dönem 1. Çalışma Grubu

30 Nisan 2010

AMAÇ VE KAPSAM

Sanallaştırmanın, sanallaştırılan bilişim kaynağına ve kullanılan yönteme göre değişen çok farklı tipleri ve uygulama alanları bulunduğu bilinmektedir. Bu belgenin hedefi, başta kamu kurum ve kuruluşları olmak üzere, bilişim teknolojileri (BT) birimlerine sanallaştırma konusunda yol gösterici olmaktır. Bu noktadan hareketle, sanallaştırmaya ilişkin tanımların, tiplerin, yarar getirebilecek kullanımların ve bu kullanımlara ilişkin olarak dikkat edilmesi gereken noktaların, süreç ve yöntemlerin, uygulama örneklerinin ve güvenliğin sağlanması ile ilgili konuların, sanallaştırmanın BT birimlerine hitap edebilecek tipleri ve uygulama alanları kapsamı içinde işlenmesi amaçlanmaktadır. Bu açıdan bakıldığında, BT çalışanları, yöneticileri ve bilişime ilgisi olan herkesin, bu raporun hedef kitlesi içinde bulunduğu görülmektedir.

BÖLÜM 1.

GİRİŞ

Bilişim sektörü ile ilgili kaynaklarda ve çevrelerde giderek daha fazla duyulmaya başlayan bir terim olan sanallaştırma, çok kısaca fiziksel bir yapının mantıksal hale getirilmesi olarak tanımlanabilir. Sanallaştırma, iş gücü kaybını ve maliyetleri azaltmasının yanı sıra, yüksek verimlilik ve esneklik sağlayabilmektedir. Üstelik bunlar, sanallaştırmanın olası yararlarının yalnızca bir kısmıdır ancak bunlar bile, bu teknolojiyi yakından incelemek için yeterli bir neden olarak ortaya çıkmaktadır.

Bilişimle ilgili her tür ve ölçekteki çalışma ortamlarını ve yapılarını düzenlerken kullanabilecek bir yaklaşım olan sanallaştırmayı destekleyen veya sağlayan çok sayıda ürün, donanım ve yazılım firmalarınca piyasaya sürülmektedir. Bu gibi ürünlerin yanında, sanallaştırma konusunda ileri yeteneklere sahip açık kaynak kodlu projelerin bulunduğu ve BT çalışmalarında etkin olarak kullanılabildikleri de görülmektedir. Ayrıca, bu konuyla ilgili ürün, proje ve çalışmalara yön veren açık standartların oluşmaya başladığı gözlenmekte; bu da, sanallaştırma yaklaşımının geldiği olgunluk düzeyi hakkında olumlu ve önemli bir gösterge olarak kabul edilmektedir.

Bu raporun ikinci bölümü, sanallaştırma kavramını yakından tanınmasını sağlamayı amaçlamakta olup, tarihçesini, sanallaştırma kavramını ve ana tiplerini incelemektedir. Bir sonraki bölümde ise, sanallaştırmanın yararları ve sanallaştırmayı hayata geçirirken karşılaşılabilecek zorluklar ele alınmaktadır. Rapor, sanallaştırmanın güvenlik konusu ile ilişkisini ve bu konuyla ilgili olarak dikkat edilmesi gereken noktaları dördüncü bölümde irdelemektedir. Sanallaştırmaya geçiş aşamalarının ve metotlarının tartışıldığı beşinci bölüm, izlenmesi gereken adımlar açısından BT yöneticilerinin, metotların detayları açısından da teknik personelin ilgisini çekebilecek düzeydedir. Ardından, sanallaştırmanın uygulama alanlarının ele alındığı altıncı bölüm gelmektedir. Rapor, kamu bilgi işlem birimleri açısından durumun ve sanallaştırma örneklerinin masaya yatırıldığı yedinci bölüm ile sürmekte ve sonuçlar ve önerilerin ele alındığı sekizinci bölümle de son bulmaktadır.

BÖLÜM 2.

SANALLAŞTIRMA NEDİR: TARİHÇE VE KAVRAMLAR

Literatürde sanallaştırmaya ilişkin farklı tanımların yer aldığı görülmektedir. Burada dikkat edilmesi gereken bir nokta, kaynakların azımsanmayacak bir bölümünün, sanallaştırmanın tanımı olarak, sunucu sanallaştırmasına özel tanımın kullandığının görülmesidir. Sunucu sanallaştırması, en popüler ve en önemli sanallaştırma tiplerinden biri olmakla beraber; sanallaştırma teriminin genelini temsil etmesi mümkün değildir. Bu nedenle, burada verilen sanallaştırma tanımlarının, genel anlamda sanallaştırmayı temsil etmesine özen gösterilmektedir.

Örneğin, Vikipedi, sanallaştırma için "bilişim kaynaklarının soyutlanması" tanımını kullanmaktadır [1]. About.com sitesinde ise "başka sistemlerin, uygulamaların veya kullanıcıların bilişim kaynaklarına erişimini basitleştirmek amacı ile o kaynakların fiziksel özelliklerinin saklanması tekniği" olarak tanımlanmaktadır [2]. ZDNET'in bu konudaki yaklaşımı oldukça basittir: "Sanallaştırma, bilgisayarın iş yapabilme yeteneğini iyileştirmek için kullanılan bir genel terimdir" [3]. Webopedia'a ise "bir cihaz veya kaynağın sanal versiyonunun yaratılması" tanımı kullanılmaktadır [4].

Toparlayacak olursak, sanallaştırma, bilişim kaynaklarının (işlemci, depolama, ağ, bellek, platform, sunucu, masaüstü, uygulama vb.) soyutlanarak, yani gerçekte var olan kaynağın değil de, gerçek kaynağa dayandırılarak tanımlanmış olan soyut halinin, ilgili bilişim kaynağının kullanıcılarına sunulması olarak basitçe tanımlanabilir. Böylece, gerçek kaynak ile kullanıcısı arasındaki bağ gevşetilebilmekte ve var olan gerçek kaynak, göreceli olarak daha az kapasiteli çok sayıda sanal kaynak olarak kullandırılabilmektedir.

Örneklemek gerekirse, bir işletim sistemi için ses aygıtları girdi ve çıktı aygıtları olarak iki türlüdür. Bu aygıtlar ana kart üzerindeki sistem veri yoluna bağlanırlar. İşletim sistemi için bir mikrofon girişi, aslında sistem veri yoluna belli formatta veri yollayan herhangi bir aygıttır.

Bir aygıt sürücüsü yazarak, aslında fiziki olarak mikrofon girişi olmayan bir bilgisayarın, uzaktaki bir bilgisayarın mikrofon girişindeki veriyi ağ üzerinden

almasını ve bunu sanki gerçek bir aygıttan gelen veriymiş gibi işlenmesi sağlanabilir. Böylece sürücü yolu ile sanal bir aygıt üretilebilir. Bu işlem kimi zaman çok kolaylıkla yapılabilmektedir.

Bu örnek genelleştirildiğinde, işletim sistemi için gerekli olan hemen her çevre birimi, sanal aygıt sürücüleri yolu ile sanallaştırılabilir.

Sanallaştırma ne şekilde yapılacak olursa olsun, sanal kaynağı oluşturan ve bunu gerçek fiziki kaynaklar ile eşleyen bir bileşen mutlaka bulunacaktır. Bu bileşen, sunduğu sanal kaynağa bağlı olarak değişiklikler gösterse de, temelde bir işletim sisteminin sorumluluk alanına giren bazı denetimlerin sorumluluğunu da üstlenecektir. Bu nedenle; sanallaştırma alt yapısı yazılımlarının geliştirilmesi işi, işletim sisteminin alt katmanlarının geliştirilmesi işi ile önemli paralellik göstermektedir. Çeşitli sanallaştırma araçlarının işletim sistemleri ile bütünleşik gelmesi veya işletim sistemlerinden kod almış olması da bundan dolayıdır.

2.1. Tarihçe

Sanallaştırma fikrini ortaya çıkaran ilk gelişmelerin, çoklu programlama ve zaman paylaşımı fikrilerinin Oxford Üniversitesinde ortaya atılması ile başladığı bilinmektedir. Bu fikirler ilk olarak Atlas projesi ile hayata geçmiş oldu. Mancehter Üniversitesi tarafından 1960'ların başlarında yürütülen bu proje ile ilk kez supervizör (bir tür sanal makine monitorü veya hipervizör) ve sanal bellek kavramları ile tanışılmış oldu.

Benzeri bir yaklaşım, IBM'in yine 1960'lı yıllarda geliştirdiği M44/44X deneysel sistemlerinde de görüldü [5]. Bu çalışma sırasında ilk kez sanal makine kavramı konuşulmaya başlandı. CP/CMS'i geliştirmeye başlamasının ardından [6], IBM, Sistem/360 ile zaman paylaşımlı ortam sunmaya başladı; ancak gerçek mimari Sistem/70 ve CP/CMS ile oluştu. Bu çalışmalar sırasında, 1966 yılında ilk kez IBM CP-40 ve IBM CP-67 ile tam sanallaştırma (full virtualization) gerçekleştirildi. Ardından, IBM S/370 üzerinde çalışmaya başladı ve ilk donanım destekli sanallaştırma (hardware-assisted virtualization) hayata geçirilirken, ilk sanal makine işletim sistemi olan VM/370 de ortaya çıkarıldı [7, 8]. Mantıksal bölünme ise, 1980'li yıllarda IBM ESA/390, Amdahl, Hitachi sistemleri ile sanallaştırma tarihinde yerini aldı [9].

IBM'in bu çabalarının yanında, aşağıda kısaca belirtilen üç proje de sanallaştırma tarihinde rol oynamıştır: 1960'ların sonunda, CDC 7600 süper bilgisayarları için işletim sistemi olarak kullanılmak üzere Lawrence Livermore

Laboratuarı tarafından geliştirilen Livermore Ana Bilgisayar Sistemi; Cray süper bilgisayarlarının eski türleri için 1970'lerin başlarında geliştirilen ve Amerika Birleşik Devletleri Enerji Bakanlığı tarafından nükleer araştırmalar için kullanılan Cray X-MP bilgisayarları üzerinde yer alan Cray Ana Bilgisayar Sistemi [10]; TCP/IP gibi yeni iletişim protokollerini desteklemek üzere Cray bilgisayarları için geliştirilen ancak kullanıcılar tarafından kabul görmeyen Yeni Livermore Ana Bilgisayar Sistemi.

1980'li yılların sonunda, sistemlerin ucuzlaması ile birlikte, merkezi sistemlerden dağıtık yapılara ve istemci/sunucu mimarisine geçişler başladı. Böylelikle, hem sunucu hem de istemci bilgisayar sistemlerinin sayıları giderek arttı.

1995'lere gelindiğinde birçok çalışma, aslında dağıtık yapı ve uygulamaları yönetmenin, kaynakları etkin olarak kullanmanın çok da kolay ve ekonomik olmadığını gösterdi. Böylece tersine giden merkezileşme süreci başladı; ancak bu kez de her fonksiyon için (LDAP, Web, uygulama, dosya, vb.) ayrı bir sunucu kullanıldı. Esas olarak birer yazılım olan bu sunucuların tek tek yönetim kolaylığının sağlanması ve ayrıca bağımlılıklarının ayrıştırılması için farklı fiziki sistemlerde konumlandırılması yaygın bir uygulama halini aldı. Bu yaklaşım ise, atıl kapasitenin artmasına neden oldu. Bakım masraflarındaki artışa ek olarak, her bir sunucunun verimi düştü ve tipik boşta kalma oranı %85-90'lara kadar yükseldi.

1990'lı yılların sonunda ekonomik gelişmeler, maliyetlerin gözden geçirilmesini ve kaynakların daha verimli kullanılması ihtiyacını doğurdu ve sanallaştırma tekrar gündeme geldi. Bu kapsamda 1998'de sanallaştırma yazılımı odaklı VMware şirketi kuruldu [11] ve ilk ürünü olan VMware Workstation 1999'da pazara sunuldu. Sunucu pazarına ise 2001 yılında VMware GSX Server ve VMware ESX Server ürünleri ile girdi. 2003'de VMware Virtual Center ve VMotion and Virtual SMP teknolojileri geldi. Windows ve Linux ortamında çalışan VMware'e, 2006'da Mac OS desteği de geldi.

Ayrıca, Intel ve AMD 2005-2006 yıllarında sanallaştırmayı destekleyecek ek donanım sunmaya başladılar [12]. Yaygın kullanılan Intel IA-32 mimarisinin sanallaştırma konusundaki eksiklerinin tamamlanması, bu mimarideki uygulamaların sanallaştırılmasını da hızlandırdı. Aynı yıllarda, daha sonra tamamen açık kaynak olan Xen yazılımı, bir araştırma projesi olarak Cambridge Universitesi'nde geliştirildi [13, 14]. Xen'in ilk ürünü 2003'de pazara sunuldu. 2007'de Citrix Systems, Xen'i satın aldı ve Xensource ürünleri olarak isimlendirdi. 2007'de bu sektörün öncülerinden Citrix, IBM, Intel, Hewlett-Packard, Novell, Red Hat, Sun Microsystems ve Oracle'ın katılımıyla Xen Projesi Danışma Kurulunu oluşturdu.

IBM de, sanallaştırma çalışmalarını 2001 yıllarında POWER mimarisi (pSeries ve iSeries) sistemlerine taşıdı. z/VM, VM işletim sisteminin en son sürümü olarak ortaya çıktı ve 2000 yılında duyuruldu. z/VM [15], IBM System z donanımlarında çalışıp, çok sayıda Linux sanal makinesinin System z ortamında çalışmasını sağlamaktadır. IBM, 2008'de Power/VM ve z/VM duyuruları ile geçmişte öne çıkarmadığı sanallaştırma konularına tekrar odaklandığını gösterdi.

Sun, VMware, Microsoft ve IBM gibi birçok şirket, sanallaştırmaya yönelik ürünlerini piyasaya çıkarmış durumdadır. Bununla birlikte, Linux birliği tarafından benimsenen ve şu sıralar en popüler dağıtımlara dahil edilen Xen, bu firmaları zorlamaktadır. Özgür yazılımlar içindeki sanallaştırma alt yapıları, Xen başta olmak üzere, birbirleri ile çok aktif biçimde kod paylaşımı sağlayarak hızlı gelişme sağlamış; bu durumu takip eden Microsoft da dahil olmak üzere bir çok ticari yazılım şirketi, bu özgür yazılım projelerinden kod lisanslama yolu ile özellik transfer etmiştir.

Sonuç olarak; eski fikir, yeniden gündeme gelmiş oldu.

Sanallaştırma, iki model (merkezi ve dağıtık) arasındaki düzeltilmiş çözüm olarak ortaya çıkmaktadır. Örneğin, sunucu sanallaştırması ile tüm bir bilgisayarı ve her bir uygulama için bilgisayarın gerekli olan yan donanımlarını satın almak yerine, her bir uygulamaya kendine ait sanal çalışma ortamı verilebilir. Bu ortamda girdi-çıktı, işlem gücü ve bellek bulunmaktadır. Bunların tümü, kullanılan fiziksel donanımı paylaşırlar. Bu da, merkezi yapı üzerinde dağıtıklığın (güvenlik, sağlamlık vb.) yararlarını ortaya çıkarır. Böylece, sistem kaynakları etkin olarak kullanılabilir ve teknolojiye yapılan yatırımdan daha iyi sonuçlar elde edilebilir.

Yukarıda da değinildiği üzere, özellikle 1990'larda yaşanan sistem sayılarındaki artış ile birlikte, sistem odalarının karmaşıklığı oldukça arttı. Bu durumu iyileştirmek amacı ile, BİB'nin önemli bir kısmı sunucu konsolidasyonuna (pekiştirme) gitmeye başladı. Burada izlenen en etkin yöntemlerin başında sanallaştırmanın geldiği görülmektedir.

Sanallaştırılan kaynakların bir araya getirilmesi ile daha yüksek kapasiteli ve tek elden yönetilebilen sanal kaynak havuzları oluşturulabilmektedir. Örneğin, sanallaştırılmış fiziksel sunuculardan oluşan bir çiftlik, çok daha yüksek sayıda sanal sunucudan oluşan bir havuzu taşıyabilmektedir. Havuzların içinde bulunan sistemlerin yatayda kolaylıkla ölçeklendirilmesi ile dönemsel değişkenlik gösteren iş yüklerinin yönetilebilmesi sağlanabilmektedir. Benzeri biçimde, arıza yapan sistemlerin hızlıca geçmişteki bir noktadaki hali ile devreye alınabilmesi veya sistem

bakımı nedeni ile oluşan kapalı kalma sürelerinin kısaltılması gibi avantajlar görülebilmektedir.

Sanallaştırma aynı zamanda belli tür güvenlik önlemlerinin uygulanması için gereken yalıtım seviyelerini de getirmektedir. Ancak sanallaştırmanın kendisini oluşturan alt yapının da bir bilişim sistemi olduğu ve bu alt yapıya dönük bilgi güvenliği politikalarının oluşturulmasının gerekli olduğu göz ardı edilmemelidir.

Ayrıca, özel veya tüzel kullanıcılara ait sanal sunucular, Sanal Veri Merkezi (VDC) ismi verilen hizmet merkezlerince ücreti karşılığında barındırılabilmektedir. Bu tip merkezlerden alınacak hizmeti kalitesi, yapılacak sözleşmeler kapsamında belirlenebilmektedir.

Dünya üzerinde, çok daha büyük çaplı sanal kaynak havuzları ve bu havuzlar üzerinde kurulan hizmet iş modelleri ile bulut bilişim yapılarına ulaşılmaya başlanıldığı da görülmektedir. Bu tip yapılarda, gereksinim duyulan her tür bilişim kaynağı bir servis olarak, bulut yapısından hizmet olarak alınabilmektedir ve kullandığın kadar öde prensibi ile maliyetlendirilmektedir.

2.2. Sanallaştırma Tipleri

Sanallaştırma denilince, genellikle ve öncelikle Sunucu Sanallaştırması anlaşılmasına rağmen, farklı bilişim kaynaklarının sanallaştırılmasına yönelik olarak farklı sanallaştırma tipleri bulunmaktadır. Burada, bu sanallaştırma tiplerinin başlıcaları ele alınmaktadır:

2.2.1. Sunucu Sanallaştırması

Bilgi işlem birimleri tarafından sanallaştırma denince ilk akla gelen sanallaştırma tipi sunucu sanallaştırması olmaktadır. Sunucu sanallaştırması temel olarak aynı donanım üzerinde birden fazla işletim sisteminin aynı anda çalıştırılması anlamına gelmektedir. Sunulan uygulamaların ve hizmetlerin farklı işletim sistemi gereksinimleri, farklı sürümlerde veya birbiriyle çelişen altyapısal ihtiyaçlar gerektirmesi ya da güvenlik gibi diğer sebeplerle birbirlerinden tamamen bağımsız çalışmaları da sık karşılaşılan zorunluluklardır. Buna karşın sunulan hizmet ya da uygulamalar, genelde üzerinde çalıştıkları donanımların kapasitelerini pek kullanmadığından, aynı donanım üzerinde birbirinden bağımsız birden fazla işletim sisteminin çalıştırılması ile donanımın en iyi şekilde değerlendirilmesi mümkün olmaktadır. Bununla beraber test ortamlarının yaratılması ve rahatlıkla

yönetilebilmesi için sunucu sanallaştırması bilgi işlem birimlerine oldukça kolaylıklar sağlamaktadır.

2.2.2. Masaüstü Sanallaştırması

Masaüstü sanallaştırması, diğer sanallaştırma tiplerine benzer şekilde, mantıksal sunumun fiziksel altyapıdan ayrılması mantığını taşır. Burada da, mantıksal masaüstü ortamı, fiziksel altyapı olan kullanıcı bilgisayarından (kişisel bilgisayar, taşınabilir bilgisayar vb.) ayrılmaktadır. Masaüstü sanallaştırması, kullanıcılara masaüstü ortamı sağlama ve kolayca yönetme, farklı isteklere esnek çözümler getirme ve son kullanıcılara yönelik işletim sistemi lisans ücretlerinde tasarruf sağlama gibi olanak sağlamaktadır.

2.2.3. Veri Depolama Sanallaştırması

Günümüzde, bellek sağlayıcıları müşterilerine yüksek başarımlı (performanslı) depolama çözümleri önermektedir. Veri depolama sanallaştırması, en temel haliyle, tek bir birimde toplanan çoklu fiziksel disk sürücülerinde bulunur. Bu tek birim, RAID uygulamalarına sahip ana bilgisayar ve işletim sisteminde sunulmaktadır. Bu, sanallaştırma olarak adlandırılabilir çünkü arka planda iki veya daha fazla sürücüden oluşmasına rağmen, tüm sürücüler kullanılmaktadır ve tek bir tutarlı sürücü olarak etkileşime girerler. Esas depolama dizisi ve bileşenleri, depolama alanı ağı (SAN) teknolojilerinin tanıtılmasını ve benimsenmesini yavaşlatmıştır. Depolama alt sistemlerini yönetmekle sorumlu olan işletim sistemi kodunda herhangi bir değişim olmaksızın, BT kurumları çoklu sunucular arasında depolama bileşenlerini paylaşmaktadırlar. Her sunucunun kendine ait fiziksel belleği olmasına rağmen, depolama yöneticileri sanal bir sürücü alanı oluşturmuşlardır ve ana bilgisayarlar için kullanıma sunmuşlardır.

Veri Depolama sanallaştırmasını bir sonraki aşamaya taşıyan daha gelişmiş teknolojiler piyasaya çıkmaya başlamıştır. Var olan ürünler, ana bilgisayara herhangi bir müdahalede bulunmadan, kurallara ve yönergelere (bellek yönergeleri, veri zamanı ya da son erişim gibi) dayanarak, belleği bir platformdan arka plandaki diğer bir platforma taşıyabilir.

Uygulama yazılımlarının depolama becerisini kullanma tarzlarındaki gelişme, zamanla disk bölümü veya disk aygıtı soyutlamasının ötesinde depolama soyutlamalarının gelişmesini de sağlamıştır. Özellikle, dağıtık ve paralel dosya sistemlerinin kullanılması ve nesne deposu biçiminde çalışan ilişkisel olmayan veri

depolarının yaygınlaşması, hem veri depolama sanallaştırması arayüzlerinin hem de alt yapılarının önemli derecede değişmeye başlamasına neden olmuştur.

2.2.4. Veri ve Veritabanı Sanallaştırması

Veri sanallaştırması kullanıcıların tamamen farklı bölgelerde yer alan çeşitli kaynaklara verinin ne olduğuna nerede olduğuna bakmaksızın erişimine imkân sağlar. Veritabanı sanallaştırması katmanlar üzerinde yapılan sanallaştırmadır. Donanım kaynaklarının genişletilmesine ve bu sayede kaynakları, uygulamaların ve kullanıcıların daha iyi paylaşılmasına imkân sağlar. Bunun yanında ölçeklendirilebilir hesaplamalara daha fazla izin verir. Veritabanı sanallaştırması veritabanı yönetim sisteminin birçok örneğini kullanmaya izin verir. Bu çalışmalar genelde veri kaynaklarına ulaşmada ve veri depolama sistemlerinde kullanılmaktadır. Var olan bilgisayar altyapısına çeviklik ve esneklik kazandırma, veritabanı başarımını arttırmak, bilgisayar kaynaklarını paylaşmak için havuz oluşturma, yönetimi ve idareyi kolaylaştırma, hata toleransını arttırma, önemli ticari verilerin eş zamanlı yedeklenmesine imkân sağlama, birliğin toplamda yaptığı masrafı aza indirmek gibi amaçlarla kullanılır.

2.2.5. Ağ Sanallaştırması

Ağ sanallaştırması, ağdaki uygun kaynakların ve uygun bant genişliklerinin her birinin, birbirinden bağımsız ve belli sunuculara ya da cihazlara atanmış kanallara etkin bir şekilde paylaştırılmasıdır. Sanal ağ ortamlarının bileşenleri arasında ağ arayüz kartı (NIC), ağ anahtarı (switch), ağ depolama araçları, sanal ağ taşıyıcıları ve ağ ortamları yer alır.

Ağ sanallaştırması vasıtası ile, fiziksel ekipmanlarda azalma ve ekipmanların azalmasına bağlı olarak enerji tasarrufu, esneklik, güvenirlik ve kolay yönetilebilirlik gibi birçok konuda ağın daha verimli bir şekilde kullanılabilmesi sağlanır.

2.2.6. Uygulama Sanallaştırması

Genel anlamıyla uygulama sanallaştırması bir uygulamanın ara katmanlar yardımıyla kendi platformu dışındaki diğer platformlarda da çalıştığını ya da birden çok platformda çalışabildiğini açıklayan bir kavramdır. Bu ara katmanın görevi uygulama ile üzerinde bulunduğu platformun anlaşabilmesini sağlamaktır. Burada sözü edilen platform ile bir donanım ya da işletim sistemi kastedilmektedir. Amaçlanan ise, uygulamanın ara katmanın farkında olmaksızın bu platformda çalıştırılabilirliğidir.

2.2.7. Bellek Sanallaştırması

Sanal bellek, günümüzün genel amaçlı işletim sistemlerince kullanılan bir yöntemdir. Uygulamalar, sanal bellek aracılığıyla gerçekte bilgisayar üzerinde ne kadar bellek bulunduğunu bilmeden, işletim sistemi üzerinden bellek alanlarına erişebilirler. Bu sayede mevcut bellek miktarından daha fazlasını kullanmak mümkün olabilmektedir.

Bellek sanallaştırmasının bir sonraki aşamasında bilişim merkezindeki sunucuların belleklerinin tek bir havuzda toplanması ve birbirlerinin belleklerini kullanabilmeleri mümkün olmaktadır. Gerçekte bellek havuzunda ne kadar bellek olduğunu bilmeyen sunucu bilgisayarlar birbirlerinin belleklerine belirli bir sanallaştırma arayüzü üzerinden erişebilir ve bellek gereksinimlerini değişen koşullara göre karşılayabilir.

Yakın zamana kadar bellek sanallaştırması, ağ hızlarının düşük olması ve gecikmelerin çok büyük olması sebebi ile mümkün değildi. Buna rağmen şu anda bile bellek sanallaştırması kullanılması bellek boyutu ile bellek erişim hızı arasında ödünleşme yapılmasını gerektirir.

Bellek sanallaştırmasının başlıca yararları şöyle sıralanabilir:

- Ortak bellek havuzu sayesinde kısıtlı bellek kaynaklarının daha verimli kullanımı sağlanır.
- Veri yoğun ya da girdi-çıktı bağımlı işlerin gerçekleştirilme sürelerini kısaltır ve verimliliği arttırır.
- Uygulamaların veri tekrarı yapmadan birden fazla sunucu üzerinde çalışmasını sağlayarak toplam bellek ihtiyacını düşürür.
- SSD, SAN ve NAS gibi diğer bellek paylaşım çözümlerinden daha hızlı erişim sağlar.
- Ortak bellek havuzu, kendisine bağlı bulunan kullanılabilir kaynakların yük dağılımını düzenler.

BÖLÜM 3.

YARARLAR VE DİKKAT EDİLMESİ GEREKEN KONULAR

Sanallaştırma günümüzde sadece bilgi işlem servislerinin kullandığı bir teknoloji değildir. Yukarıdaki bölümde sanallaştırma teknolojilerinin ne kadar farklı kullanım alanları olduğu görülmektedir.

Temelde kaynakların optimize edilmesi ile yönetilebilirlik, ölçeklenebilirlik, toplam sahip olma (TCO) maliyetlerinin düşürülmesi, felaket senaryolarında hızlı geri dönüşler veya donanımla da desteklenmiş 7/24 kesintisiz çalışma gibi sistem yönetimi uzmanları için çok cazip faydaları ile sanallaştırma teknolojileri hızlı bir kullanım ve yayılma göstermiştir. Artık sadece sistem yönetimi uzmanları değil sıradan bir son kullanıcıda sanallaştırma teknolojilerinin pek çoğundan faydalanabilmektedir.

Bu kadar tercih edilen bir teknoloji olması sağladığı faydalarla açıklanabilen sanallaştırma elbette beraberinde dikkat edilmesi gereken pek çok konuyu da taşımaktadır. Sanallaştırmanın sağladığı faydaları ve dikkat edilmesi gereken hususlar iki ana başlık olarak aşağıda maddeler halinde detaylı olarak değerlendirilmektedir.

Çoğu zaman sanal bir ortamın gerçeğinden hiç bir farkı olmadığı için güvenlik konusu gerçek ortamlarda nasıl dikkatle takip ediliyorsa sanal bir ortam içinde aynı şekilde değerlendirilmelidir. Sadece bir kaç GB'lık bir alana kurulabilen ve herhangi bir USB bellek ile rahatça taşınabilen bir uygulama sunucusunun güvenliği için daha fazla çaba sarf etmek zorunda kalınabilir. Bu örnekte olduğu gibi bazen sanal bir ortam gerçeğinden daha fazla güvenlik riski taşıyabilir.

Sanallaştırma teknolojileri ile ilgili bu tür riskleri ve güvenlik konusundaki son gelişmeleri taşıdıkları önem nedeniyle başlı başına bir bölüm olarak ele alınmış ve bir sonraki bölümde detayları ile sunulmuştur.

3.1. Sanallaştırmanın Yararları

Sanallaştırma teknolojilerini kullanılarak birçok yarar sağlanabilmektedir. Bunlardan bazıları aşağıda sıralanmıştır:

- Fiziksel sunucuların sayısını azaltma.
- Veri merkezi için gerekli olan altyapı ihtiyacını azaltma (enerji, soğutma, alan, yedekleme, ağ geçiş bağlantı noktaları, KVM bağlantı noktaları).
- Sunucular tek bir merkezden yönetilebildiği için yönetimsel ek yükü azaltma.
- Yeni sunucuları kolayca mevcut ortama ekleme kabiliyeti. Yeni bir fiziksel sunucuyu eklemek günler hatta haftalar sürerken, sanallaştırma teknolojileri ile yeni bir sanal sunucu oluşturmak sadece birkaç dakika alabilmektedir.
- Sanal sunucuların donanım bağımsızlığı. Diğer bir ifade ile, sanal sunucular donanım bağımsız herhangi bir sunucu üzerinde çalışabilmesi.
- Konsolidasyon sayesinde daha "çevreci" bir veri merkezi ve sunucu ortamı oluşturulabilmesi.

Kurum mimarisinin temeline inildiğinde ve rekabeti devam ettirebilmek için zamanla nasıl geliştiklerine bakıldığında, başarıya giden yolun sunucu işletim sistemi ve kurum uygulamalarından geçtiği görülmektedir. Kurumu ayakta tutan yazılımlar ve bu yazılımların yeniden yapılandırması dile getirildiğinde, çok pahalı ve tehlikeli bir süreçten bahsedilmektedir. Bir değişiklik gerçekleştirildiği zaman uyumluluk ortadan kalkabilmekte ve geliştirme ile sınama süresi beklenenden uzun olabilmektedir. İşte sanallaştırma tüm bu gibi durumlarda devreye girmektedir ve kurumlara istediklerini vermektedir: Daha fazlası!

Sanallaştırmaya daha fazla gereksinim duyulduğu durumlar ise, aşağıdaki gibi bir liste ile özetlenebilir:

a. Sunucu Çiftlikleri

Sunucu çiftliği (server farm) yöneticileri sanallaştırmayı başarıya giden yolda bir zorunluluk olarak görmektedirler. Daha önceki yapılandırmalarda kullanılan makineler standart uygulamaları çalıştırırlarken, yeni makineler sadece işletim sistemi kurularak çalışabilen birçok sanal makineler oluşturabilmektedirler. Bu makinelerde küçük bir ana işletim sistemi bulunmaktadır. Bu işletim sistemi ise ihtiyaca göre birçok sanal misafir makineler yaratabilmektedir. Sunucu çiftliği yöneticileri iş yükü miktarı değiştiği sürece tüm gün bu sanal makineleri denetleyebilmektedirler. Daha önce sadece donanımla yapılabilen bazı işlevlerin artık yazılımla gerçekleştirilebilmesi yöneticilere sınırsız hareket alanı tanımaktadır.

Şirketler kendi makinelerinden mümkün olduğunca yararlanmak ve donanım masraflarını en aza indirmek için büyük zamanlar harcamaktadırlar. Daha sonra uzmanlar bu makinelerin sayısının artık yetmeyeceğini düşündükleri anda sanal makineler oluşturma zamanı geldiğini anlarlar. Ancak, zamanında satın alınmış makineler sadece yüklenen işletim sistemini veya tek bir iş yükünü kaldırması için toplanmış olabilirler. Bu durumda daha önceki iş yükü ve işletim sistemi sanal makine haline dönüştürülebilir. Böylece satın alınan yeni ve güçlü makine üzerinde bunun gibi birçok sanal sistem çalıştırılabilir. Dolayısıyla satın alınacak sunucu sayısından tasarruf edilmiş olunur.

b. Değişken Hedefler

Günümüzde sunucu çiftlikleri için gerekli olan makinelerin sayısı en yoğun iş yüküne göre hesaplanmaktadır. Çoğu sunucu modelinin iş yükü, günlük yaptığı etkinliklere göre değişim göstermektedir. Şirketler, sanallaştırma ile fiziksel makinelerin iş yükünü artırarak önemli miktarda tasarruf sağlamaktadırlar. Sanal ve fiziksel makinelerin işlem yapmadığında kapatılabilir olması da toplam maliyeti önemli ölçüde düşürmektedir. Bu durum sanallaştırmanın önemli bir yararını daha ortaya çıkartmaktadır. Çok sık kullanılmayan makineler sanallaştırılıp o halde de kullanılabilirler. Elbette tüm bunların sonucunda şirketler donanıma vermiş oldukları parayı da amorti etmiş olmaktadırlar.

c. İnternet Servis Sağlayıcılar (İSS)

Günümüzdeki birçok İSS'de sanallaştırmanın getirdiği sınırsız paralellikten faydalanmaktadır. Temel kural şudur: Ne kadar çok makine çalışırsa o kadar fazla müşteri gelir. Bu sunucuların her biri aslında onlarca sanal makineye ev sahipliği yapmaktadırlar. Örneğin, tek bir makinede 50 farklı web sitesinin birden yayını gerçekleştirilebilir. Ama tahmin edilebileceği gibi bu sitelerden her birine düşen trafik miktarı çok sınırlı olacaktır. Yine de her sanal makine yaklaşık olarak gerçek bir sunucunun yapabildiklerini aynen gerçekleştirecektir. ISS, tek bir makineyi 50 istemci için kazanç kaynağı olarak görecektir ki, bu çok çekici bir değerdir. Fakat yine de işin asıl güzel olan kısmı bu değildir. İşin güzel tarafı: Bir sanal makinenin iş yükü giderek artar ve gerçek makine zorlanmaya başlarsa, o sanal makine daha güçlü bir sunucuya rahatlıkla taşınabilmektedir. Bunların hepsi gerçek zamanlı olarak gerçekleşebilir. ISS'ler arasında geçiş yapılırken sunucuların sadece birkaç saniyeliğine kapatılmaları gerekebilir. Çoğu zaman bu anlık kopukluğun farkına bile varılamaz.

3.1.1. Masraflarda Azalma

Bilişim hizmeti veren kurumlar ve firmalar, sanallaştırma teknolojilerinin kullanımı ile birçok farklı alanlarda masraflarda azalma anlamında kazançlar sağlayabilmektedir. Maliyet ve masrafları azaltan, sanallaştırmanın sonucu olarak ortaya çıkan başlıca etkenler şunlardır:

- Donanım biriminin etkin ve verimli kullanımı sonucu olarak, daha az sayıda donanım biriminin yeterli olabilmesi;
- Donanımların bakım işlevlerinin kolaylaşması ve hızlanması;
- Enerji tüketimi, soğutma ve fiziksel alan kullanımının azalması;
- Yedekleme ve hatadan kurtarma işlemlerinin kolaylaşması;
- Yeni yazılım ve donanım ürünlerinin testlerinin kolaylaşması ve kullanıma açılma sürelerinin kısalması.

Örneğin, BT sektöründe faaliyet gösteren büyük firmalardan birinin, kendi BT altyapısına ilişkin olarak yürüttüğü sanallaştırma çalışmalarının sonucu olarak, 3 bini aşkın dağıtık sunucu sayısını 30 kadar yüksek kapasiteli sunucuya indirmeyi, veri merkezi için gerekli alan miktarını %85 azaltmayı ve 5 yıl içinde 4 Milyar Doların üzerinde tasarruf sağlamayı başarmış olduğu bilinmektedir.

Veri merkezi altyapılarında, kablolama, iklimlendirme maliyetleri ve fiziksel alan kullanımında oluşan azalma neticesinde net bir kazanç sağlanmaktadır. Sunucu sayısının azalması ve yönetim kolaylıkları artması nedeniyle destek ve yönetim anlamında daha az insan kaynağına ihtiyaç duyulacak, kazanılan zaman tasarrufları sayesinde yeni teknolojileri araştırma ve uygulama şansı artacak ve kurum ve firmalara katma değer sağlanmış olacaktır. Sanal ortama geçiş ile beraber yeni sunucu (işlemci, ana bellek, disk) istekleri, sanal olarak, çok kısa süreler içinde karşılanabilir olacaktır. Böylece, yeni sunucular için kabin ve kablo ihtiyacı olmayacaktır. Ek taleplerde (ana bellek, işlemci, disk, ağ bağdaştırıcısı) sunucuya müdahale etmeksizin (teknik personele ihtiyaç duymaksızın) konfigürasyonlarda değişikliğe gidilebilmektedir. Sanal altyapılardan maksimum fayda sağlamak için iyi yapılandırılmış ve yönetilebilir bir sanal platform topolojisi tasarlanmalıdır. Kurumsal ihtiyaç ortaya net olarak koyulmalı ve bu anlamda gereken donanım ve hazır yazılımlar temin edilmelidir.

3.1.2. Çevreci Bilişim

Hızla değişen Dünya'nın gündeminde insanlığın en büyük ortak problemi ve endişesi haline gelmiş olan çevre ve çevresel dengelerin bozulması giderek daha fazla önem taşımaktadır. Artan enerji maliyetleri ve küresel ısınma nedeniyle gelişen çevre bilinci, enerji kaynaklarının en uygun ve etkin şekilde kullanılmasını zorunlu kılarken, enerjiden en fazla yararlanan teknoloji ürünlerini de değiştirmektedir.

Bilişim teknolojileri ve yeşil teknolojinin kesiştiği noktadaki '*Çevreci BT'* hareketi, hem enerji üretim ve kontrolündeki sorunları aşmak, hem de veri merkezleri ve kişisel bilgisayarlarda harcanan enerjinin miktarını azaltmak için çalışıyor. Bu doğrultuda çevreci BT'nin ortaya çıkardığı giderek yükselen eğilimlerden biri de çevreci veri merkezleridir. International Data Corporation (IDC)'nin araştırmasına göre Avrupa'daki veri merkezlerine harcanan enerji, İngiltere'nin sokak aydınlatmaya harcadığı enerjinin 6 katından daha fazladır. IDC'nin yaptığı bir başka araştırmada bir sunucu sistemi için ödenen her bir doların yarısının enerji tüketimi ve soğutmaya gittiğini ortaya koymaktadır [16].

a. Çevreci bir yapılanma için yol haritası

Gartner Group'un 2008 yılı başında hazırladığı raporda çevreci BT her yönü ile tanımlanmaktadır. Şirketler göz önünde bulundurularak yapılan bu tanıma göre çevreci BT; kurumsal operasyonların ve tedarik zincirinin çevresel sürdürülebilirliği için bilgi ve iletişim teknolojilerinin en iyi bir şekilde kullanımı anlamına gelmektedir. Rapor, pek çok BT organizasyonunun enerji tasarrufu tarafındaki konuları özümsemiş durumda olmasına rağmen bu süreçlerin, kurumların maddi yapılanmasıyla bağlantısı konusunda aynı durumun geçerli olmadığını da göstermektedir. Yine aynı rapora göre her BT organizasyonu, maliyetlerini azaltırken, çevresel başarımı da geliştirebilmektedir. Bilgi teknolojileri donanımlarının geri dönüşümü ise önemli bir başka nokta olarak ortaya çıkmaktadır. Araştırmanın ortaya koyduğu bir diğer saptama da BT yapılanmalarında çevre programı için kurumların atması gereken ve aşağıda sıralanan 10 adımdır:

- Çevre politikası ve stratejilerini belirleyin;
- Süreci ölçümleyin ve analiz edin;
- Çevreci kültürü oluşturun;
- Gerekli değilse lütfen kapatın;
- Veri merkezinde enerji tasarrufu için bütünsel hareket edin;

- ‘Her zaman açık’ yerine ‘her zaman ulaşılabilir’ mantığına geçin;
- Enerji faktörünü her karar aşamasında hesaba katın ve BT enerji yükünü kullanın;
- Çevreci yazıcıları ve çıkışları garantileyin;
- Teknoloji üreticilerini zorlayın;
- Teknoloji üreticilerinin kendi çevresel programlarını inceleyin.

b. Yeşil veri merkezleri

Yeşil veri merkezi; verinin yönetimi, yedeklenmesi ve yayılmasına ilişkin sistemin maksimum enerji verimliliği ve minimum çevresel zarar sağlayacak şekilde saklanmasıdır. Yeşil veri merkezi inşa etmek ve sertifikalandırmak maliyetli olmasına karşın uzun vadede düşünüldüğünde operasyonel ve bakım açısından tasarruf sağlamaktadır. En büyük avantajı çalışanlara sağlıklı ve rahat bir çalışma ortamı sunmasıdır. Buna ilave olarak yeşil hizmetler her zaman yerel yönetimlerle iyi ilişkiler kurulmasını sağlamaktadır.

3.1.3. Risklerde Azalma

Birçok kurumda aynı sunucu üzerinde birden çok hizmet verilmesi oldukça sık görülen bir durumdur. Örneğin web hizmeti verilen bir sunucu üzerinde birden çok web uygulaması, hatta web servisleri çalışıyor olabilir. Bu uygulamalarda çıkan bir sorun ya da bir saldırı bu sunucu üzerinde çalışmakta olan servisin (örneğin, Apache ya da IIS gibi web sunucuları) normal çalışmasını etkileyebilmektedir. Bu hizmetlerdeki olası bir açık bu sunucuda çalışan tüm hizmetlerdeki bilgilerin güvenliğini riske atmaktadır. Aynı sunucu üzerinde hem kuruma ait web sayfalarının tutulduğu, hem de diğer kurumlarla bilgi alışverişinin sağlandığı web servislerinin bulunduğu düşünüldüğünde, kurum web sayfalarındaki bir açıktan faydalanarak içeri sızmayı başaran bir saldırgan, aynı sunucu üzerinde hizmet verilen web servisleri ile taşınmakta olan ve çok daha fazla gizlilik değeri olan bilgilere de erişim şansına sahip olabilecektir. Bunun haricinde, uygulamalardan biri için gerekli olan bir değişiklik servisin yeniden başlatılmasını gerektirebilir. Servisin yeniden başlatılması ise bu servise bağımlı olan tüm hizmetlerin kesintiye uğraması anlamına gelecektir ki bu birçok zaman hizmetlerin kullanılmadığı zamanlarda bu çalışmaların yapılmasını gerektirecektir. Verilen bu hizmetleri ayrı sunucularda oluşturmak ise bu gibi sorun ve güvenlik açıklarından en az şekilde zarar görülmesini sağlayacak, aynı fiziksel makine üzerinde oluşturulmuş olsa bile farklı sanal sunucularda bu hizmetlerin verilmesiyle yalıtım sağlanmış olacaktır. Sunulan hizmetler ya da

kurumca kullanılmakta olan uygulama sunucularının kritiklik derecelerine göre sınıflandırılması, hatta gerekiyorsa farklı ağ bölümlerinde tutulacak şekilde ayrıştırılmasının kuruma maliyeti sanallaştırma ile oldukça düşmektedir. Tüm bu ölçütlerin maliyetleriyle birlikte değerlendirilmesi ve buna göre planlamaların yapılması uygun olacaktır.

3.1.4. Esneklik

Sanallaştırma, getirdiği esneklikler ve kolaylıklarla en çok bilgi işlem birimlerinin ilgisini çekmeyi başarmıştır. Bir sunucu üzerinde yapılmış bir değişikliğin beklenen sonucu vermemesi durumunda anlık kopyasına geri dönüş çok hızlı biçimde yapılabilmektedir. Diğer taraftan, bir sunucu yapılandırmasının aynısından bir tane daha oluşturmak istendiğinde bunu bir kaç basit işlemle yapabilecek olanaklara sahip olunacaktır. Ya da bir uygulama sunucusu kurulacaksa ve güvenlik sebepleriyle bu uygulamayı diğer sunuculara kuramama sorunu ile karşılaşıldığında, uygulamaya özel bir sunucu almak ya da eski sunuculardan birini kullanmak zorunda kalınacaktır. Bazı durumlarda uygulamanın çalışabilmesi için çok düşük bir hafıza rahatlıkla yeterli olabilecektir, ancak yeni bir sunucu alınması durumu düşünüldüğünde bu uygulama için çok yüksek kapasiteli hafızaya sahip bir sunucu alınması söz konusu olabilmektedir. Ancak bu oldukça maliyetli bir yatırım anlamına gelmektedir. Eski bir sunucu kullanıldığında ise, ilerde bu uygulamanın daha fazla hafızaya ihtiyaç duyduğu durumda yapabilecekler bellidir. Çok hızlı gelişen teknolojiyle beraber, ya zorlukla tedarik edilebilecek hatta belki de bulunamayacak eski bir hafıza kartına ihtiyaç var demektir ya da bu uygulama yeni bir sunucuya taşınmalıdır. Sanallaştırma durumunda ise, çok düşük seviyelerde bir hafıza ile başlayarak ihtiyaç duyulduğu durumda hafızanın artırılabilmesi söz konusudur ki, bu bilgi işlem birimlerinin sahip olduğu oldukça önemli bir kolaylıktır. Elbette ki bu durum örnekteki gibi yalnızca hafıza için değil tüm donanım kaynakları için geçerlidir. Oluşturulan kaynak havuzlarının sunucular için tanımlanmış olan öncelikleri de göz önünde tutularak otomatik olarak dağıtımı bile yapılabilmektedir.

3.1.5. Özgürlük: Marka Bağımlılığından Kurtulma

Veri merkezlerinde bulunan donanım kaynaklarına ilişkin olarak kapasite artırımı veya güncelleme gerektiğinde, ilk başta ürünlerin alınmış olduğu markaya bağlı kalma zorunluluğu oldukça sık olarak karşı karşıya gelinen bir durumdur. Özellikle sunuculara ilişkin olarak gelişen bu bağımlılık önemli boyutlara ulaşmakta ve diğer donanım ürünlerine ilişkin benzer bağımlılıkları da tetikleyebilmektedir.

Bahsi geçen donanım kaynaklarının sanallaştırılması ile bu bağımlılıktan kurtulmak mümkün olabilmektedir. Burada sanallaştırma yazılımı, altyapıdaki olası farklılıkların üzerini örtecek ve üst yapılara yansıtmayacak bir uyumlandırma katmanı olarak da rol oynayabilmektedir. Böylece, ileride bir kapasite artırımı veya güncelleme gerektiğinde, o sanallaştırma yazılımı ile uyumlu olarak çalışabilecek herhangi bir markanın ürünlerini seçmek mümkün olabilecektir. Ancak, bunun için seçilmiş olan sanallaştırma yazılımının, belirli bir donanım markasına bağımlı olmadığı konusuna dikkat etmek gerekmektedir.

Ayrıca, sanallaştırılma sonucunda sanallaştırma yazılımının kendi markasına bağımlı hale gelme riskini en aza indirmek üzere, seçilen sanallaştırma yazılımının başka sanallaştırma ürünleri ile uyumlu olup olmadığı konusu irdelenmeli ve mümkün olduğu ölçüde, diğer ürünler ile uyumlu olarak çalışabilen seçenekler içinden bir seçim yapılmaya çalışılmalıdır. Burada, seçilecek ürünün açık standartları desteklemesi, önemli bir gösterge olacaktır. Bu konuyla ilgili yapılan araştırmalara bakıldığında, sanallaştırma uygulamış olan veri merkezlerinin önemli bir kısmının, birden fazla ürün markasını kullanmakta olduğu görülmektedir (bkz. 7.1.1. Dünya'da Durum).

3.1.6. Dayanıklılık ve İş Sürekliliği

Sanallaştırma kullanılarak sistemlerin hatalara ve aksi durumlara dayanıklılıkları artırılabilir. Örneğin, taşıyıcı fiziksel sunucuya bakım işlemi yapılması gerektiğinde veya bu sunucuda bir sorunla karşılaşıldığında, bu fiziksel sunucu üzerinde bulunan sanal sunucular, kullanıcılara yansıtılmadan başka bir fiziksel sunucu üzerine kaydırılabilir. Böylece iş sürekliliği kesilmemiş olur. Bunun yanında sanallaştırılmış servislerin tam kopyaları düzenli olarak alınabilir. Böylelikle, bir problem oluştuğunda bir önceki sorunsuz duruma hızlıca geri dönülebilir. Bu noktada dikkat edilmesi gereken bir nokta ise, sanal sistemlere yönelik olarak dayanıklılığı ve iş sürekliliğini yüksek tutmak için, taşıyıcı sunucuların yüksek erişilebilir durumda tutulmalarının gerekli olduğudur. Fiziksel sunucuların yüksek erişilebilirliği sağlanmadan uygulanacak bir sanallaştırma, bu anlamda risk taşıyabilecektir.

3.1.7. Konsolide Bilgi İşlem Altyapısı

Sunucu konsolidasyonu, toplam sunucu sayısını veya sunucuların kurulu olduğu alanların sayısını azaltmak amacı ile sunucu kaynaklarının kullanımını verimli hale getirme yaklaşımı olarak tanımlanabilir. Yaptıkları işe oranla, çok sayıda

olan, çok kaynak tüketen ve fazla yer kaplayan sunucuların aşırı yayılmasına (server sprawl) yanıt olarak ortaya çıkmış pratik bir yaklaşımdır.

Konsolide ve daha sade bir bilgi işlem altyapısı elde edilmesi, sanallaştırma teknolojilerinin kullanıldığı birçok projenin doğal bir sonucudur. Bu altyapıya geçişte, sunucu sayılarına ve sunucuların kurulu bulundukları alanlara ilave olarak, aşağıda sıralanan parametreler üzerinde de azalma gözlemlenmektedir:

- Kabin sayılarında,
- SAN ve Ağ kablolamasında,
- SAN ve Ağ erişim cihazlarının sayılarında,
- Harici disk sistemlerinin alan kullanımı ve sayılarında,
- Enerji tüketim oranları ve buna bağlı kablo altyapılarında.

Bilgi işlem altyapılarının önemli sorunlardan birisi de kablolama ve bu düzenin düzgün şekilde yönetilmesidir. Sanallaştırma sayesinde sunucu sayılarında azalma ve bu sunucuların daha etkin kullanımı doğal olarak gerek enerji, gerekse ağ ve disk iletişimi için kullanılan kablo altyapısında azalma meydana getirecektir. Az sayıda uç, daha az sorun yaşatacak ve konsolidasyon sağlayacaktır. Örneğin bir sunucuda 2 adet ağ, 2 adet enerji, 2 adet disk bağlantısı, 1 adet monitör, 1 adet klavye, 1 adet fare, 1 adet yönetim portu kablosu olmak üzere ortalama 10 adet kablo ihtiyacı bulunduğunu varsayalım. Kurum ve firma hizmet sunması gereken 10 adet servis olduğunda 10x10=100 adet kablo edecektir. Bu ihtiyacın sanal altyapıyla beraber 2 sunucu ile karşılandığı bir ortamda 10x2=20 kablo ile çözüm sağlanacaktır. Bu örnek için %80 oranında azalma sağlandığı görülmektedir. Fiziksel kablolama oranının azalması doğal olarak kenar anahtarlar, SAN anahtarlar ve enerji sağlayan diğer cihazlar açısından da ihtiyaçların azalmasına neden olacaktır. Sunucu ve kabin kullanımının azalması neticesinde sistem odası altyapısında fiziksel hacimden de kazanç sağlanmış olacaktır.

3.1.8. Kolay Yönetilebilirlik

Sanallaştırma kullanıldığı zaman sanallaştırılmış bütün sistemlerin yönetimi kolaylaşmaktadır. Tüm sistemlerin istenildiği zamanda bir kopyası alınıp yönetim işlemleri üzerinde yapılabilir. Bunun yanında, sistemin üzerinde bir işletim sistemi çalışmasından farklı olarak bazı güvenlik açıkları sanallaştırma programı tarafından kapatılabilir. Sistemin kullanacağı donanım kaynakları da dahil olmak üzere tüm istenilen özellikler sistem kapatılmadan veya kullanıcılar için bir kesinti olmadan yapılabilir.

3.1.9. Başarım (Performans)

Gereksinimlere çok daha iyi uyacak sanal kaynakların tanımlanması ile önemli başarım artışları elde etmek mümkün olabilmektedir. Diğer yandan, sanallaştırma yöntemleri düzgün ve doğru planlanarak uygulanmadığında başarım olarak istenilen veya beklenen elde edilemeyebilir. Sanallaştırmanın amacı ortak kaynakların en verimli şekilde kullanılabilmesini sağlamaktır. Ortak kaynak kullanımı, yüklü sunucuların yükünü azaltacak ve diğer sunucuların başarımını olumsuz etkilemeyecek şekilde dağıtacaktır. Sanallaştırma uygulanmadan önce planlama iyi yapılmalıdır. Kullanılacak olan bütün donanımın sanallaştırma desteğinin olması yüksek başarım için gereklidir.

Sanallaştırmaya geçirilecek olan platformların esas olarak işlemci, bellek ve disk kullanımlarının önceden profilinin oluşturulması ve bu çalışma sonrasında hangi platformların aynı havuzda yer alacağına karar verilmesi önemli bir ön koşuldur. Örneğin, sürekli olarak aynı zamanda disklere yoğun biçimde erişmek isteyen iki ayrı uygulamanın sanallaştırılsa bile aynı fiziki sistemde bulunan bir havuzda yer alması ister istemez başarımı olumsuz etkileyecektir.

Genel anlamda işlemci dışı yük gereksinimleri açısından tamamlayıcı olan platformların bir arada tutulması hedeflenmelidir. İşlemci yükü açısından ise, benzeri paralel işlem ve iş parçacığı (thread) kullanım profili olan platformların aynı fiziki sistemde, yüksek düzeyde paralelleştirilmesi olanaklıdır.

Sanallaştırma başarımını önemli ölçüde etkileyebilecek bir diğer konu da sanallaştırılmış sistemlerin biri birleri ile olan bağımlılıklarının incelenmesi ve tek bir platformda gerçekleştirilen bir işlemin, sanallaşmış olmasından dolayı bir diğerinde yeni bir etki yaratıp yaratmadığının saptanmasıdır. Örneğin, birçok bilgi sistemi DNS sunucularını yoğun biçimde kullanır. Sanallaştırılmış bir DNS sunucusunun artıları ve eksilerinin iyi değerlendirilmesi, DNS kaynaklı problemleri ve başarım dar boğazlarını önemli ölçüde azaltabilir.

3.1.10. Verimlilik

BT birimlerinin, yetersiz planlama ve yanlış yatırımlardan kaynaklanan yüksek maliyetler yüzünden önemli sıkıntılar yaşadığı görülebilmektedir. Bu nedenle, kuruluşlarındaki giderleri azaltırken kendi derecelerinde verimlilik göstermeye de ihtiyaç duyarlar. Bu, son yıllarda gittikçe belirginleşen bir durumdur ve bu yüzden BT yöneticilerinin gider azaltma cephaneliğine gelecek her yeni silah

hoş karşılanmaktadır. Bu yeni silahlardan bir tanesi ise sanallaştırma olarak öne çıkmaktadır.

İngiltere Maliye Bakanlığı'nın açıklamış olduğu bütçe raporunda; 2011 itibariyle kamu sektörünün verim tasarrufuna ekstra £5.000 katkı yapma zorunluluğu getirilmiştir. Zaten hali hazırda £30.000 katkı yapan kamu sektöründe bu zorunluluk kaygı ile karşılanmıştır. Bu ek katkıyı sağlayabilmek amacıyla yeni ve sıkı önlemler alınması gerekliliği ortaya çıkmıştır. Bunun sonucunda kurumlar vermiş oldukları hizmetleri aksatmadan bu katkıyı sağlayabilmek amacıyla, doğal olarak hemen BT birimlerine başvurmuşlardır [17].

Verimliliği arttırmanın en kolay ve en etkili yollarından birisi bir sanallaştırma programı uygulamaktır. Araştırmacı firma Quocirca'nın hizmet müdürü Clive Longbottom, "Sanallaştırmayı gereken iş miktarı yüzünden erteliyorsanız şimdi tekrar değerlendirme zamanıdır" demiştir: "Sanallaştırma bir yatırımdır, elde edeceğiniz hızlı kazanç ise olağanüstüdür. Eğer olanağınız varsa veri merkezleriniz için de sanallaştırmaya yatırım yapın, bu sayede muhafazadan, veri merkezindeki enerjiden ve gayrimenkulden tasarruf elde edeceksiniz".

Veri merkezleri, enerjinin yetersiz kullanıcılarıdır. Geleneksel bir sunucu sadece bir işletim sistemini çalıştırabilir; kapasitesinin yalnızca %10'unu kullanabilir ve büyük miktarlarda enerji tüketir. Longbottom şöyle açıklamaktadır: "Eğer bir sunucu 70 Vat işlemciye sahipse ve bunun sadece %10'unu kullanıyorsanız sunucu yaklaşık 55 Vat kullanıyor demektir". Burada sunucu enerjiyi boşa harcamaktadır ve sunucu soğutmasının ekstra gideri ise, onu çalıştırmaktan neredeyse dört kat daha pahalıdır. "%10 fayda sağlıyorsunuz fakat sunucunun %100 lük kısmı için para ödüyorsunuz ve çevresel giderler için de dört kat masraf yapıyorsunuz" diyor Longbottom. "Bu sürdürülemez çünkü çevreye pahalıya mal olur ve BT bütçesine büyük bir darbedir".

Ancak sanallaştırma bir fiziksel sunucunun farklı işletim sistemlerini çalıştırabilmesini sağlar. Böylece birçok sanal sunucu gibi hareket etmiş olur. Fiziksel sunucu, %10 kapasiteyle çalışmak yerine, kapasitesinin %50'siyle veya daha fazlasıyla çalışır. Sonuç olarak veri merkezindeki beş sunucunun dördü kapatılabilir ve böylece bu sunucuların çalıştırma ve soğutma masraflarından tasarruf edilebilir. Sanallaştırma, ev sunucularına daha büyük bir veri merkezi bulma zorunluluğunu da erteler. Kullanım çoğaldıkça kullanılmamış sunucuları kolayca açılabilir.

3.1.11. Dış Kaynak Kullanımı

BT dış kaynak kullanımı (outsourcing), kendi altyapısını kurmada sıkıntı çeken birçok kuruluş için öncelik haline gelmiştir. Ekonomik sıkıntı içindeki birçok firma, BT giderlerini azaltma ihtiyacı duymuştur ve bir kısmı dış kaynak kullanımına yönelmiştir. Dış kaynak kullanımından önceleri kaçınan firmalar, şimdilerde konuya sıcak bakmaktadırlar. Çünkü ekonomik durgunluk, fiyatları aşağı çekmiştir ve imalatçıları daha esnek koşullar sunmaya teşvik etmiştir.

Uzun süredir var olan web sunucu barındırma ve sunma hizmetine benzer bir yaklaşım, sanallaştırma yöntemlerini kullanarak çok daha fazla yaygınlaşmaktadır. Uygun yöntemlerle sanallaştırılmış olan kaynaklar, kullanıcıları olan özel veya tüzel kişilere ücreti karşılığında sunulabilmektedir. Bunların arasında, sanal sunucu, sanal veri depolama alanı ve hatta sanal ağ gibi örnekleri vermek mümkündür. Bu yöndeki gidiş, sanal veri merkezlerinin sayısının artmasını ve bulut bilişim yaklaşımının yaygınlaşmasını da getirebilecektir.

Yapılmış olan bir araştırmaya [18, 19] göre, birçok sektör, BT dış kaynak kullanımıyla aktif bir şekilde ilgilenmektedirler. Dev şirketler arasında yapılan bu tarz anlaşmalar, böyle bir oluşumun büyük boyutuyla Dünya pazarına geldiğinin önemli işaretleridir. Aynı araştırmanın sonuçları, şirketlere, kazanmak ve ticareti sürdürmek için sanallaştırma ve dış kaynak kullanımı gibi yeni teknolojilere sahip olmalarını da önermektedir.

3.2. Dikkat Edilmesi Gereken Konular

Sanallaştırma teknolojileri, pek çok yarar sunmalarının yanı sıra, uygulama da dikkat edilmesi gereken bazı konuları da içlerinde barındırmaktadır. Farklı bir yaklaşım gerektirmesi ve yetişmiş insan gücüne ihtiyaç duyulması, sanallaştırma teknolojileri ile ilgili dikkat edilmesi gereken konulardan sadece birkaç tanesidir. İlerleyen sayfalarda bu konudaki ana başlıklar tek tek ele alınıp açıklanmaya çalışılmaktadır.

3.2.1. Farklı Yaklaşım ve Uzmanlık Gerektirmesi

Sanallaştırma normal sistem yöneticiliğinden daha farklı düşünmeyi gerektirir. Gerek sanallaştırmanın altyapısının oluşturulması süreci boyunca gerekse sanallaştırma sonrası bakım ve sistem yönetimi kapsamında konu hakkında uzmanlık ve bilgi birikimi hedeflenen dönüşümün başarısı için temel faktörler arasındadır.

Sanallaştırılmış sistemler normal sistemlerden çok birlikte çalışan, anında yedeklenebilen sistem öbekleri şeklinde görülmelidir. Böyle bir sistemin kullanımına geçilmesi durumunda, sistem yöneticileri eski anlayışları ile bu sistemi yönetemeyeceklerinin farkında olmalıdır. Bu konudaki kaynakları detaylı olarak araştırmalı ya da sanallaştırma ile ilgili var olan bir uzmandan eğitim almalıdır. Bu eğitimin yapılmaması Hatalı Yönetilme maddesinde belirtilen sonuçların ortaya çıkmasına sebep olacaktır. Örneğin, sanallaştırılmış bir platformun güvenliğini sağlamak veya üzerindeki uygulamaların bakımını gerçekleştirmek normal sistemlere göre farklılıklar göstermekte ve özel uzmanlık gerektirmektedir. Misafir bir işletim sistemindeki bir açıktan yararlanıp sanal makine monitörünü ele geçirmeye çalışan bir saldırgan için alınacak önlemlerin farklılığı buna örnek olarak verilebilir.

Sanallaştırma konusunda yeterli uzman personel bulunmaması firmaların ve kurumların sanallaştırmaya başlamasını geciktirici önemli faktörlerden biri olarak ortaya çıkmaktadır. Bu kapsamda yeterli seviyede personel yetiştirmek hem pahalı hem de kimi zaman mümkün dahi olamamaktadır. Elbette, bu teknolojinin popülaritesinin artması ve yaygınlaşması ile yetişmiş uzman sayısının gün geçtikçe artmakta olduğu da göz ardı edilmemelidir.

3.2.2. Hatalı Yönetilme

Bilişim platformunun sanallaştırılması ile hedeflenen önemli kazanımlarından birisi kolay yönetilebilir bir platform oluşturulmasıdır. Ancak, dikkatlice planlanmamış ve kurumun ihtiyaçlarına göre tasarlanmamış bir sanallaştırma altyapısı, yetersiz uzmanlık veya sürecin iyi yönetilememesi gibi faktörler sadece sistem yönetiminde değil sanallaştırma ile hedeflenen tüm muhtemel kazançlara sekte vuracaktır.

Gerçekleştirilen sanallaştırma ile uygulamaların kapsamına bağlı olarak altyapının düzenli olarak denetlenmesi gerekmektedir. Yedekleme ve geri yükleme, bellek yönetimi, ağ bağlantısı, güvenlik, sunucu oluşturma ve değişiklik yönetimi süreci gibi konular üzerinde durulması gereken yönetim konularıdır. Bu kapsamda sıklıkla karşılaşılan sorunların başında sistemi eskisi gibi tek başına çalışan sistem gibi yönetmeye çalışmak gelmektedir. Yönetim sürecinde eskiden olduğu gibi sistem güncellemeleri için tüm sistem indiriliyorsa, bağlı olunan kullanıcılar düşünülmeden sistem yeniden başlatılıyor veya sistem yönetimi çalışan sistem üzerinde yapılıyorsa bu sanallaştırmanın beklenen getirilerini ortadan kaldırabilmektedir.

Sanallaştırılmış bir ortamda dikkat edilmesi gereken bir diğer husus ise hangi uygulamaların sanallaştırılacağının belirlenmesidir. Her uygulama sanallaştırma için uygun değildir. Uygun olsa bile doğru bir yaklaşım ile gerçekleştirilmediği sürece

olumsuz sonuçlar doğurabilir. Örneğin, küçük çaplı uygulamalar aynı donanım üzerinde diğer sanal sunucularla birlikte çalışan bir sanal sunucu üzerinde yer alabilir. Diğer taraftan, örneğin bilimsel işlevler veya finansal işlemler gerçekleştiren birçok işletim sistemi çağrıları yapan bir yazılım paketi tek başına bir sanal sunucuda ve hatta doğrudan işletim sistemi üzerinde çalışacak şekilde kurulabilir. Ek olarak, uygulamanın kritiklik seviyesine göre başarım, kapasite, süreklilik ve güvenlik özelliklerine göre sanal sunucu kullanımı çeşitlilik gösterebilir.

Kısaca, sanallaştırma sürecinde ve sonrasında hedeflenen kazanımlara ulaşabilmenin yolu doğru ve etkin yönetimden geçmektedir. Bu çerçevede, özellikle üretici firmalardan sağlanan araçların ve kaynakların en iyi şekilde kullanılması anahtar rol oynamaktadır.

3.2.3. Oluşturma Maliyeti

Sanallaştırma çözümleri için çalışmaya başlandığında farklı ürün ve çözümler konusunda gerçekten iyi bir araştırma yapılıp bilgilenmek gerekmektedir. Çünkü sanallaştırarak fayda sağlamak istenilen alanlarda, gerçekleştirilen maliyetlerin hiç bir zaman geri dönmeyeceği gerçeğiyle karşılaşılabilir.

Hangi sanallaştırma teknolojisinin (sunucu, uygulama, masaüstü, oturum sanallaştırması v.b.) kullanılacağı belirlendikten sonra bilgi sistemleri için mimari yapıyı ortaya çıkaracak çalışmaların gerçekleştirilmesi gerektirmektedir.

Bu aşamada maliyetler de ortaya çıkmaya başlayacaktır. Kullanılacak mimari yapıya ve sanallaştırma teknolojisine bağlı olarak maliyetlerde farklılıklar görülecektir.

Aşağıda temel maliyet kalemlerine dikkat çekilmektedir:

- Mimari yapı çalışmaları: Bilgi sistemlerinizin mimari yapısı ve kullanılacak sanallaştırma teknolojisi için yapılacak bu çalışmalar günlük işlere ilave olarak gerçekleştirilecektir ve ciddi bir zaman maliyeti çıkaracaktır. Bu süreçte sanallaştırma ile ilgili ürünlerin pek çoğunda mevcut olan ve ihtiyaçların belirlenmesinde kullanabilecek yazılımsal araçlardan mutlaka faydalanmak gerekmektedir.
- Donanım maliyetleri: Mimari yapı ve sanallaştırma teknolojisi belli olduktan sonra ihtiyaç duyulacak donanımlar bir maliyet kalemi olarak ortaya çıkmaktadır.

- Veri depolama maliyeti: Sunucu, masaüstü ve uygulama sanallaştırması gibi çalışmalarda sistemin vazgeçilmez bileşenlerinden biri de iyi bir veri depolama cihazıdır.
- Yazılım maliyetleri: Kullanılacak olan sanallaştırma platformu, yan bileşenleri ve bu platformda sanallaştırılacak olan işletim sistemleri ile uygulama yazılımlarının lisans bedelleri önemli bir maliyet kalemidir.
- Güvenlik maliyetleri: Kesintisiz çalışmadan felaket kurtarmaya, yedekleme sistemlerinden güvenlik ihtiyaçlarına kadar her kalem bir maliyet kalemi oluşturmaktadır.
- Yetişmiş eleman maliyetleri: Sanallaştırma teknolojilerinizin kullanımı, yönetimi, servis ve desteğinin verilmesi için gerekli olan elemanların yetiştirilmesi veya yeni istihdam edilmesi de bir maliyet kalemi olarak yer almaktadır.

3.2.4. İnsan Faktörü

Sanallaştırmaya başlamadan önce tüm alternatifleri değerlendirmek gereklidir. Sanallaştırma kararı alırken birtakım sorunlarla karşılaşılması olasıdır. Temel zorluklar teknik konularla ilgili değildir. Planlama, kapasite planlama ve üst yönetimden destek alma gibi zorluklardır. Sanallaştırmaya girdiğiniz bu noktada teknolojiden çok daha fazla faktör söz konusudur. Örnek olarak, insan, süreç ve finansal faktörler verilebilir. Her stratejide olduğu gibi anlamlı bir sonucun üst yönetime ispat edilmesi gerekmektedir. Hem iş birimlerinin hem teknik birimlerin desteğini almak çok önemlidir. Kendi bütçelerine sahip olan şirketler bazı işleri kendileri belirlemek isterler. Ortamı mümkün olduğunca uyumlu hale getirmek ve modüler bir yapıda ilerlemenin faydalı olacağı düşünülmelidir. Sanallaştırmada yeterli süreçler ortaya koyulamadığında, yönetim daha karmaşık bir hale gelebilmektedir. Sanallaştırma bugüne kadar hep konsolidasyon şeklinde devam etmiştir. Olması gereken aslında servis odaklı bir sanallaştırma yaklaşımıdır. Otomasyon her zaman ciddi bir şekilde değerlendirilmeli ve dinamik olarak kaynak paylaşımlarına önem verilmelidir.

İnsanlar sık kullandıkları araçlardan kolay vazgeçmek istemezler. Bazen alışkanlıklardan bazen de yeniliğin getirdiği bilinmezlik güvensizliği ortaya çıkarmaktadır. Ancak, sanallaştırma gibi yeni bir yapılanma sürecine girmeden önce yeterli bilgilendirme ve eğitimler verildiği takdirde, bu duruma olan direnç de o kadar azalır. Sanallaştırma ile birebir çalışacak teknik personelden tutun, uygulamaları kullanacak son kullanıcılara, hatta direkt bir ilgisi olmayacak idari görevlerdeki

yöneticilere kadar yeterli bir bilgilendirme gereklidir. Kurumdaki insanların sanallaştırmayı benimsemesi, hem gelecekteki kurum kültürüne katkı sağlamakta, hem de bu geçiş sürecindeki olası problemleri azaltmaya faydalı olmaktadır.

Sanallaştırma çok ciddi bir değişimdir. Gerektiğinde yeni rollere bürünüp yeniden organizasyonlar yapmak gerekebilir. Bu değişim, insan kaynağı açısından da ciddiyetle ele alınmalı; insan faktörü göz ardı edilmemelidir [20].

3.2.5. Uygun Olmayan Ortamlarda Kullanım

Sanallaştırma bilgi teknolojilerini yöneten ve kullanan kişi ve kurumlara büyük avantajlar sağlamasına rağmen her zaman herkes için aynı kazanımlar söz konusu olmayabilir. Hatta, kullanılan bazı özel hizmet sunucularının veya uygulamaların yapısı nedeniyle anılan çözümler bazı kurumlar için uygun bulunmayabilir. Sanallaştırmanın, kurumun yapısı için uygunluğu; uygulandıktan sonra yönetimde kolaylık, ekonomiklik, güvenlik gibi konularda avantajlı olup olmayacağı planlanmalıdır.

Tablo 3.1: Sunucu Sanallaştırması Gider Karşılaştırma Parametreleri

Öncesi	
A	Sunucu sayısı
B	Sunucu, kurulum, yazılım başına maliyet
C	Sunucu başına iletişim portları dahil ağ gideri
D	Sunucu başına disk
E	Sunucu başına maliyet (B + C + D)
F	Sunucu başına yıllık maliyet - 3 yılda amortisman (E / 3)
G	Yıllık elektrik ve iklimlendirme
H	Yıllık sistem odası, güvenlik ve raf işgali
I	Sunucu başına yıllık maliyet (F + G + H)
J	İşletim personeli maliyeti (~1 operatör / 20 Sunucu)
K	Yönetim ve sistem müh. maliyeti (~1 kişi / 100 sunucu)
L	Kurulu adet için toplam maliyet (A x (I + J + K))
Sonrası	
M	Sunucu sayısı
N	Sunucu, kurulum, yazılım başına maliyet
O	Sunucu başına iletişim portları dahil ağ gideri
P	Sunucu başına disk
Q	Sunucu başına maliyet (N + O + P)
R	Sunucu başına yıllık maliyet - 6 yılda amortisman (Q / 6)
S	Yıllık elektrik ve iklimlendirme
T	Yıllık sistem odası, güvenlik ve raf işgali
U	Sunucu başına yıllık maliyet (R + S + T)
V	İşletim personeli maliyeti (~1 operatör / 20 Sunucuya)
W	Yönetim ve sistem müh. maliyeti (~1 kişi / 100 sunucuya)

X	Kurulu adet için toplam maliyet (M x (U + V + W))
Sanallaştırma Kazançları	
	Toplam sunuculardan tasarruf ((A x F) - (M x R))
	Toplam altyapıdan tasarruf ((G + H) x A - (S + T) x M))
	Toplam insan kaynaklarından tasarruf ((J + K) - (V + W))
	Sanallaştırma % Tasarruf ((L – X) / L)

Örnek olarak, masaüstü sanallaştırmasında dağıtık yapıdaki gerçek kişisel bilgisayarların merkezileştirilmesi ve ortak hafıza ünitesini kullanmaları verilebilir. Bu durumun gerekliliklerinin iyi tespit edilmesi ve yapılacak yatırımların hesaplanması gerekir. Ortak hafıza kullanmak, ayrı ayrı hafıza birimi kullanmaktan daha pahalı bir yöntemdir. Kimi durumda, uygulandığında ekonomikliğini kaybedebilir. Aynı zamanda gerekli olan ağ alt yapısı için yapılacak yatırımın da hesaplanması, sanallaştırmanın maliyetinin tespit edilerek, ilgili ortam için uygun olup olmadığının görülmesini sağlayacaktır [21].

Bir başka örnek olarak sunucu sanallaştırması verilebilir. Burada, uygulama öncesi ve sonrası giderler, yol gösterici olarak Tablo 3.1'de verilene benzer şekilde hesaplanarak, karşılaştırılabilir.

3.2.6. Lisanslama Sorunları

Sanallaştırmaya yönelik yazılım lisansları henüz yaygın olarak uygulanmamaktadır. Bu tip lisanslamalarda, lisans gereksinimi sanallaştırma uygulamasından bağımsız olarak hesaplanmalıdır. Bazı durumlarda, uygulanan lisans yapılarında belirsiz durumlar olabilir. Bu tip problemler ileride işleri bürokratik sebeplerle aksatabileceği için, bu hususlara dikkat edilmesi ve yazılımların alınacağı şirketlerle diyaloga geçilmesi gerekmektedir.

3.2.7. Merkezi Yapı

Merkezi bir yapı yönetilebilirlik ve ölçeklenebilirlik için çok iyi bir mimari yapı olsa da, her tür felaket senaryosuna cevap vermek bazen çok yüksek maliyetlere sebep olabilmektedir. Bu maliyetleri karşılamak istemeyen kurum veya kuruluşlar zaman için de bir takım sorunlarla karşı karşıya kalabilmektedirler. Aşağıda bu sorunların bir kısmına değinilmektedir:

Merkezi yapılarda genellikle tek yedekleme cihazı kullanılır. Sistemlerin yapısına bağlı olarak bu durum bazen ciddi bir risk içermektedir. Ayrıca yedekten geri dönme senaryoları denenmemekte, alınmış manyetik teyp yedeklerinden geri dönüşler zaman kaybı gibi görülerek üzerinde fazlaca düşünülmemektedir.

Büyük sunucu sanallaştırması yapılan merkezlerde bir sistematik oluşturulmadan işe başlandığı zaman çok kısa bir sürede hangi sanal sunucunun hangi amaçla yaratıldığı konusunda ciddi karmaşalar yaşanmaktadır. Sanal sistem üzerinde kimsenin kullanmadığı, bu kez sanal sistemin kaynaklarını boşa harcayan çöplükler oluşabilmektedir.

Merkezi yapılardaki sorunların bir kısmı da elektrik, iletişim ağı cihazları ve iklimlendirme gibi çevresel sorunlardan oluşmaktadır. Bu sorunların en başında elektriksel sorunlar gelmektedir. Yedekli ve seri veya paralel olarak çalışacak bir kesintisiz güç kaynağı sistemi (KGS) yerine tek bir KGS sistemi genellikle tercih edilmektedir. Bu gibi durumlarda cihazda yaşanacak her tür sorun doğrudan sistemleri etkilemektedir.

İletişim ağı cihazları için de bir yedeklilik kavramı genellikle düşünülmemektedir. Bir kenar anahtarın güç ünitesinin yedekli olması lüks gibi görünmekte, ancak bir elektrik sorunun da arıza yapan güç ünitesi nedeniyle çalışmayan bir anahtar yüzünden bazen bir grup insanın iş yapamaz hale gelmesi ile ciddi bir işgücü kaybı yaşanabilmektedir.

Merkezi yapılardaki çevresel sorunlardan bir diğeri de sistem odalarının iklimlendirme yapılarının gerekli özen ve dikkatle hazırlanmamasıdır. İleriyi düşünmeden bugünkü ihtiyaçlar için yapılan yatırımlar veya hızlı büyüme dönemlerinde gözden kaçan iklimlendirme ihtiyaçları sistem odaları için en önemli sorunlardan birini oluşturmaktadır. Sunucular aşırı ısınmadan dolayı durduğu zaman hem ihmal edilen iklimlendirme çalışmalarının hem de merkezi yapının sakıncaları daha net ortaya çıkabilmektedir.

3.2.8. Sanallaştırma Katmanlarının Getirdiği Ek Yük

Bilişim kaynakları üzerinde kurulu bulunan her bir katman, altyapı kaynakları için bir yüktür. Sanallaştırma yazılımı da, sanallaştırmayı sağlamak için altyapı üzerinde kurulu bulundurmak durumunda olan bir katmandır ve kendisine düşen görevleri yerine getirebilmek için kaynağa (işlemci zamanı, bellek, veri alanı vb.) gereksinim duyar. Bu durumun, sistemlerden alınacak başarım değerlerinde bir miktar kayıp olarak ortaya çıkması mümkündür.

Başarım kaybının en alt düzeyde olması ve hatta mümkünse sanallaştırma ile elde edilebilecek başarım kazancının altında kalabilmesi için eldeki sistem ve uygulama yapısına en uygun çözümlerin uygulanması gerekmektedir.

3.2.9. Vazgeçme Maliyeti

Sunucu sanallaştırması gibi kurumun temel sunucu yapılanmasını değiştirecek bir proje çalışmasına başlarken öncelikle göz önünde bulundurulması ve değerlendirilmesi gereken önemli unsurlardan bir tanesi de vazgeçme maliyetidir. Çıkış maliyeti olarak da adlandırılan vazgeçme maliyeti denildiğinde yalnızca ücret ödemeleri düşünülmemelidir. Herhangi bir işlem sürecinde harcanacak olan zaman maliyeti, durması muhtemel temel servislerin kurumsal maliyeti, bu süreçte harcanacak olan iş gücü maliyeti ve en önemlisi olası veri kayıpları sonucunda oluşacak olan maliyetlerin toplamı olarak düşünülmelidir.

Bir örnek üzerinden konuyu detaylandırmak gerekirse:

"A Kurumu" sanallaştırma yöntemi ile sunucularını sanallaştırmak üzere proje çalışmaları yapmaktadır. Yapılan değerlendirmeler sonucunda "Sanallaştırma" teknolojisinin kurum açısından faydalı olduğu sonucuna varılmış ve "X Çözümü"nün kullanılması kararı alınmıştır. Bu çözümü "Y Firması" sağlamaktadır. Çözüm uygulamaya alınır ve tüm sunucular sanallaştırılır. Ancak bir süre sonra aşağıdaki durumlardan bir ya da birkaç tanesi ile karşılaşılır:

- "X Çözümü"nde önemli bir güvenlik problemi ortaya çıkmış ve "X Çözümü"nü üreten firma bu açığı kapatmakta gecikmeler yaşamaktadır. Mevcut sunucular üzerinde kritik bilgi ve işlemler olması nedeni ile acilen ilgili servislerin güvenli ortama aktarılması gerekmektedir;
- "X Çözümü" ile oluşturulan bu yapılanmada bazı yükler altında sorunlar ortaya çıkmaya başlamıştır;
- Yeni geliştirilmiş olan "Z Çözümü" ile kurumsal ihtiyaçlar çok daha sorunsuz ve yüksek başarım ile karşılanacak hale gelmiştir;
- "X Çözümü" ile veri kayıpları oluşmaya başlamıştır…

Bu durumda "A Kurumu" mevcut yapılanması için kullanmakta olduğu "X Çözümü"nden vazgeçmek ve "Z Çözümü"nü uygulamakla karşı karşıyadır. Kurumun vermekte olduğu servislerin durdurulması gibi bir durum söz konusu değildir. Kritik sorular bu noktada ortaya çıkacaktır.

- "X Çözümü"nden vazgeçip "Z Çözümü"ne geçmek mümkün müdür?
- "X Çözümü"nden vazgeçtiğimizde veri kayıplarımız olacak mıdır?
- "Z Çözümü"ne geçiş sürecimiz ve maliyeti ne kadar olacaktır?

Tüm bu ve benzeri soruların yanıtları bizlere vazgeçme maliyeti boyutlarını gösterecektir.

Vazgeçme maliyeti olarak karşımıza çıkacak olan bu tür risklerin önceden göz önünde bulundurularak en aza indirgemenin temel unsuru "Açık Standart"lara uygun geliştirilmiş olan çözümlerin tercih edilmesi olacaktır [22].

3.2.10. Hukuksal Açıdan Durum

Rapor hedef kitlesinin Kamu Kurumları olması nedeni ile yapılacak olan değerlendirmeler bu kapsam içerisinde ele alınacaktır. Örneğin, ülkemizde hiçbir kamu kurumunun kendi sunucularını özel bir firmaya ait veri merkezlerinde ya da kendisine ait olmayan bir sunucu üzerindeki sanallaştırılmış ortamda tutmayacağı gerçeğinden hareketle, bu tür durumlarda ortaya çıkması muhtemel Hukuksal durumlar ele alınmamıştır.

Kamu kurumları açısından sanallaştırma ortamlarında ortaya çıkması muhtemel hukuksal sorunları 3 ana başlık altında ele alabiliriz:

i. İzinsiz erişim

ii. Sanallaştırılmış ortamın ve bu ortamdaki içeriğin sahipliği

iii. Lisanslama

Bu alanların her biri “Sunucu Sanallaştırması” ve “Masaüstü Sanallaştırması” boyutları ile farklılıklar gösterebileceğinden her bir alan kendi içerisinde iki farklı açıdan değerlendirilmeye çalışılacaktır.

a. İzinsiz Erişim

Fiziksel sunucu açısından “izinsiz erişim” durumunda oluşan hukuki durumun sanallaştırılmış sunucularda herhangi bir farklılık oluşturmayacağı düşünülmektedir. Bu durumda aynı kanun maddeleri ile değerlendirilmesi mümkün olabilecektir.

Ancak, masaüstü sanallaştırması durumunda durum biraz karmaşık yapıya ulaşabilmektedir. Masaüstü sanallaştırmasında kişiye ait olan dosyalar da Sanal Masaüstü'nde (yani sunucuda) ya da ortak erişim sağlanabilen depolama sunucularında bulunabileceğinden herhangi bir hukuki sorumluluk gerektiren içeriğin kim tarafından oraya konulduğu konusunda adli inceleme aşamasında sorunlar çıkabileceği açıktır. Bu durumda bilgi işlem personelinin de sorumluluğunun ortaya çıkması düşünülebilir.

Ofise izinsiz girip bilgisayarın birebir kopyasını çıkarmak kimi kurumlarda imkansız denecek kadar zor olabilir. Ancak, sistem yöneticisinin sanal masaüstüne

erişmesi ve birebir kopyasını çıkarıp kurum dışına taşıyabilmesi dakikalar içerisinde olabilecektir. Bu eylemin oluştuğunun tespiti de kimi zaman mümkün olmayabilecektir.

b. Sahiplik

Sunucunun sanal ya da fiziksel olmasının kamu kurumları açısından herhangi bir farklılık oluşturacağı düşünülmemektedir. Kaldı ki herhangi bir kurumun fiziksel anlamda kendisine ait olmayan herhangi bir merkezde fiziksel sunucu barındırması ile sanal sunucu barındırması arasında da bir farklılık oluşacağı düşünülmemektedir. Bu durumda sanal sunucu sahipliği konusunda Hukuki bir farklılık oluşmayacağı düşünülebilir.

Masaüstü sanallaştırması durumunda sanal masaüstünün ve üzerinde bulunana dosyaların kime ait olacağı konusu tartışma yaratabilecek nitelikte olabilir. Sanal masaüstü dosyalarının tamamına sistem yöneticilerinin fiziksel erişimin mevcut olması, olası problemli içeriğin sahibinin tespiti açısından da problemlerin ortaya çıkmasına neden olabilecektir.

c. Lisanslama

Sunucularda çalışacak olan yazılımların sanal sunuculara uygun olacak şekilde yeniden lisanslanmaları gerekebilecektir. Örneğin, bazı uygulamalar fiziksel makine üzerinde mevcut soket sayısı baz alınarak lisanslanmaktadır. Bu ve benzeri lisanslama yöntemlerinin sanal ortamlar için yeterli olmayacağı açıktır. Bu durumun hukuki sorunlara yol açmasını önlemek amacı ile yazılım üreticilerinin biran önce sanal ortamları kapsayacak şekilde lisans düzenlemesine gitmeleri gerektiği de açıktır.

Masaüstü sanallaştırması yönteminde de benzer durumların ortaya çıkabileceği düşünülmektedir. Özellikle USB gibi aygıtlar aracılığı lisans kontrolü yapan yazılımların bu yöntemleri yeniden gözden geçirmeleri gerekecektir. Sanal masaüstlerinde ortak kullanıma açılacak olan bir USB aygıtı vasıtasıyla tek bir anahtar kullanılarak mevcut yapıdaki tüm masaüstlerinde aynı yazılımı çalıştırma olanağı ortaya çıkabilecektir.

BÖLÜM 4.

GÜVENLİK

Her geçen gün, e-devlet projelerinin de hayata geçirilmesi ile gerek kurumsal gerekse kişisel bilgilerin elektronik ortamlarda aktarılması, saklanması ve yetkiler dahilinde bu bilgilere erişimin gerekliliği bilgi güvenliğini oldukça önemli bir noktaya taşımıştır. Aynı zamanlarda bilişim teknolojilerindeki sanallaştırmaya olan yönelim de sanallaştırma ile bilgi güvenliği terimlerinin günümüzde sıklıkla beraber anılmaya başlamasına sebep olmuştur. Bilişim teknolojilerinde kullanılan yöntemler ve araçların çeşitliliği göz önüne alındığında, bilginin güvenliğini her aşamada sağlıyor olmak önemini artırmakta, bununla beraber sanallaştırma kavramının getirdikleri ile geleneksel güvenlik çözümlerine yeni bakış açıları da oluşmaya başlamaktadır.

Bilişim teknolojilerindeki çeşitli güvenlik ihtiyaçlarıyla bazı sanallaştırma çeşitleri ya da teknikleri yaratılmış olduğu gibi, bazı sanallaştırma çeşitlerinin de ne kadar güvenli ve güvenilir olduğu ya da kurumun bilgi güvenliği politikalarına uygunluğu sorgulanmaktadır. Önde gelen sanallaştırma çözümü üreticileri çeşitli güvenlik endişelerini gidermek amacıyla bu yönde geliştirmelere ağırlık vermekte ve dış çözümlerle bütünleşik yapılara olanak sağlar hale gelmektedir. Sanallaştırma planları yapmakta olan kurumların kolay yönetim ve tasarruf gibi getirileri hesaplarken, tüm yapılarını kapsayan yeni bir güvenlik politikası oluşturmanın ve ürünün güvenlik yönünden iyi incelenmesinin gerekliliğine dikkat etmelidirler.

4.1. Güvenlik için Sanallaştırma

Sanallaştırma, bilişim sistemlerinin güvenliğini artırmak için de kullanılabilecek bir yaklaşım olarak ortaya çıkabilmektedir. Bu bölümde, sanallaştırmanın hangi açılardan güvenliği artırabileceğine ilişkin temel konular ele alınmaya çalışılacaktır (ancak Bal Küpü ve Bal Küpü Ağları konusu 6.2.5'de sunulduğu için burada tekrarlanmamıştır):

a. Hızlı Erişim ve Müdahale Olanağı

Kötü niyetli bir kişinin bir kurumun sistemine sızarak bir sunucuyu ele geçirmesi ve işlev dışı bırakması yalnızca olasılıklardan biridir. Daha da kötüsü, sızılan sunucuya yerleştirilen bir zararlı uygulama ile sunucuya sonrasında da erişim sağlanabilmesi ya da bu sunucudan erişimin olduğu diğer sunucular hakkında bilgi

toplayarak bir sonraki hedef için de çalışılıyor olabilmesidir. Böyle bir durumun farkına varan sistem yöneticisi öncelikle kötü niyetli kişinin erişim yollarını kesecek ve bu sunucuyu, verdiği hizmette en az kesintiye sebep olacak şekilde zararlı uygulamadan arındıracaktır. Eğer yapılan saldırı sunucuyu hizmet veremeyecek duruma getirmiş veya zararlı içerikten kurtulmanın yolu yalnızca temiz bir kurulum ve hizmetin yeniden yapılandırılması ise bu karmaşık ve uzun zaman alacak bir süreç olabilir. Ancak söz konusu sunucu eğer sanallaştırılmış bir sunucu ise sistem yöneticisinin elinde hizmet sunucusunun yakın geçmişte alınmış temiz bir anlık kopyasının (snapshot) bulunması çok olasıdır. Ya da sanallaştırma olanakları ile bir sunucu kopyasının çıkarılması da çok kolay bir hal aldığından en azından yakın zamanda yedeklenmiş sistemin bir kopyası (clone) da sistem yöneticisinin elinde olacaktır. Bütün bunların da ötesinde, sanallaştırma ortamları ek bir fiziksel donanım gerektirmediğinden hizmet sunucularında yedekliliğin sağlanması için kolaylık getirmektedir. Bütün bu olanaklar sistem yöneticilerinin güvenlik sorunlarına hızlı ve rahat müdahale edebilmelerini sağlamaktadır.

Bu tip sorunları en hafif şekilde atlatabilmek için hizmete ilişkin verilerin sunucu üzerinde değil bir veri depolama alanında tutulması kolaylıklar getirecektir. Böylelikle ele geçirilmiş sunucu yerine bu sunucunun temiz bir kopyası devreye alındığında hizmete kalınan yerden devam edebilecek şekilde düzenlemelerin yapılması sağlanabilecektir. Sunucuların anlık kopyalarının sıklıkla alınması ve belirlenen daha seyrek periyotlarla sunucuların tam bir kopyasının çıkarılması, eğer olanak varsa sunucunun verdiği hizmetin yedekli olarak çalıştırılması bu tip riskler açısından önemlidir. Ancak burada dikkat edilmesi gereken konu, çıkarılmış olan kritik verilere sahip sunucu yedeklerine, bu yedekler gerçekte başka bir sanallaştırma ortamında çalıştırılabilir birer dosya olduklarından, bu dosyalara erişimlerin yetkiler dahilinde sağlanmış olmasıdır.

Sanallaştırma, bilişim teknolojilerinde karşımıza çıkan güvenlik ihtiyaçlarına birçok konuda yardımcı olmaktadır. Güvenilirliği kuşkulu bir uygulamanın gerçek bir ortamda çalıştırılmadan önce gerçek ortamı temsil eden bir sanal makinede çalıştırılarak incelenmesi ve güvenilirliği onaylandıktan sonra gerçek makinede çalıştırılması, günümüz teknolojileriyle bu sanal makinenin hazırlanması oldukça kolay olduğundan güvenlik açısından önemli bir katkı yaratmaktadır. Bunun da ötesinde bu tip bir uygulamanın işletim sistemi üzerinde sınırlı bir çalışma ortamında çalışmasını sağlayarak, çalıştırıldığı ortama ya da bu ortamdaki diğer uygulamalara erişiminin engellenmesi ya da sınırlanması tekniği kum havuzu oluşturma (sandboxing) olarak bilinir. Örneğin, antivirus ve güvenlik duvarı gibi bazı güvenlik

yazılımları ve hatta Microsoft Windows 2003 ve sonrası sunucu işletim sistemleri getirdikleri bazı teknolojiler (örneğin, Software Restriction Policies) ile sanal bir kum havuzu yaratarak yetkisiz kodların çalışmasını engelleyebilmektedir [23, 24, 25].

b. Uygulamaların Farklı Sanal Sunucularda Kullanılabilmesi

Güvenlik ile ilgili olarak sanallaştırmanın kullanılabileceği başka bir konu da uygulama ve servislerin ayrı sanal makinelere dağıtılarak güvenlik açıklarının birbirini etkilemesini engellemektir. Örneklendirmek gerekirse, aynı bilgisayarda (farklı fiziksel makinelere tedarik edilemediği için) iki ayrı web temelli uygulamanın ve e-posta servisinin beraber çalıştığını varsayalım. Bu durumda web yazılımlarından birisindeki bir güvenlik açığıyla program çalıştırma yeteneği kazanan bir saldırgan diğer web uygulamasının verilerini ve hatta sistemdeki bütün kullanıcıların e-postalarını ele geçirebilir. Fakat sistem kaynakları uygunsa bu bilgisayar üzerinde üç ayrı amaca yönelik üç sanal makine kurulduğunda ve her sanal makineye sadece bir uygulama ya da servis kurulduğunda güvenlik açıkları sadece uygulamanın çalıştığı sanal makine için geçerli olacak ve diğer uygulamaların verileri korunmuş olacaktır.

Sanallaştırma yazılımı sanal makinelerin farklı sanal adres uzaylarında ve farklı dosya sistemleri üzerinde çalışmasını sağlar. Böylelikle uygulamalar tamamen birbirinden ayrılmış bir ortamda, birbirinden haberdar dahi olmaksızın çalışır. Kum havuzu oluşturmak için dosya sistemi hapsi temelli (örneğin, chroot, jail vb.) yöntemler de vardır. Bu yöntemler de uygulama dosya sisteminde belli bir dizinin altına hapsedilir ve o dizini ana dosya sistemi olarak görür ve üst dizinlere erişimine izin verilmez. Bu yöntemlerde aynı işletim sistemi çekirdeği, çekirdek belleği ve sistem kaynakları kullanılmaktadır. Sanallaştırmada ise sanal sistemler birbirinden izole işletim sistemleridir, çekirdek düzeyinde farklı bellek uzayı ve farklı sistem kaynakları kullanırlar. Dolayısıyla elde edilen ayrıklaştırma daha kuvvetlidir. Ayrıca her sanal sistem başlı başına tüm bir işletim sistemi olduğu için uygulamaların işletim sistemi ve ortama ilişkin uyum talepleri daha düzgün olarak karşılanabilir. Örneğin, farklı işletim sistemi, kütüphane çeşit ve sürümlerini talep eden uygulamalar hapis ortamına göre çok daha kolay çalıştırılabilecektir.

Aynı sunucuda çalışan uygulamalara göre çok daha güvenli olsa da her uygulamaya ayrı sanal makine kurulması yüzde yüz güvenlik sağlayamaz. Sanal sistemler paylaştıkları kaynaklara göre birbirine karşı güvenlik tehdidi oluşturabilirler. Sanallaştırma yazılımında ciddi bir açık olması durumunda misafir sistemde kod çalıştırma, bellek alanlarına erişme, ağ paketlerine erişme gibi şekillerle diğer sanal

sistemlere saldırı gerçekleştirmek mümkün olabilir. Bu yüzden her türlü sanallaştırma uygulamasında sanallaştırma yazılımının güvenliği en üst düzeyde titizlik gösterilmesi gereken konudur. Sanallaştırma katmanına ilişkin güvenlik zayıflıkları en kısa zamanda giderilmelidir.

c.Sanal Özel Ağların Güvenliğe Katkısı

Sanal Özel Ağ (VPN) sunucuları güvensiz ağlar üzerinde güvenli iletişim tünelleri oluşturmak için kullanılmaktadır. Genel kullanım alanları arasında; kurum bölgeleri arası bağlantıları, çözüm ortakları ile iletişim veya gezgin istemcilerin yerel ağa güvenli bağlanabilmesi sayılabilmektedir. Sıkça karşılaşılan sanal özel ağ güvenlik açıkları arasında, sanal özel ağ sunucularında harici kimlik doğrulama sistemleri kullanılmaması, sunucunun yerel ağda bulunması sonucu yerel ağa doğrudan erişim, istemciler ile İnternet arasında iletişim izolasyonu olmaması ve zayıf şifreleme algoritmalarının seçilmesi sayılabilmektedir. Güvenlik açığı barındıran sanal özel ağa sızabilen bir saldırgan, kurum ağına doğrudan erişim sağlayabilmekte ve yerel kullanıcı haklarına sahip olabilmektedir.

Sanal özel ağ sunucuları kendilerine ayrılmış bir DMZ bölümü ve güvenlik duvarı aracılığıyla yerel ağa bağlanmalıdır. Böylece güvenlik duvarına gelen iletişim şifresiz olacak ve üzerinde erişim denetimi yapılabilecektir. Gezgin kullanıcıların bağlantısında ise sayısal sertifika veya tek kullanımlık parola gibi kimlik doğrulama yöntemleri kullanılmalıdır. Şifreleme amaçlı kullanılacak algoritma mutlak suretle günümüzde kolayca kırılamayan algoritmalar (3DES, AES vb.) arasından seçilmelidir. Kullanılacak istemci yazılımları, İnternet kullanımı ile sanal özel ağ kullanımı arasında yalıtım yapmalı ve istemcilerin İnternet'te farklı kaynaklara erişimini kısıtlamalıdır. Ayrıca uzak erişimlerde sahip olunan yetkiler, yerel ağda sahip olunan yetkilerden çok daha az olacak şekilde yapılandırılmalıdır.

VPN sistemi eş zamanlı olarak yüksek miktarda bağlantı yapılmasına uygun bir altyapı sağlamaktadır. Ancak, VPN istemci kullanımındaki hatalar, başarım düşüklüğü, kopma ve bağlanamama gibi sorunlara neden olabilir. VPN kullanımında aşağıdaki konulara özellikle dikkat edilmesi gerekmektedir [26].

- Her VPN sertifikası ile aynı anda sadece ve sadece bir adet bağlantı.
- VPN erişiminin yapılabilmesi için bulunulan ağdan UDP 1194 numaralı portun geliş ve gidiş trafiğine ve TCP 1194 portuna gidişin açılması ve gelecek yanıtlarında kabul edilmesini sağlayacak şekilde yerel güvenlik duvarı yapılandırılmalıdır.

- VPN sistemi kullanıcı PC'leri yerine tercihen yerel ağ geçidi üzerinde yapılandırılmalıdır.
- VPN sertifikaları kesinlikle korunmalı ve paylaşılmamalıdır.

d. Masaüstü Sanallaştırmanın Güvenliğe Katkısı

Özellikle kurumsal kullanımda en ciddi güvenlik sorunlarından birisi masaüstü bilgisayarların güvenliğini yönetmektir. Her kurumda kurumun büyüklüğüne göre yüzlere ve hatta binlere varan kişisel bilgisayar ve kullanıcı olabilir. Bu bilgisayarların dönemlik bakım, kurulum ve güvenlik denetimlerini yapmak özellikle dağınık fiziksel konumdaki bilgisayarlar için oldukça zordur. Kişisel kullanıcılar çoğu durumda hem bilgi hem de bilinç olarak bilgisayarlarındaki sorunları giderecek ve güvenlik politikalarını işletecek düzeyde olamazlar.

Bu durumlarda sanallaştırma, düzenli güncellenebilen, güvenlik aylarları yapılabilen, gözlenebilen masaüstü sistemleri yaratmak için kullanılabilir. Bu uygulamalarda kişilere ağdan yüklenen ve sanal masaüstü sistemine uzaktan bağlantı sağlamaktan başka bir yeteneği ve amacı olmayan ince-istemciler (thin-client) verilir. Kişilerin gerçek masaüstü sistemi bir sanal sistem bulutu üzerinde çalıştırılır. Böylelikle sistem yöneticileri masaüstlerinin güvenlik ayarlarını, güncelleme ve bakımlarını bulut üzerinde gerçekleştirir. Kullanıcılar bulut üzerinde belirlenen güvenlik politikalarının dışına çıkamazlar. Dışarıdan yönelecek her türlü tehdit buluttaki güvenlik araçları tarafından engellenebilir ve izlenebilir.

Masaüstü sanallaştırmasının güvenlik dışında da avantajları vardır:

- Kullanıcı masaüstünün fiziksel konumdan bağımsız hale gelmesi ve her yerden aynı masaüstüne erişimin mümkün olması;
- Sadece günün, ayın ve yılın belli dönemlerinde kullanılan masaüstü bilgisayarlar için fiziksel bilgisayar alınmayıp ortak kaynak ortamından kullanılması; böylece kaynakların verimli kullanılması;
- Her seferinde yüzlerce tam teçhizat bilgisayar almak yerine bulutta ölçeklendirme yapılarak sistemin zamanla gerek duyuldukça arttırılması ve yenilenmesi.

Öte yandan her türlü kullanıcı etkileşiminin ağ üzerinden buluta aktarılmasını sağlayabilmek için kurumun ağ altyapısının da kuvvetli olması gerekmektedir. Özellikle yerel ağ dışı uygulamalarda tepki hızlarının düşmemesi için ağ ve sistem boyutlandırmasının doğru yapılması ve tasarımın titizlikle yürütülmesi gereklidir. Ayrıca masaüstü sanallaştırması kullanıcıların hak ve özgürlüklerini de doğal olarak

kısıtlayacaktır. Kullanıcıların kendi işletim sistemlerini, yazılımlarını seçmesi ve kurması kısıtlanmış olacaktır. Dolayısıyla ev kullanıcısı gibi uygulamalardan çok bu kısıtlamaların özellikle istendiği kurumsal uygulamalarda güvenli sanallaştırma daha uygun olacaktır.

4.2. Olası Riskler ve Önlemler

Birçok bilişim yaklaşımının uygulanmasında olduğu gibi, sanallaştırmanın uygulanmasında güvenlik açısından özen gösterilmesi gereken noktalar bulunmaktadır:

a. Sanal Sunucuların Sayıca Artması ve Unutulabilmesi

Sanal sistemlerin başlıca handikaplarından biri yönetim zorluğudur. Eğer sanal sistemlerin yönetilmesi için herhangi bir yazılım kullanılmıyorsa, "*Acaba hangi fiziksel makine üzerinde hangi sanal sunucular vardı?*", "*X sanal sistemi acaba hangi fiziksel sunucudaydı?*" gibi sorular sıklıkla kafamızda belirecektir. Buna paralel olarak, unutulan sanal sunucuların işletim sistemi veya üzerinde koşan uygulamaların bakım işlemleri, işletim sistemi güncellemeleri, servis paketlerinin ve yamalarının takibi, zararlı yazılımlara karşı kullanılan programlara ilişkin güncellemeler, yönetimsel anlamda erişim zorluğu vb. sorunlar gelişmeye başlayabilecektir. Bu durumun sonucu olarak da, ilgili sanal sunucu, üzerinde koşan uygulamalar ve tutulan verilerle ilgili ciddi güvenlik açıkları oluşabilecektir. Özellikle, gereğinden çok sanal sunucunun kurulumu ile bu gibi sorunların çok daha fazla artacağı da açıktır.

Sanal sistemlerin yönetimini kolaylaştıracak programlar kullanılmadığında sistemlerde herhangi bir sorun olduğunda gerçekten sorunu oluşturan sisteme erişebilmek oldukça vakit alacak ve o sanal sunucu üzerinde verilen hizmetlerin kesinti süreleri artacaktır. Eğer bu sistemler üzerinde kilit hizmetler veriliyor ise hizmetin kesilmesi ile hizmeti alan kişi/kişiler/bayi/kurum gibi yerlerde mağduriyetler oluşmaya başlayacak, işlemler aksayacak, aynı zamanda kurum adına saygınlık kayıpları da gündeme gelecektir.

b. Çok Katmanlı Yapı

Sanallaştırılan bir sistemin idame edilmesi ve bakım işi sanallaştırmanın kullanılmadığı sisteme göre yazılım bakımından artacaktır. Çünkü, sanallaştırılmamış sistemlerle kıyaslandığında, sistem üzerinde koşan ve yönetilmesi gereken bir fazla katman bulunacaktır. Ev sahibi sistem için gereken yönetime ek olarak sanal sistemin yönetimi ve bu ikisinin etkileşimini sağlayan

sanallaştırma katmanının yönetimi gerekecektir. Ancak burada unutulmamalıdır ki, sanal sistem için donanımsal bakım oldukça kolaylaşacaktır ve eğer sanal sistemler bir ev sahibi sistemi paylaşıyorlar ise donanım yönetimi ev sahibi sistem için yapıldığında sanal sistem sayısı kadar sanallaştırma kullanılmayan sistemin yönetimine göre kolay olabilir.

Sanallaştırma sistemi, ev sahibi sistem ve sanal sistemin işletim sisteminin seçiminde sistemlerin uyumu göz önünde bulundurulmalıdır. Örneğin Xen, pek çok Linux dağıtımında ayrıca elle kurulum gerektirirken, openSUSE tarafından resmi olarak desteklenmektedir. Dolayısıyla Xen kullanılacaksa ev sahibi sistem olarak openSUSE seçmekte fayda vardır. Benzer şekilde ev sahibi sistemin seçiminde donanım ile tam uyumluluk açısından donanım üreticilerinin sürücü için destek sağladığı işletim sistemlerinden birini tercih etmek daha uygun olmaktadır.

c. Tek Hata Noktası

Birçok sanal sistemin tek gerçek sistem üzerinde konuşlandırılmasının pek çok getirisi bulunduğu bilinmektedir. Ancak bu yapıdaki bir sistemin en büyük götürüsü gerçek sistemde oluşabilecek bir sorunun tüm sanal sistemleri beraberinde etkilemesidir. Eğer gerçek sisteme bir BIOS virüsü bulaşırsa, sistemin donanımsal bir parçası arızalanırsa, sanallaştırma yazılımında bir sorun olursa veya sisteme donanımı ya da sanallaştırma yazılımını hedefleyen bir saldırı yapılırsa sistem üzerindeki tüm sanal sistemler de bozulacaktır. Gerçek sistemde olan tüm hatalar bütün sanal makinelere yansıyacaktır. Bunun önlenmesi için anti virüs tarzı zararlı yazılım engelleyici güncel programların barındırılması ve çalışan gerçek sistemin durumunun çok iyi gözlenmesi gerekmektedir. Ayrıca, yedek sistemlerin tutulması da önerilebilir. Böyle bir problemle karşılaşıldığında sabit disklerin yedek makineye taşınması hızlı bir şekilde tüm sistemi ayağa kaldırabilecektir.

d. Sanal Ağların Rolü

Ağ topolojileri yaratılırken farklı güvenlik seviyelerine farklı ağ bölümlemeleri yapılmakta ve bu bölümler arası geçişlerin güvenlik duvarı ve saldırı tespit sistemleri tarafından izlenmesi ile müdahaleleri sağlanmaktadır. Benzer şekilde zararlı içeriğe karşı taramaların da yapılması birçok kurum tarafından mevcutta bulunan uygulamalardır. Bütün bu güvenlik önlemlerinin sanallaştırma planları yapılırken dahil edilmesi kurum açısından çok dikkat edilmesi gereken bir konu olmalıdır. Tek bir fiziksel makine üzerinde farklı güvenlik bölümlerine ait sunucuların bulunması ve bu sunucular arası trafiğin izlenemiyor olması, bu kurumda büyük güvenlik açıkları olduğu anlamına gelecektir. Ya da kurumsal sanallaştırma ürünlerinde bulunan bir

özellik olan sanal makinenin fiziksel makine değiştirmesi (live migration) işlemi sırasında akan trafiğin şifreli olmaması sebebiyle içeriğinin elde edilebilmesi de, her ne kadar bu işlem adanmış bir ağ arabirimi üzerinden yapılsa bile, bir güvenlik açığı olarak sayılabilir. Kurumun planlarını yaparken farklı güvenlik bölümlerindeki sunucular için farklı fiziksel ortamlar ayırması bir önlem olarak düşünülebilir. Bununla beraber farklı ağ bölümlerinde bulunan sanal makinelerin diğer ağ bölümlerine geçişi, geleneksel olarak yapıldığı gibi bu trafiğin izlenebileceği ağ geçitlerine yönlendirilmelidir. Önde gelen sanallaştırma çözümü üreticilerinin bu tip güvenlik açıklarının önüne geçebilmek amacıyla geliştirmiş olduğu teknolojiler incelenmeli ve kurumun diğer güvenlik ürünleri ile bütünleşik çalışabilmeleri istenmelidir. Örneğin, VMware'in geliştirmekte olduğu VMsafe ürünü harici güvenlik ürünlerinin kontrol ve müdahalelerine olanak tanıyan bir güvenlik katmanı oluşturabilmekte, sanal ortamlarda güvenlik ürünü üreticilerinin çözümler geliştirebilmesi amacıyla uygulama yazılımı arabirimi paylaşımı sağlayan bir çözüm sunmaktadır. Bu sayede fiziksel sunucular ile çalışma yönteminde her sunucuya ayrı bir anti-virüs uygulaması yüklenmesi yerine bu uygulama arabirimi sayesinde merkezi bir virüs taramasının da yolu açılabilmekte olup aynı zamanda sanal ağlar üzerinde de izleme ve kontrol de sağlanabilmektedir [27, 28].

e. Sanallaştırma Yönetim Aracının Rolü

Sanallaştırma aracında bir güvenlik açığı olması demek bütün sanallaştırılmış sistemlerin artık güvensiz olduğu anlamına gelir. Bu açıkları ve zafiyetleri önlemek için anti-virüs yazılımı, atak önleme sistemleri, güvenlik duvarları ve benzeri güvenlik sistemleri kullanılmalıdır. Bunun yanında alt tarafta çalışan işletim sisteminin ve sanallaştırma yazılımının da tüm güncellemeleri zamanında yapılmalıdır. Tek Hata Noktası maddesinde belirtildiği gibi gerçek sistem ve gerçek sistemin işletim sistemin başına gelecek herhangi bir şey tüm sanal sistemleri etkileyeceği için gerekli önlemler alınmalıdır.

Bu durumu bir örnekle açıklayalım. ESX için kullanılan sanal makine monitörü tüm sürücüleri içinde tuttuğu için, üzerinde çalışan tüm sanal makineler ortak sürücü kullanmaktadır. Yani her sanal makinenin kendi özel sürücüsü yoktur. Diğer bir ifade ile, ESX sunucusu üzerinde çalışan fiziksel Ethernet kartının sürücüsü sanal makine monitörü içinde durmaktadır. Bu durumda riskin büyüklüğü ortaya çıkmaktadır. Her sanal makine sürücüye doğrudan erişebildiği için değişiklik yapma şansı olabilir. Kötü niyetli bir kişi herhangi bir sanal makine üzerinden yeni bir sürücü ithal edip, bunu sanal makine monitörü üzerine gönderebilir. Bu sürücü özel olarak tasarlanmış bir ağ sürücüsü olabilir ve sanal makine monitörü içine transfer

edilen bu sürücü ile diğer sanal makinelerin ağ trafiği dinlenebilir. Ek olarak özel tasarlanmış bir klavye sürücüsü ithal edilerek basılan tuşlar yakalanabilir.

Bir diğer örnek olarak, sanal makinelerden birisi üzerinde sürücüye bulaşan bir virüs, bu sürücüyü kullanan diğer sanal makineleri de etkileyebilir gibi çok farklı senaryolar üretmek mümkündür. Bunun nedeni ise yekpare yapıdaki sanal makine monitörü kontrolündeki sanal sunucuların, sürücü tarafında sanal makine monitörüne doğrudan erişebiliyor olmasıdır.

Hyper-V tarafında ise sürücüler işletim sistemlerinin içinde durduğu ve temel girdi-çıktı işlemleri VSP/VSC-VMBus üzerinden gerçekleştiği için, yekpare yapıdaki güvenlik riskleri bu mimaride söz konusu değildir. Sanal makinelerin sanal makine monitörüne müdahale etme şansları yoktur. Herhangi bir sanal makinenin başına bir problem geldiğinde, bu sorun sadece yerel olarak kendisini etkilemektedir.

Sanallaştırma teknolojisinin göreceli olarak yeni olması bu tür platformlardaki güvenlik saldırıları şimdilik düşük seviyede tutsa da, önümüzdeki dönemde çok çeşitli saldırı türlerinin yaygınlaşması beklenmektedir. Gerek mevcut saldırı türlerinin (servis kesintisi – DoS, bellek taşması, Truva atı, vb.) sanal sunuculara yönelik geliştirilmiş sürümleri, gerekse tamamen sanal sunucuları ve sanal makine monitörlerini hedef alan yeni saldırı tipleri sanal yazılımların artmasına paralel olarak yaygınlaşmaktadır.

Yukarıda da belirtildiği gibi sanal makine saldırılarının temel hedefi bir sanal sunucuyu ele geçirmek ve sonrasında sanal makine monitörünün kontrolünü sağlayarak diğer sanal sunuculara doğru yayılmaktır. Bu kapsamda, her bir sanal sunucunun güvenlik ihtiyaçlarını güvenlik politikaları çerçevesinde detaylı olarak karşılamak, sunucu bölümlemelerini ve izolasyonunu eldeki tüm araçları etkin bir şekilde kullanarak gerçekleştirmek ve elbette bu hususların doğru yönetilmesini sağlamak gerekmektedir. Bu amaçla, sanal sistemler için geliştirilmiş araçların kullanılması (sanal sunucular arasında veri iletişimin izlenerek şüpheli trafiğin raporlanması, zararlı kodların belirlenmesi gibi işlevleri sağlayan güvenlik araçları) geleneksel güvenlik araçlarına göre daha güvenli platform oluşturmayı sağlayacaktır. Ek olarak, sayısal imza, donanım tabanlı sertifikasyon, gömülü şifreleme gibi koruma teknolojileri ile sanal bileşenler arasında veri iletişimi güvenli hale getirilebilmektedir.

Sanal bir ortamın karmaşık ve dinamik yapısı her geçen gün yeni saldırı türlerinin ve zafiyetlerin ortaya çıkmasını sağlamaktadır. Geleneksel güvenlik önlemlerinin yetersiz kalması nedeniyle yeni araçlara ihtiyaç duyulmaktadır. Ancak

halen gelişmekte olan ve geçen zamanla birlikte olgunlaşan bilgi birikimi ile sanal sistem üreticileri ihtiyaç olan güvenlik ürünlerini geliştirmeye devam etmektedirler.

f. Fiziksel Sistemin Paylaşılmasının Rolü

Aynı sanallaştırma ortamında ve aynı sanal anahtar üzerine bağlanmış sanal makinelerin birbirlerinin trafiğini izleyebilme ve böylelikle gizli bilgileri edinebilme riski bulunmaktadır. Bu riskin önüne geçmek için sanallaştırma üreticileri sanal anahtarların gelişigüzel (promiscuous) çalışma modunu ön tanımlı olarak kapalı tutmaktadır. Bu çalışma modu açık olduğu durumda sanal anahtar üzerinden geçen tüm trafik bu sanal anahtar üzerindeki tüm sunucular tarafından izlenebilir olmaktadır. Bu modun kapalı olması ile yetinmeyerek sanal sunucular ile sanallaştırma ortamı arasındaki iletişimin IPSEC ya da güçlü bir şifreleme yöntemi ile yapılması en güvenilir yöntem olacaktır [28, 29].

g. Sanal Sistem Yedeklerinin Alınması ve Korunması

Fiziksel sistemlerde olduğu gibi, sanal sistemlerde de veriler çok çeşitli şekillerde saklanabilirler. Bunların dışında, sanal sistemlerin sabit disklerinin taşıyıcı sistemin dosya sisteminde bir dosya olabilmesi farklı bir yedekleme yöntemini de kolaylıkla uygulanabilir ve popüler hale getirmiştir. Bu yöntem, sanal sistemin kısa bir süre duraklatılarak sistemin çalışması ile ilgili bilgilerin, sabit diski içeren dosya ile beraber kopyalanmasıdır. Sistemin yeniden başlatılabilmesi için her türlü veri saklandığından, bu yöntemde geri yükleme de çok hızlı bir şekilde gerçekleştirilebilmektedir.

Normal bir sistemin yedeklenmesinde, gereken dosyalardan fazlasının yedekleme yapılan ortama aktarılmaması mümkündür ve tercih edilir. Sanal sistemin yedeğinin çalışma anı verileri ve sabit diski içeren dosyanın içeriğinin kopyalanması yöntemiyle alınması durumunda ise, yedekleme dosyalarının içeriği incelenerek sanal makinenin tüm yapılandırması, üzerinde çalışan bütün programların tüm detayları ve saklanmayıp sadece çalışma anında hafızada bulundurularak güvenlik altına alınmaya çalışılan tüm veriler belirlenebilir.

Bu nedenle, bahsedilen yöntemle alınan yedeklerin mutlaka kuvvetli bir şifrelemeden geçirilip saklanması gerekir. Ayrıca ek önlemler olarak sanal makineden veya çalıştığı sistemden kolayca erişilemeyecek bir ortamda, fiziksel güvenliği de sağlanarak saklanmasında fayda vardır. Yedeklerin şifrelenmesi işlemi çok işlemci zamanı aldığından taşıyıcı sistemde yapılması tercih edilmeyeceğinden, yedeğin şifreleneceği sisteme de güvenli bir bağlantı ile aktarılması gerektiği unutulmamalıdır.

h. Sanal Sistemlere Yönelik Güvenlik Tehditleri

Sanallaştırma sistemlerinde, sanallaştırmayı sağlayan yazılım katmanı ve zaman zaman kullanılan donanım desteği, hem taşıyıcı sistem hem de sanal makineler tarafından erişilebilir ve görece karmaşık sistemler olduğundan, çeşitli saldırılara açıktır. Bu saldırılara karşı taşıyıcı sistem üzerinde alınabilecek önlemlerden bazılar yazılım kümesinin minimal tutulması, SELinux (Güvenliği Yükseltilmiş Linux – Security Enchanced Linux) dağıtımları gibi, detaylı güvenlik politikasının belirlenmesi ve uygulanması sağlayan bir işletim sisteminin kullanılması ve ağ bağlantısının güvenliğini sağlanmasıdır.

Sanal sunucuların kendilerinin de güvenlik tehdidi altında bulunabilecekleri göz önüne alınmalı ve taşıyıcı fiziksel sistemlerde alınanlara benzer önlemlerin sanal sunucularda da kullanılmasına çalışılmalıdır. Bu önlemler arasında sanal sistemin İnternet'e erişimine izin verilmemesi, USB portları üzerinden sanal sistemlere erişilememesi gibi önlemler sayılabilir.

i. Kullanılan Donanımın Güvenlik Üzerine Etkileri

Raporun ilk bölümlerinde de detaylı olarak bahsedildiği gibi, sanallaştırmada donanım kullanımlarında iki yöntem öne çıkmaktadır: Fiziksel donanımı sanal makine üzerindeymiş gibi adresleyerek doğrudan kullanımı sağlayan tam sanallaştırma ve gerçekte var olmayan sistem kaynağını ve donanımı sanki sanal makine üzerinde mevcutmuş gibi kullanılabilen işletim sistemi destekli sanallaştırma. Ancak, gerçekte var olmayan aygıtların sisteme tanıtılması onların ana sistem üzerinde adreslenmesini gerektirmektedir. Bahsedilen iki sanallaştırma tipinin de aygıt ve kaynak kullanımları birbirlerinden farklıdır. Bu farklılıklar güvenlikle ilgili olarak farklı sonuçlar doğurmaktadır:

- **Tam sanallaştırmada aygıt güvenliği:** Tam sanallaştırmada, aygıt sanal makinelerden birine tahsis edilerek kullanılabilir. Bu durumda diğer çekirdeklerin bu aygıtlara erişimi sanal sunucu tarafından engellenir. Bu durum ana sunucu üzerindeki bir saldırgan tarafından da kesilemez. Çünkü bu kaynak, sanal çekirdeğin yüklenmesi sırasında ana çekirdek üzerinde rezerve kaynak olarak işaretlenir ve süreç yalıtımı işlemi ile diğer çekirdeklerin ve süreçlerin erişimi engellenir. Süreç ana kaynak üzerinde kilitli olduğundan bunun bir saldırgan tarafından açılması mümkün değildir. Bu işlemin gerçekleşebilmesi için çekirdeğin aygıtla ilişkisini kopartması gerekmektedir. Bu aygıt ana sistem aygıtlarından biri ise bunun yapılabilmesinin tek yolu çekirdeğin durdurulmasıdır.

Çekirdeğin durdurulması işlemi ana sistemden yapılabilmektedir. Ancak bu, sanal işletim sisteminin de durması anlamına gelir ve sanal makinenin kapatılması sonucunu doğurur. Bu durum, sistem yöneticisi yetkisi gerektirmektedir. Sistem yöneticisi haklarıyla bu işlemin yerine getirilmesi sanallaştırma ile ilgili bir güvenlik sorunu değildir.

- **İşletim Sistemi destekli sanallaştırma aygıt güvenliği:** İşletim Sistemi destekli sanallaştırmada tam sanallaştırmadan farklı olarak mevcut olmayan aygıtlar için de sanal bir kaynak oluşturup kullandırmak mümkündür. Örneğin, belleğinizi olduğundan büyük göstermek ya da olmayan bir aygıt kaynağı yaratarak çekirdekle ilişkilendirmek mümkün olabilmektedir. Bu sebeple kaynak kullanımlarında ana sistem üzerinden olmayan kaynak yönlendirmeleri ile sanal sistemlerdeki kaynaklar yanıltıcı olabilmektedir.

Bu kaynaklar, tam sanallaştırmadan biraz daha farklı olarak ana çekirdek üzerinde rezerve edilmezler. Sadece adresleri konuk sistem çekirdeğine olduğundan farklı iletir. Bu durumda çekirdeğin üzerindeki işlemci kimliği de dahil olmak üzere birçok veri olduğundan farklı gösterilebilir. Diğer taraftan, bu işlemi engellemek de mümkündür. Bu önlem konuk sistem çekirdeğinin bütünlüğünün kendi içerisindeki kontrolü ile sağlanmaktadır. Ek olarak, konuk sistem çekirdeği üzerindeki kontrol kaynak kodu üzerinden ya da makine dili üzerinden değiştirilebildiği ve tıpkı sanallaştırma yapılmamış işletim sistemlerindeki çekirdek saldırıları gerçekleştirilebildiği unutulmamalıdır.

Ortak bellek kullanımları kısmında bu konu ile ilgili daha detaylı bilgi sunulmaktadır.

j. Kurumun Güvenlik Politikası ile Uyum

Hassas verilerini koruması bir kurum için hayati öneme sahip olabilir. Kurumlarımızda bu tarz bilgilere erişimi olan pek çok çalışan bulunmaktadır. Bu kişiler kurumun kendilerine sağladığı masaüstü ya da dizüstü bilgisayarlarda bu tür bilgileri yerel olarak tutarlar. Çalınan bir dizüstü bilgisayarı ya da sabit diski bozulan bir masaüstü bilgisayarı kurum için bilginin istenmeyen ellere düşmesi ya da tamamen yitirilmesi sonucunu ortaya çıkarabilir.

Sanallaştırma, sunduğu çözümlerle kurumlardaki tüm verilerin merkezi olarak saklanmasına olanak tanır. Kurum bütün uygulamalarını ve bilgilerini tek bir merkezi sunucuda tutup burada sakladığı verilere kullanıcıların uzaktan erişmesini sağlayabilir. Kullanıcılar ince istemciler aracılığıyla yerel hiçbir veri tutmadan bütün

işlerini uzaktaki bir sunucu üzerinde tamamlayıp veriyi de her zaman kurumun iyi korunan sunucularında bırakabilirler. Böylece hassas bilgilerin yalnızca tek bir yerde tutulması ve güvenlik önlemlerinin bu merkezde yoğunlaştırılması sağlanır. Masaüstü sanallaştırma böylece kurumlara bilgi güvenliğini daha rahat sağlama seçeneği sunar.

Ancak, sanal sistemlerin güvenliğini sağlamak için izlenmesi gereken yöntem, sanal sistemlere ilişkin güvenlik önlemlerinin kurumun güvenlik politikaları ile uyumlu olmasının sağlanması ve kurumun güvenlik süreçlerinin sanal makinelerin yöneticileri aracılığıyla bütün sanal makinelerde istisnasız ve sürekli uygulanmasının sağlanmasıdır. Bu nedenle kurum bilişim güvenlik süreçlerinin oluşturulmuş ve uygulanıyor olması sanallaştırmaya güvenli geçişin önemli ön koşullarındandır.

BÖLÜM 5.

SÜREÇLER VE YÖNTEMLER

Sanallaştırma ile sağlanmak istenen faydalara ulaşabilmek için çalışmalarda izlenmesi gereken süreçler ve yöntemleri bu bölümde incelenecektir. Yönetilebilirlik, ölçeklenebilirlik, esneklik, güvenlik ve ihtiyaçlara hızlı cevap vermek gibi pek çok fayda sağlaması beklenilen bir sanallaştırma çalışmasının bu beklentilere gerçekten cevap verebilmesi için her şeyden önce önemli bir analiz ve planlama süreci gerekmektedir. Sonra da kullanılacak olan sanallaştırma teknolojisine bağlı olarak farklı yöntemler uygulanmaktadır. Bu bölümde tüm bu konularla ilgili detaylı bilgi yer almaktadır.

5.1. Sanallaştırmaya Geçiş Aşamaları

Sanallaştırmaya geçiş süreci, var olan bir fiziksel sunucu kümesinden diğerine geçişe benzer bir süreçtir. Hizmetlerin devamının sağlanması gerektiğinden, aktarım süreci kapsamlı bir şekilde planlanmalı ve yönetilmelidir.

Sanallaştırmaya geçiş süreci başlıca üç temel adımdan oluşur (Şekil 5.1). Sanallaştırmanın, BİB'nin işletme ve yönetim yöntemleri açısından bazı farklılıklar doğurduğu bilinmektedir. Geçiş süreci, bu farklılıklar göz önüne alınarak dikkatle yönetilmelidir.

Sanallaştırılan sistemlerin yönetiminde dikkat edilmesi gereken en önemli noktalardan biri kaynak paylaşımıdır. Kaynakların ortak kullanımı yoluyla kullanılırlığın arttırılması sanallaştırmanın amaçlarından olmakla beraber, dikkatli yönetilmemesi halinde yüklü sunucuların yükü daha az ancak önemli diğer sunucuların başarımını olumsuz etkilemesine neden olabilir.

Sanallaştırma sunucularında ortaya çıkabilecek herhangi bir problem halinde, problemli sunucu üzerindeki sanallaştırılmış sunucuları diğer sanallaştırma sunucularına aktararak devamlılığın sağlanması gerekecektir. Gereken sanallaştırma sunucularının sayısı ve kapasiteleri hesaplanırken devamlılık için gerekecek kapasite fazlasının da göz önüne alınması gerekir.

Şekil 5.1: Sanallaştırmaya Geçiş Aşamaları

5.1.1. Sanallaştırmaya Hazırlık

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

- **Mevcut kurumsal bilişim altyapısı envanterinin çıkarılması:** Kurum/şirket öncelikli olarak sanallaştırmanın gerekli olup olmadığına karar vermesi gerekir. Bilişim altyapısına yakın zamanda yatırım yapılmış ise ve bu yatırımda kurum ihtiyacını karşılanıyorsa sanallaştırmanın fayda ve maliyet açısından bir getirisi olmayacaktır. Mevcut durumdaki kurumsal envanterin sanallaştırma altyapısına uygunluğu araştırılmalıdır. Bu altyapı uygunsa eksik kalan noktalar üzerine sanallaştırma tasarımı yapılıp projeye devam edilmesi uygun olacaktır. Mevcut donanım envanterin yenilenmesi ihtiyacının doğduğu noktada sanallaştırma teknolojilerine uygun tasarımın öngörülerek çalışmaların yapılması anlam kazanacaktır.
- **Kapasite planlama:** Kurumsal ölçeğin ne olduğuna bakılmaksızın sanallaştırma teknolojilerine yatırım öncesi mutlaka gerekli teknolojik araçlar kullanılarak bir kapasite planlaması yapılmalıdır. Kapasite planlamaya yönelik olarak seçilecek sanallaştırma teknolojisi çözüm üreticilerinin veya hizmet sağlayıcıların kapasite planlama servislerinin olup olmadığı ve bu noktada ne kadar tecrübeye sahip olduklarının araştırılması gerekmektedir. Kapasite planlama araçları yapılan çalışma sonrasında işlemci, hafıza, disk ve iletişim ağı altyapı ihtiyacını ortaya çıkaracaktır. Kapasite planlama hizmeti konusunda birçok üreticinin hazır yazılım ürünleri mevcut olduğu gibi, bu konuda 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.
- **Planlama sonrası gerçekleştirilecek yeni yatırım:** Mevcut altyapının yeterliliğinin değerlendirilmesi ve kapasite planlama çalışmaları sonucunda yeni yatırım ihtiyacı doğabilir. Bu ihtiyacın belirlenmesi hususunda sanallaştırma yazılımı, sanal ortam yönetim yazılımı, sunucu,

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.

- **Toplam fayda maliyet analizi:** Sanallaştırma teknolojisine geçiş kararı öncesi mutlaka bir toplam fayda ve maliyet analizi yapılmalıdır. Mevcut altyapı ve yeni ihtiyaçlar göz önüne alınarak bu kapsamda bir değerlendirme gerçekleştirilmelidir. Sunucu, disk, iletişim ağı, işletim sistemi ve enerji maliyetlerinde ne kadar kazanç sağlandığının yapılan analizlerde ayrıntılı olarak incelenmesi gerekmektedir.

Teknik açıdan ise, sanallaştırma projesine başlamadan önce ilk olarak mutlaka kapasite planlaması yapılmalıdır. Kapasite planlama raporu sonucu tüm teknik ekipçe değerlendirilmelidir. Sanallaştırma çalışmalarında ilgili teknik birimlerden (sistem, iletişim ağı, yedekleme, disk yönetim birimleri) en az bir personelin aktif katılımının sağlanması gerekir. Sanallaştırma projesinin teknik personel arasında kabul görmesi ve desteklenmesi sorun olmaktan çıkacaktır. Harici disk sisteminde lisanslamaya mutlaka dikkat edilmelidir. Çünkü disk sistemi sanallaştırma projesinin en önemli parametrelerden birisidir. Dolayısıyla lisanslamasından (asgari kaynak kullanımı – thin provisioning), tekil yedekleme – deduplication, replikasyon, kapasite bağımlı ve kapasite bağımsız gibi) ön belleğe kadar mutlaka iyi tarif edilmesi gerekir. Sanallaştırma yazılımın üzerinde koşacağı sunucu ve bileşenlerinin mutlaka sanallaştırma teknolojisini desteklemesi gerekir. Kurumun yedekleme alt yapısı değerlendirilmeli, eğer yetersiz ise bu husus proje kapsamında çözülmelidir. Bu konuda da lisanslama unutulmamalıdır. Proje sonucunda gelecek tüm ürünler ile ilgili teknik personelin eğitim programına (sanallaştırma yazılımı, disk yönetimi, yedekleme yazılımı gibi) tabii tutulması gereklidir. Projede geçen donanım ve yazılım ürünleri için iyi tarif edilmiş destek mekanizması sonradan yaşanılacak sorunlara çabuk çözüm bulunması için önem arz edecektir. Proje boyunca her aşamasıyla ilgilenecek en az bir personel, proje lideri olarak belirlenmelidir. Sanallaştırma projesi başından sonuna kadar mutlaka belgelendirilmeli ve sistem odasında kullanılan tüm donanımlar (donanım birimleri ve kablolama altyapısı gibi), sanayi ölçütlerinde etiketlenmelidir. Kablolama gruplarına göre farklı renkler kullanılmalı; iletişim cihazları (omurga, yönlendirici vb.) için kullanılan kabinlerde ısınma sorunun oluşmaması için dikkatle uygulanmalıdır. Fiber kablolama olduğunda, mutlaka dış etkenlere karşı fiziksel güvenlik önlemlerinin alınması gerektiğinden, kapaklar kapatıldığında hava alınamaz hale

gelinmekte ve cihazların başarımı düşmektedir. Bu kabinlerde cam kapak yerine delikli kapak kullanılmasının sağlanması önerilmektedir. İyi yönetilmeyen sanal ortamın, kısa zamanda sanal makine çöplüğüne dönüşmesi kaçınılmaz olacaktır. Sanal ortamın güvenliğini (fiziksel bilgisayar ve sanal makine) sağlamak için proje kapsamında mutlaka çözüm sağlanmalıdır. Tüm yumurtalar bir sepete konulacağı için sepetin güvenliğini sağlamak son derece kritik hale gelmektedir. Mevcut altyapının sanallaştırma projesini kaldıracak alt yapıda olup olmadığı dikkat edilmelidir (örneğin, enerji altyapısı, klima alt yapısı).

Gerçekleştirilmesi gereken çalışmalara ve yerine getirilmesi gereken rollere baktığımızda, şu noktaların öne çıktığını görmekteyiz: Ortaya çıkan kapasite planlama raporları neticesinde yapılacak yatırımın sistem, iletişim ağı ve yazılım geliştirme yöneticileri tarafından değerlendirilmesi gerekir. Kapasite planlama raporları sonrasında ortaya çıkan ihtiyacın ilgili birimlerce detaylı bir şekilde incelenmesi ve bu kapsamda ihtiyaç duyulan ürünlerin teknik özelliklerine karar verilmesi gerekmektedir. Sanallaştırma alt yapısı hazırlanırken ilgili teknik birimlerin rol ve sorumluluk alanlarına göre ihtiyaçları belirlenir. Teknik 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.

Sanallaştırmaya hazırlık için iş kalemlerini çıkarılırken aşağıda sıralanan hususlara, maliyet kalemleri olarak, özellikle dikkat edilmesi gerekir:

- **Kapasite Planlama Raporu:** Kapasite planlama çalışmaları için bu konuda çözüm odaklı rapor üretecek çeşitli yazılım araçları mevcuttur. Bu yazılım araçları kapasite planlama esnasında kullanılmak üzere bir maliyet oluşturabilir. Ayrıca kapasite planlama bu konuda çözüm sağlayan firmalardan danışmanlık hizmeti şeklinde temin edilebilir.
- **Sanallaştırma çözümünün alt yapıya uygunluğunun tespitine yönelik test çalışmaları:** Sanallaştırma çalışmalarının hazırlık aşamasında tercih edilecek ürünlerin mutlak suretle test edilmesi gerekmektedir. Bu kapsamda yapılacak olan testler için bir yatırım gerekebilir. Test çalışmaları için mevcut altyapıda ki ürünler uygun değilse bir test platformu yatırımı gündeme gelebilir. Ayrıca bu testlerin gerçekleştirilmesi için küçük çaplı bir hizmet ihtiyacı ortaya çıkabilir.

5.1.2. Sanallaştırmanın Etkinleştirilmesi

Sanallaştırma hazırlık çalışmaları sonrasında gerçekleştirilecek yatırıma karar verildikten sonra üst yönetimin bir planlama ve organizasyon yapması gerekmektedir. Test çalışmaları sonrasında raporlar değerlendirilmiş ve sanallaştırmanın etkinleştirilmesine karar verilmişse, bu konuda bütçe değerlendirmesi gerçekleştirilmelidir. Kapasite planlama raporu göz önüne alınarak ilgili teknik birimlere gerekli görev dağılımı yapılır. İhtiyaç duyulması halinde insan kaynağı yatırımı gerekip gerekmediği konusunda bir değerlendirme yapılmalıdır.

Sanallaştırma teknolojisinin etkinleştirilmesi çalışmalarında kurumun tüm bilişim hizmetlerini sunan birimlerine çeşitli görevler düşmektedir. Bu birimlerin birbirleriyle koordineli olarak çalışması gerekmektedir. Kurumda sistem yöneticileri kendilerini ilgilendiren sunucu, işletim sistemleri, disk ortamı ve sanallaştırma yazılımlarının kurulum çalışmaları gerçekleştirmelidir. Ağ yöneticileri bu platformun üzerinde çalışacağı ağ topolojisini belirlemeli ve ilgili donanım ve yazılımlar üzerinde gerekli konfigürasyonları yapmaları gerekmektedir. Tüm ağ aktif cihazlarının sorunsuz bir şekilde çalışıp çalışmadığının testleri mutlaka yapılmalıdır. Yazılım geliştirme birimleri sanal ortama geçiş sonrasında uygulama ortamlarında herhangi bir değişiklik yapılması gerektiği bir durum söz konusu olursa bu çalışmaları başlatmalıdırlar. Bu çalışmaların tamamında mevcut suretle belgelendirmelerin eksiksiz bir şekilde oluşturulması oldukça önem arz etmektedir.

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 ortamında ki 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.

Diğer taraftan, sanallaştırma iş kalemlerini çıkarırken aşağıda sıralanan ana maliyet kalemlerine dikkat edilmesi gerekmektedir.

- **Sanallaştırma yazılımı:** Sanallaştırma teknolojisine geçiş için olmazsa olmazlardan biri de bu teknolojinin altyapısını sağlayacak olan sanallaştırma yazılımıdır. Tercih edilecek sanallaştırma yazılımının, proje kapsamında kullanılacak yazılım ve donanım ürünleriyle uyumlu olup olmadığının incelenmesi oldukça önemlidir. Hangi donanım, yazılım ve işletim sistemi mimarilerini desteklediği araştırılmalıdır. Sanallaştırma yazılımının, sanal ortama taşınması planlanan mevcut servis ve uygulamaları destekleyip desteklemediği konusunda gerekli incelemelerin yapılması kritik önem taşımaktadır.

  Sanallaştırma yazılımlarının lisanslama modellerinin dikkatlice araştırılması ve kapasite planlama çalışması sonucunda çıkan ihtiyacı karşılayıp karşılamadığı tespit edilmelidir. Bu kapsamda alınması planlanan sanallaştırma yazılımının sunduğu teknolojik yeteneklerin irdelenmesi ve kuruma uygun çözümün tespit edilmesi oldukça önem arz etmektedir. Sanallaştırma yazılımları genel olarak işlemci ve çekirdek sayıları ile teknolojik yeteneklerine göre lisanslanmaktadır. Bu nedenle, ihtiyaç duyulmayan yazılımsal çözümün proje maliyetini gereksiz yere yükselteceği bilinmelidir.

- **Sunucu sistemleri:** Sunucu sistemlerinin tüm bileşenlerinin sanal platforma uygunluğunun ön koşul olarak değerlendirilmesi gerektiği bilinmelidir. Kurumun sağladığı bilişim hizmetlerinin sunucu teknolojisinin seçiminde önemli bir faktör olduğu unutulmamalıdır. Hizmetlerin çeşitliliğine göre oldukça farklı platform tercihleri gündeme gelebilmektedir. Sanallaştırma teknolojilerini ilgilendiren tüm bileşenlerde olduğu gibi yatayda ölçeklenme hususu sunucu seçiminde ihmal edilmemesi gereken en önemli noktalardan bir tanesidir. Mevcut sunuculara daha sonra doğabilecek ihtiyaca göre işlemci, hafıza, disk veya aynı platforma uygun sunucunun bir bütün olarak alt yapı değişikliğine gidilmeden büyüyebilen sistemlerin tercih edilmesi önemlidir.

- **Harici disk sistemi:** Gerek sunucu sanallaştırması gerekse masaüstü sanallaştırması için harici disk sistemi vazgeçilmez bileşenlerden birisidir.

Tercih edilecek disk sisteminin desteklediği yeni teknolojiler sanallaştırma anlamında kuruma oldukça farklı imkanlar sağlayabilir. Diskin kullanılma şekline yönelik teknolojik yetenekler sanallaştırma yazılımının getirileri ile birleştirildiğinde projeye ciddi getirileri olacaktır. Örneğin, tekil yedekleme ve asgari kaynak kullanımı gibi teknolojik yetenekler başarım ve disk kullanım oranlarında çok ciddi kazanımlar sağlanmaktadır.

- **Ağ iletişim yatırımı:** Sanallaştırma teknolojilerine geçiş ile beraber ağ alt yapısında da yatırım gerekebilir. Mevcut topolojinin geneline bakıldığında tercih edilecek ağ cihazlarının sunucular ve disk ortamları ile doğrudan ilişkisi vardır. Sanal makinelerin kesintisiz olarak çalışması, sunucular arası geçişlerde iş sürekliliğinin sağlanması konularında güçlü ve yedekli bir ağ altyapısının oluşturulması önemlidir.

5.1.3. Sanallaştırmanın Bakımı ve Sürdürülmesi

Yönetimsel açıdan bakıldığında, kaynakların etkin kullanılması için sanallaştırma ortamına geçiş sonrasında organizasyonel değişikliklerin gündeme gelebildiğini görmekteyiz. Sanal ortamın yönetilmesi kolaylık arz edeceğinden artan insan kaynağının verimli kullanılabilmesi için yeni yapılanma ihtiyacı doğabilir. Bu konuda teknik birimlerin ve üst yönetimin bilgilendirilmesi gerekebilir.

Teknik açıdan ise, sanallaştırma ortamında iş sürekliliğinin sağlanması için gerekli iş adımları tanımlanmalıdır. Bu konuda hızlı geri dönüşlerin sağlanması için yedekleme stratejilerinin iyi yapılandırılmış olması gerekir. Alınan yedeklerin ve anlık kopyaların geri dönüş senaryoları planlamalı ve bu senaryolar belirlenen periyotlar çerçevesinde test ortamlarında denenmelidir. Sanallaştırma yazılımı ve üzerinde çalıştığı donanımların belli periyotlar halinde 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 düzgün olarak konfigürasyonunun yapılması ve log dosyalarının düzenli olarak takip edilmesi gerekmektedir. Sanallaştırma ortamında kullanılan tüm yazılımların yeni sürümleri ve yamalarının takip edilmesi ve test ortamında denendikten sonra canlı sistemde devreye alınmasına ilişkin süreçlerin tanımlanması oldukça önemlidir.

Sanala geçiş sonrasında hizmetin doğru şekilde idamesi sürecinde yedekleme, yedeklerden geriye dönüş, ilgili yazılımlar ve donanımların periyodik kontrolleri ve ortaya çıkabilecek yeni ihtiyaçların değerlendirilmesi gibi iş kalemleri gündeme gelecektir. Bu çalışmaların gerçekleştirilmesi için yeni rollerin

tanımlanması gerekmektedir. Örneğin mevcut yedekleme süreçlerinin güncellemesi ve yeni stratejilerin eklenmesi gerekebileceğinden bu alanda yeni rol tanımlarına ihtiyaç duyabilir. Kurumların hali hazırda süreç yönetimi hizmetlerinin sanallaştırma sonrasında yeniden masaya yatırılması gerekebilir. Fiziksel ortamdan sanala geçiş sonrasında hizmetlerin kesintisiz olarak devam etmesi için farklı iş süreçleri tanımları ortaya konulmalıdır. Sanal ortamı tek bir konsoldan yönetebilen yazılımlar için belirlenen teknik personellere yetkileri çerçevesinde erişim imkanları sağlanmalıdır. Bu tarz yazılımlarda genelde yetkilendirme imkanları mevcuttur. Bu çerçevede sistemi sadece izleyebilecek personeller için izleme yetkileri tanımlanmalı, yönetim hakkı olanlara kaynakları belirleme, yeni sanal makineler oluşturabilme gibi hakları dikkatli bir şekilde vermelidir.

Bu aşamadaki ana maliyet kalemleri şu şekilde sıralanabilir:

- **Yedekleme:** Kurumun mevcut yedekleme sistemlerinin sanallaştırmayla doğacak ihtiyacı karşılayıp karşılamadığı araştırılmalıdır. Yeni bir yatırıma ihtiyaç var ise sanallaştırma çerçevesinde yatırımı planlanan diğer bileşenler göz önünde bulundurularak gerekli önlemler alınmalıdır.
- **Destek ve yönetim:** Kapasite planlama konusunda danışmanlık alınmasının önemli olduğu gibi projenin gerçekleştirilmesi ve idamesi hususlarında da destek alınması oldukça önem taşımaktadır. Kurumsal proje geçişlerinde yaşanacak sorunların ivedilikle çözülebilmesi için destek sürecinin çok iyi tarif edilmesi gerekmektedir. Bu konuda gerek üretici gerekse çözüm sağlayıcı destek sürecine dahil edilmelidir. Sanallaştırma projesi geçişi sonrasında çeşitli yönetimsel değişiklikler gündeme gelebilir. Fiziksel bir sistemin yönetiminin yanı sıra sanal bir ortamın yönetilmesinin ortaya çıkaracağı yeni bir hizmet anlayışı ve personel ihtiyacı gereksinim olarak karşımıza çıkabilecektir.
- **Eğitim:** Bilişim altyapılarında sanal ortamlara yönelim durumunda gerek sanallaştırma hizmetini sağlayan yazılımlar olsun gerek 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 yönetimi kolaylaştıracak araçları ise şu şekilde listeleyebiliriz:

- **Sanal makineleri tek bir konsoldan yöneten yönetim yazılımları:** Sanallaştırma projelerinin etkinleştirilmesi sonrasında merkezi yönetim yazılımları çok büyük önem arz etmektedir. Bütün sanal makineleri tek bir ortamdan yöneten yazılımlar teknik personele büyük kolaylık sağlamaktadır. Bu araçlar sayesinde bütün donanımsal kaynaklarınızı merkezi olarak yönetebilir ve sanallaştırmaya ilişkin gerek sanallaştırma sunucularına gerek bunlar üzerinde çalışan sanal sistemlere doğrudan erişim imkanı sağlanmaktadır.

- **İzleme yazılımları:** Sanallaştırma projelerinde önemli araçlardan biri de izleme yazılımlarıdır. Bu araçlar sayesinde sanal ortamdaki makinelerinizi ve tüm donanımlarınızın durumlarını takip edebilirsiniz. Herhangi bir sorun anında ilgili personele otomatik olarak uyarı gönderebilen bu yazılımlar sistemin idamesi için çok önemlidir. Ayrıca bu tarz yazılımlar sistemde yapılan tüm konfigürasyon değişiklerini log dosyalarında tutmakta ve bu da geriye dönük sürecin takibi açısından oldukça önemli olmaktadır.

- **Yedekleme ve Anlık Kopya Yaratma Yazılımları:** Yedekleme ve anlık kopya yaratma çözümleri aslında bütün sistemler için önemli olduğu gibi sanal ortamlarda da vazgeçilmez bileşenlerdendir. Yedekleme yazılımlarının sanal ortama uygunluğu bu hususta dikkat edilmesi gereken bir ölçüttür. Sanal ortamların yedeğinin alınması fiziksel ortamlara göre farklılık arz edebilir. Yedekleme yazılımlarından alınan yedeklerin belirli politikalarla arada bir geriye dönük olarak testlerinin yapılması gerekmektedir. Sanallaştırma altyapısı harici disk kullanımını zorunlu hale getirmiş ise bu disk sistemlerinin desteklediği teknolojilerden de faydalanılmalıdır. Özellikle anlık kopya yaratımı yazılımları, tekil yedekleme ve asgari kaynak kullanımı gibi özelliklerden de faydalanılmalıdır.

- **Afet kurtarma için çözüm sağlayan yazılımlar:** Farklı yerleşkelere kurulan çözümler ile iş sürekliliğinin sağlanması büyük önem taşımaktadır. Herhangi bir felaket durumunda bir merkezin devre dışı kalması neticesinde bu tür yazılımların teknolojik yeteneklerine bağlı olarak diğer tarafın ayağa kalkması kısa sürelerde gerçekleşmektedir. Sanal ortamda çalışan sanal makinelerin kopyalarının alınarak herhangi bir sorunda sanal makine bazlı kısa sürede geri dönüş sağlanabilir.

5.2. Farklı Sanallaştırma Tipleri İçin Yöntemler

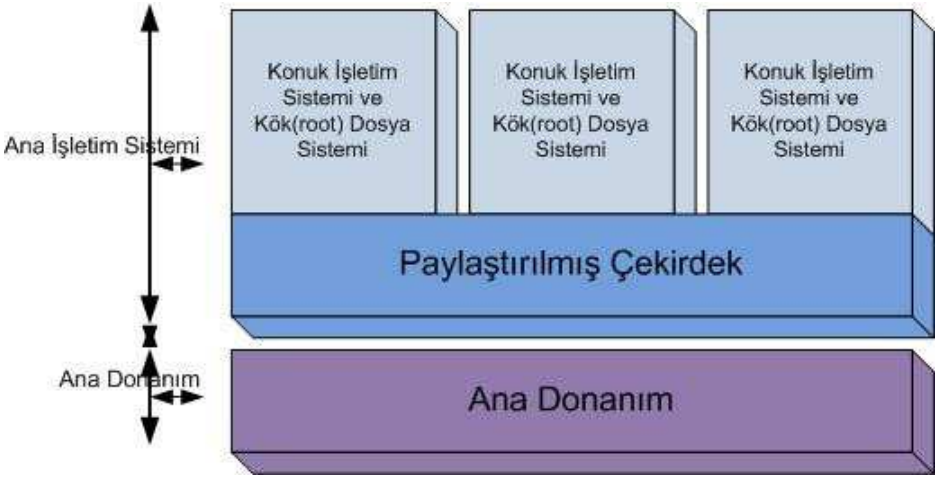
Farklı sanallaştırma teknolojileri elbette ki farklı yöntemlerle gerekleştirilmelidir. Her sanallaştırma teknolojisi farklı altyapı, donanım ve yazılım teknolojilerine ihtiyaç duymaktadır. Bu ihtiyaçları bir araya getirip gerçekleştirilmek istenen sanallaştırma yapısını oluşturmak için izlenmesi gereken yöntemler bu alt bölümde açıklanmaktadır.

5.2.1. Sunucu Sanallaştırması

Sunucu sanallaştırmasını elde etmenin çeşitli yöntemleri bulunmaktadır:

a. Çekirdek paylaşımlı sanallaştırma (Shared Kernel Virtualization)

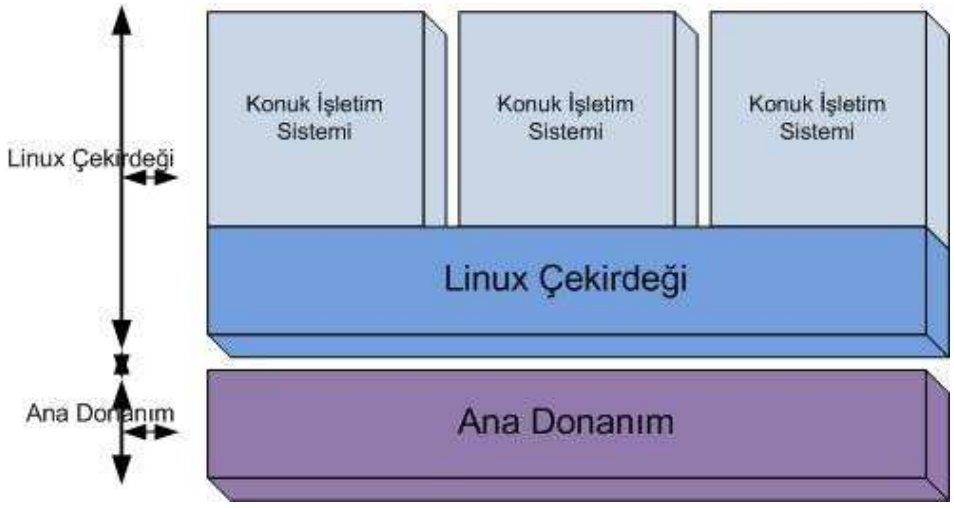
Bu yöntemle sanallaştırma Linux ya da UNIX tabanlı işletim sistemlerinin mimari avantajlarını kullanarak sağlanmaktadır. Bu işletim sistemlerinde çekirdek (kernel) tüm işletim sistemi ve donanım arasındaki iletişimi sağlayan bir katman olarak görev almakta olup, kök dizini (root) ise tüm çalıştırabilir dosyalar, uygulama kütüphaneleri ve diğer dosyaların tutulduğu alanı tarif etmektedir (Şekil 5.2). Bu yöntemde tüm sanal makineler aynı çekirdeği kullanarak donanıma erişebilirken farklı kök dizinlerini kullanarak birbirlerinden ayrılmaktadır. Bu yöntemin uygulanması söz konusu işletim sistemlerinde var olan dinamik olarak kök dizininin değiştirilebilmesi yeteneği (chroot) sayesinde mümkün olmaktadır. Bu yöntemin avantajı başarım konusunda en üst seviyede verim alınabilmesi iken, dezavantaj olarak farklı işletim sistemlerinin, hatta aynı işletim sistemi olsa bile farklı çekirdek kullanımı durumunda bu yöntemin kullanılamaması sayılabilir. Bu yöntemi kullanan yazılımlara örnek olarak, Linux VServer, Solaris Zones and Containers, FreeVPS, OpenVZ verilebilir.



Şekil 5.2: Çekirdek Paylaşımlı Sanallaştırma

b. Çekirdek seviyesinde sanallaştırma (Kernel Level Virtualization)

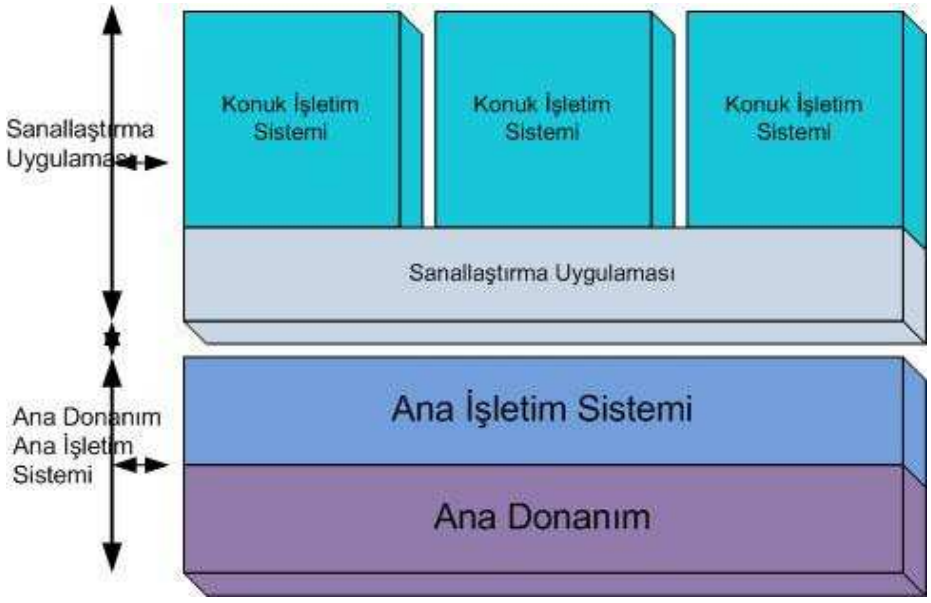
Çekirdek paylaşımlı sanallaştırmaya çok benzer bir yöntem olmakla beraber, anabilgisayar işletim sistemi çekirdeği sanal makineleri yönetebilmek için özel eklentilere sahip olacak şekilde değiştirilmiştir ve her sanal makinenin kendine ait ayrı bir çekirdeğe sahip olması ile diğerinden ayrılmaktadır (Şekil 5.3). Bu yöntemde çekirdek paylaşımlı sanallaştırmadaki kısıtlamalara ek olarak konuk işletim sistemi çekirdeklerinin, üzerlerinde bulundukları anabilgisayar işletim sistemi çekirdekleri ile aynı donanıma özel derlenmesi gerekmektedir. Bu yöntemi kullanan yazılımlara örnek olarak, User Mode Linux (UML), Kernel-based Virtual Machine (KVM) verilebilir.



Şekil 5.3: Çekirdek Seviyesinde Sanallaştırma

c. Konuk edilen işletim sistemi sanallaştırma (Hosted Virtualization)

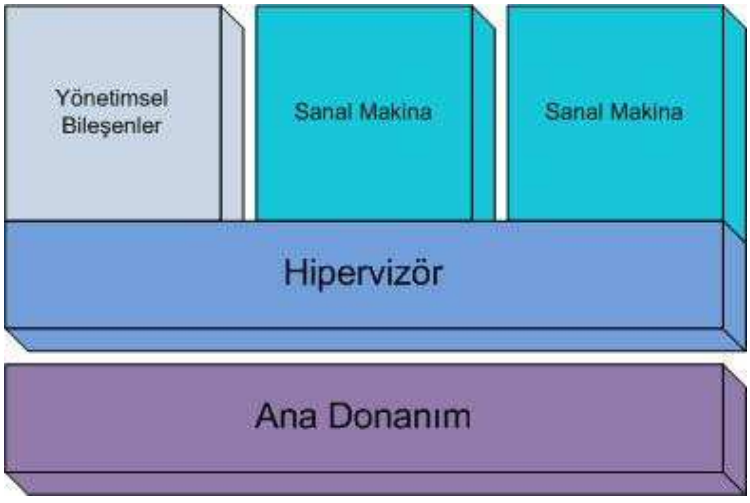
En kolay anlaşılabilir sanallaştırma yöntemidir. Fiziksel host herhangi bir değiştirilmemiş işletim sistemi (Windows, Linux, Unix, MacOS X) kullanır ve bu işletim sistemi üzerinde çalışan bir yazılım aracılığıyla sanallaştırma gerçekleştirilir. Bu yazılım, sanal makinelerin çalıştırılması, durdurulması ya da fiziksel donanıma erişimlerinin yönetilmesini sağlayan bir ara katman olarak görev aldığı gibi; konuk işletim sistemi üzerinden gelen komut akışlarını (instruction stream) tarayarak, bu komutların daha alt katmanda donanıma doğrudan erişebilecek şekilde yeniden yazılmasını (binary rewriting) sağlamaktan da sorumludur (Şekil 5.4). Avantaj olarak anabilgisayar ve konuk işletim sistemleri üzerinde herhangi bir değişiklik ihtiyacı getirmez ve işlemci üzerinde herhangi bir sanallaştırma desteğine ihtiyaç duymazlar. Buna karşılık ara katmanların çokluğu sebebiyle başarım olarak çok verimli değillerdir. Bu yöntemi kullanan yazılımlara örnek olarak, VMware Server, VirtualBox verilebilir.



Şekil 5.4: Konuk Edilen İşletim Sistemi Sanallaştırma

d. Sanal makine monitörü seviyesi sanallaştırma (Hypervisor Virtualization)

x86 mimarisinde işletim sistemlerinin ve uygulamaların donanıma erişebilmeleri için Halka (Ring) 0,1, 2 ve 3 olarak adlandırılan 4 farklı yetki seviyesi bulunmaktadır (Şekil 5.5). Kullanıcı seviyesi uygulamalar en az yetkili olan Halka 3 seviyesinde çalışırken işletim sistemleri daha üst yetki isteyen komutlarını çalıştırabilmek amacıyla hafızaya ve diğer donanımlara direk erişime yani Halka 0 seviyesinde ihtiyaç duymaktadır. Ancak x86 mimarisi üzerinde sanallaştırmanın mümkün olabilmesi için sanallaştırma katmanının işletim seviyelerinin de daha altında en üst yetkili olacak şekilde (Halka 0) donanıma direk erişim izni olması gerekliliği vardır.



Şekil 5.5: Sanal Makine Monitörü Seviyesi Sanallaştırma

Bunu sağlayabilmek amacıyla temelde 3 başlıkta ele alınabilecek teknikler geliştirilmiştir:

- **Tam sanallaştırma (Full Virtualization using Binary Translation):** Bu yöntemde VMM (Virtual Machine Monitor, Sanal Makine İzleyici) adlı sanallaştırma katmanı Halka 0 seviyesine yerleşmiş ve donanıma doğrudan erişim sağlayabilir pozisyondadır. Halka 1 seviyesine ise konuk işletim sistemi yerleşir ve donanıma VMM aracılığıyla erişebilmektedir. VMM, sanal işletim sisteminden gelen istekleri ikilik çevrime (binary translation) tabi tutarak çalıştırır. Ancak başarım endişeleri sebebiyle kullanıcı istekleri VMM ara katmanı üzerinden değil donanıma direk erişim ile olmaktadır. Bu yöntemin avantajı, sanal işletim sistemi herhangi bir değişiklik ihtiyacı duymamakla beraber aslında sanal olduğunun da farkında değildir. Dezavantajı ise nispeten (işletim sistemi destekli sanallaştırma metoduna göre) başarımda olmaktadır. Microsoft Virtual Server, VMware ESX, Workstation ve Server bu yöntemi kullanan ürünlere örnek olarak verilebilir.

- **İşletim Sistemi destekli sanallaştırma (veya Benzetim sanallaştırma, Paravirtualization, OS Assisted Virtualization):** Bu yöntem başarım ve verimliliği artırmak amacıyla, Halka 0'a yerleşen sanal işletim sistemi (paravirtualized guest OS) ile donanım arasına girerek iletişimi sağlayan bir sanallaştırma katmanı getirmektedir. Sanal işletim sistemi donanımla iletişime geçerken sanallaştırma katmanını kullanacak şekilde değiştirilmiştir. Sanallaştırma yapılamayan işletim sistemleri komutları yerine sanallaştırma katmanına gönderilen hiper çağrı (hypercall) adı verilen özel komutlar kullanılmaktadır. Sanallaştırma katmanı aynı zamanda hafıza yönetimi, kesmelerin yönetimi (interrupt handling) ve saat koruması gibi diğer kritik çekirdek işlemleri için de hiper çağrı arayüzleri içermektedir. Tam sanallaştırmada sanal işletim sistemi kendisinin sanal olduğunun farkında olmazken ve duyarlı işletim sistemi çağrıları ikilik çevrime uğratılırken yazılım destekli sanallaştırma bu noktalarda farklılık göstermektedir. Bu yöntemin en temel getirisi, daha az sanallaştırma yükü getirerek başarımın artışını sağlamasıdır. Ancak başarım artışı sanal makine üzerindeki iş yüküne göre değişkenlik gösterebilir. Dezavantajı ise sanal işletim sistemi üzerinde değişiklik gerektirdiğinden değiştirilemeyen işletim sistemlerini (örneğin, Microsoft Windows) desteklemiyor olması ve uyumluluk ile taşınabilirlik gibi

konularda zayıf kalmasıdır. Xen, VMI (Virtual Machine Interface, Sanal Makine Arabirimi) desteği ile VMware ESX, Workstation ve Server bu yöntemi kullanan ürünlere örnek olarak verilebilir.

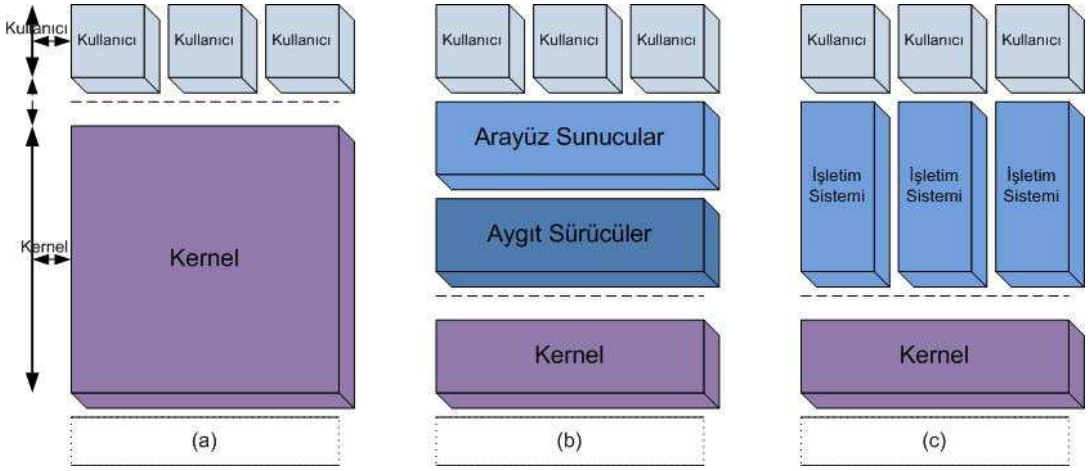
- **Donanım destekli sanallaştırma (Hardware Assisted Virtualization):** Donanım üreticileri sanallaştırma tekniklerini daha da basitleştirerek katkıda bulunmak amacıyla işlemci teknolojilerinde yenilikler getirmişlerdir. İlk olarak Intel, Virtualization Technology (VT-x) ile ve AMD, AMD-V ile Halka 0'ın da altında kök modu (Root Mode) yetki seviyesini getirmişlerdir. Bu yetki seviyesine yerleşen sanallaştırma katmanı yüksek yetki seviyesi gerektiren ve duyarlı çağrılarını işletim sisteminden otomatik alarak ikilik çevrime ya da yazılım desteğine gerek duymadan çalıştırabilir. Bu yöntemin avantajı sanal işletim sistemlerinde değişikliğe ihtiyaç bırakmaması olarak verilebilir. Ancak yeni bir teknoloji olduğundan tüm x86 mimarisine sahip donanımlar tarafından desteklenmemekte, bununla beraber günümüz teknolojileriyle çok fazla işlemci yüküne sebep olmaktadır. Xen, Microsoft Hyper-V, VMware ESX, Workstation ve Server bu yöntemi kullanan ürünlere örnek olarak verilebilir.

e. Mikro çekirdek seviyesi sanallaştırma (Microkernel Virtualization)

Yaygın kullanılmamakla birlikte, gömülü sistemlerde, özellikle gerçek zamanlı veya gerçek zamana yakın başarım beklenen, cep telefonları, havacılık sektörü yazılımları ve askeri uygulamalar gibi alanlarda çalıştırılması gereken sistemler için de sanallaştırma yapılmaktadır. Bu sistemlerin ihtiyaçlarının farkları nedeni ile sanallaştırılan yazılımın ihtiyaç duyduğu sanal kaynakların tam olarak tespit edilmesi ve çok dikkatli analizi ile sadece o kadar altyapının bulunduğu minimal bir işletim sistemi çekirdeğinin ve işletim sistemi katmanlarının (örneğin, dosya sistemi) oluşturulması sağlanmaktadır. Bu alt yapıya kısaca mikro çekirdek adı verilmektedir.

Mikro çekirdek sanallaştırılması çoğu kez hipervizör sanallaştırması ile karşılaştırılmaktadır. Hipervizör sanallaştırmasında, hipervizör, birden fazla işletim sistemini barındırır, ancak mikro çekirdek sanallaştırmasında mikro çekirdek doğrudan uygulama yazılımlarını barındırmaktadır (Şekil 5.6). İki sistem arasında hatırı sayılır bir fark bulunmaktadır. Mikro çekirdek sanallaştırmasının ana problemi, ve yaygınlaşmasının önündeki engel, uygulama yazılımlarındaki güncellemelerin mikro çekirdek üzerinde de kapsamlı testlere neden olmasıdır.

Mikro çekirdek sanallaştırmasındaki araçların çoğunluğu akademik projeler olmakla birlikte Green Hills INTEGRITY[1] örneğinde olduğu gibi EAL6+ seviyesinde güvenlik derecelendirmesi almış ticari mikro çekirdek sanallaştırma çözümleri de bulunmaktadır.



Şekil 5.6: İşletim Sistemleri gruplanması: a) Yekpare çekirdek, b) Mikro çekirdek c) Dikey Yapılandırılmış İşletim Sistemleri

5.2.2. Masaüstü Sanallaştırması

Masaüstü sanallaştırması üç ana yöntemle uygulanabilir [30, 31]:

a. Uzak Masaüstü Bağlantısı

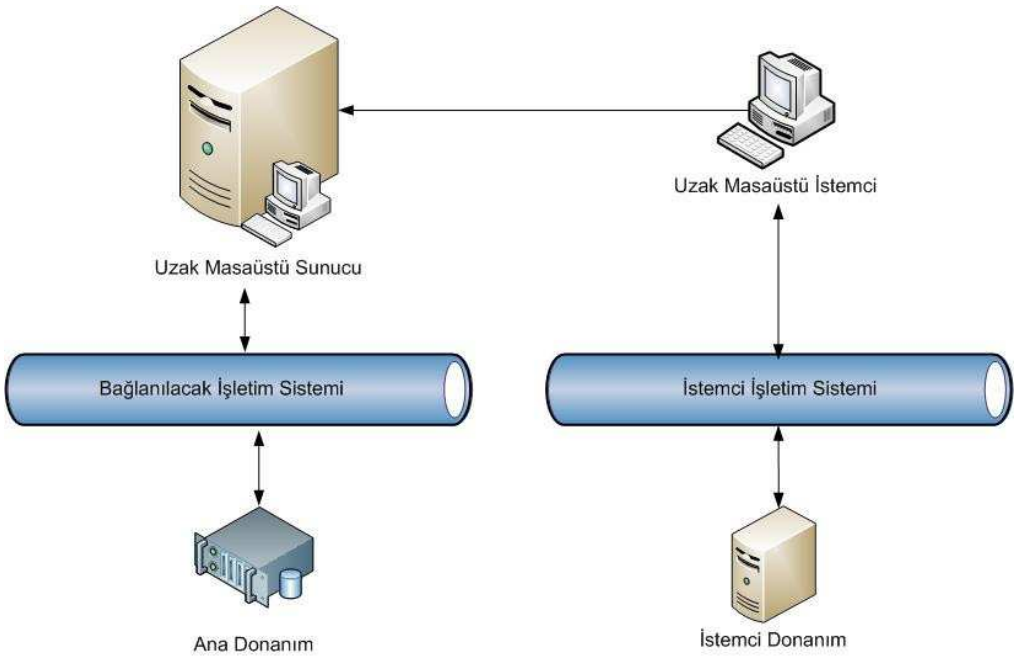
Uzaktaki bir bilgisayarın kaynaklarından yararlanılması için uzaktaki bilgisayarın denetiminin ele geçirilmesi işlemidir (Şekil 5.7). Bu yöntemi gerçekleştirmek için, önce ekranı paylaşılacak bilgisayara gerekli uzak masaüstü sunucusu, sonra da paylaşılan ekranı kullanacak bilgisayarlara uygun sistemin istemcisi kurulur. Aşağıda, bu yöntem ile masaüstü sanallaştırmayı sağlayan bazı örnekler verilmektedir:

- **Güvenli Komut Satırı Erişimi (Secure Shell, SSH):** Unix ve Linux tabanlı sistemlerde kaynakların komut satırı aracılığıyla kullanılması için uzaktaki bir bilgisayardan bağlanılmasına destek verilmesi özelliğidir. Cygwin gibi aracı programlarla Windows işletim sistemli bilgisayarlarda da kullanılabilir. Bu yöntem karşı taraftaki bilgisayarın kaynaklarına erişim sağladığı gibi bazı bilgilerin istemci tarafında yerelmiş gibi kullanılmasına da olanak sağlar.

[1] INTEGRITY gerçek zamanlı işletim sistemi, http://www.ghs.com/products/rtos/integrity.html.

- **Microsoft Uzak Masaüstü:** Microsoft'un tüm güncel işletim sistemlerinde hazır gelen uzaktan erişim özelliği, sunucunun izin vermesi durumunda, yalnızca IP numarası ya da bilgisayar adı yazarak uzaktaki bir bilgisayarın masaüstüne erişilmesini sağlar. Sıradan Windows işletim sistemi uzaktan aynı anda yalnızca tek bir kullanıcının bağlanmasına izin verirken, sunucu sürümleri birden çok kullanıcının aynı anda bağlanmasını desteklemektedir. Bu tür bağlantı Linux ve Solaris gibi diğer işletim sistemlerinde kullanılamaz.

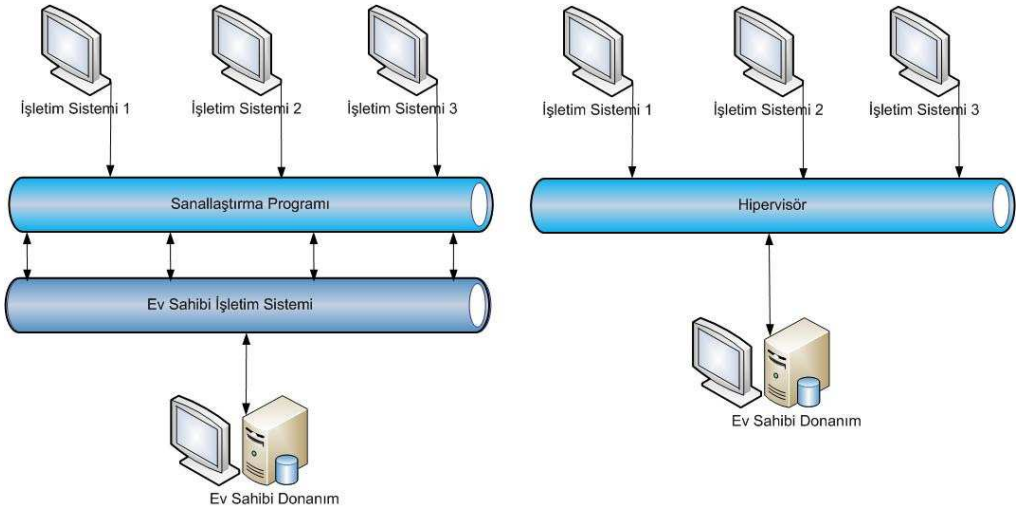
- **VNC (Virtual Network Computing – Sanal Ağ Bilişimi):** Uzaktaki bir bilgisayara kurulan VNC sunucusu sayesinde basit bir el bilgisayarından bile uzaktaki bilgisayarın masaüstüne erişim sağlama yöntemidir. Bu hizmeti gerçekleştirmek için bir VNC sunucusunun uzaktan izlenecek bilgisayara önceden kurulması ve ayarlarının yapılması gerekir. VNC genel olarak Microsoft Uzak Masaüstü'nden farkı bütün işletim sistemleriyle çalışması, standardının açık olması, sınırsız kullanıcı hizmeti sunması (aynı anda bir sunucuya birden fazla kullanıcının erişmesine olanak sağlaması) sayılabilir. Ancak Microsoft ürünlerinden farklı olarak bilgisayara kurulum gerektirmektedir. VNC'nin Microsoft Windows üstünde kullanılması durumunda kullanıcılar Windows dışında ayrı bir parola kullanarak sisteme erişir. Bu nedenle Windows kullanan makinelerde zaten üzerlerinde bulunan Uzak Masaüstü'nün kullanılması daha sorunsuzdur.



Şekil 5.7: Uzak Masaüstü Bağlantısı

b. Yerel Sanal İşletim Sistemi:

Yerel bir bilgisayarda mevcut bulunan işletim sisteminin içinden başka bir işletim sisteminin kurularak bu yeni masaüstüne erişilmesi yöntemidir (Şekil 5.8). Bu yöntemde yeni işletim sisteminin kurulması ve çalıştırılması için bir aracı sanallaştırma yazılımı kullanılması gereklidir. Bu yazılımlar bilgisayarın sahip olduğu donanım özelliklerine göre seçilmelidir. Aşağıda bu yazılımların bazıları sıralanmıştır:



Şekil 5.8: Sanal İşletim Sistemi

- **VirtualBox:** x86 tabanlı bilgisayarların üzerinde x86 tabanlı başka bir işletim sistemi kurmak üzere kullanılan bir sanallaştırma yazılımıdır. Açık kaynak sürümü olduğu gibi kurumsal sürümü de bulunmaktadır. Her yeni kurumsal sürümü çıktığında eski sürümünün özellikleri açık kaynak olan sürüme aktarılmaktadır. Sun'ın bir ürünü olan VirtualBox için kurumsal müşterilere destek de sunulmaktadır.
- **VMware Workstation:** VirtualBox'ın aynı işlevlerine sahip olan ticari bir yazılımdır. Daha fazla işletim sistemine destek vermektedir.
- **Xen:** Değişik işlemci mimarilerini desteleyen açık kaynak Xen sanal makinesi değişik işletim sistemlerini desteklemektedir.
- **KVM ve QEMU:** Linux sistemlerde KVM ve QEMU açık kaynak yazılımları birlikte işletim sistemi sanallaştırma amacıyla kullanılabilir.

Bu yöntemi uygulamak için, önce hali hazırda kullanılan işletim sistemi ya da hipervizör üzerine yukarıda bahsi geçen sanallaştırma yazılımı kurulur. Kurulması planlanan misafir işletim sisteminin kurulum medyası sanal ya da gerçek olarak

edinilip sanallaştırma yazılımına gösterildikten sonra misafir işletim sistemi sanallaştırma yazılımı üzerine gerçek donanım üzerine kuruluyormuş gibi kurulur. Bazı sanallaştırma yazılımları, ev sahibi ve misafir işletim sistemleri arasında iletişim sağlamak için misafir işletim sistemine yardımcı araçlar kurmak isterler.

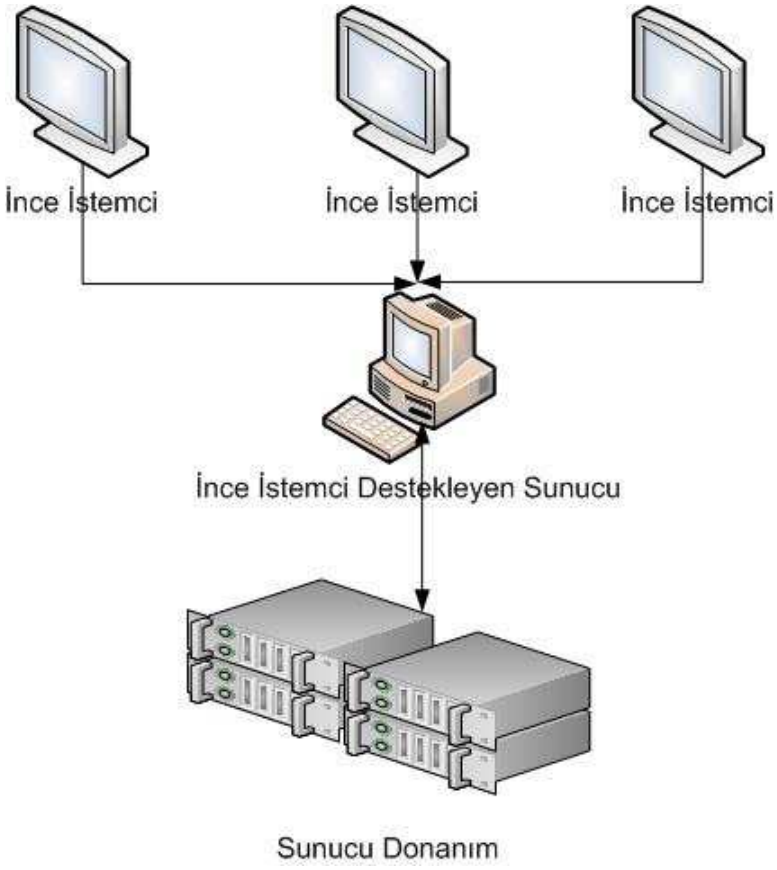
Bu modelde, sanal masaüstü veya masaüstleri, kullanıcı bilgisayarının üzerinde çalışır. Bunun için farklı yaklaşımlar kullanılabilir: Bunlardan ilkinde, kullanıcı bilgisayarı üzerine kurulan bir istemci sanal makine monitörü (client hypervisor) kurulur. Diğer işletim sistemleri, bu sanal makine monitörünün üzerinde konuk edilir. Burada sanal makine monitörü, donanım üzerinde mutlak ve tam kontrol sağlamaktadır. Diğerinde ise, sanallaştırma katmanı, normal bir uygulama olarak, kullanıcı bilgisayarı üzerinde kurulu bulunan işletim sistemi (Windows, Linux vb.) üzerine kurulur. Böylece, bir sanal ortam yaratılmış olur ve bu ortama farklı işletim sistemleri veya aynı işletim sisteminin farklı kopyaları kurulabilir. Ayrıca, İşletim Sistemi Akıntısı (OS Streaming) yaklaşımında, kullanıcı bilgisayarı çalıştırıldığında işletim sistemini uzaktaki sunucudan alarak çalıştırır ve yine uzaktaki bir sunucunun disk imajına erişerek çalışmaya devam eder. Burada, kullanıcı bilgisayarı üzerinde herhangi bir yazılım kurulu olmasına ve disk bulunmasına gerek yoktur ve dolayısı ile ince istemci kullanımı mümkündür.

c. Donanımda İnce İstemci Aracılığıyla Uzak Masaüstü Bağlantısı (Konuk edilen masaüstü sanallaştırması - Hosted desktop virtualization)

Sanal masaüstlerinin bir sunucu üzerinde konuşlandırıldığı durumlara verilen isimdir. Burada, kullanıcı bilgisayarı üzerinde bulunması gereken tek yazılım, bağlantı aracısıdır (connection broker). Bu nedenle, ince istemci (thin client) türü cihazlar, kullanıcı bilgisayarı olarak bu yaklaşımla birlikte kullanılabilmektedir (Şekil 5.9). Kullanıcı, bir bağlantı aracı yazılımı üzerinden sunucuya erişir ve ilgili arayüzü RDP (Remote Desktop Protocol) gibi standart bir protokol ile alır. Kullanıcı bilgisayarlarına düşen görev, sunucu tarafından üretilen arayüz görüntülerini ekrana yansıtmak ve kullanıcıdan gelen klavye, fare vb. girdileri sunucuya iletmektir.

İnce istemci denen bu tür donanımlar kullanıcıya herhangi bir işlem yeteneği sunmayabilir; asıl görevleri sunucudan aldıkları görüntüyü ekrana basmak ve kullanıcıdan alınan girdileri sunucuya iletmektir. Bütün işlem sunucu üzerinde gerçekleşir ve işletim sistemi de sunucunun üzerindedir. Kullanıcı yazılım altyapısı ile ilgili hiçbir konuda yetki sahibi değildir. Sunucu üzerinde işletim sistemi değişmesi

dahi kullanıcı tarafında bir değişiklik gerektirmez. Sunucu tarafında bu sanallaştırmayı sağlamak için uyumlu bir işletim sistemi kullanılmalıdır.



Şekil 5.9: Donanımda İnce İstemci Aracılığıyla Masaüstü Bağlantısı

Bu yöntemi uygulamak için, ince istemcilerin kendisine bağlanmasını destekleyen sunucu kurulduktan sonra ince istemcilere, sunucunun bilgilerini girilerek sunucuya bağlanılır.

Bu sanallaştırma şekli, birbirine çok benzer iki şekilde karşımıza çıkabilmektedir: *Sanal Masaüstü Arayüzü* (Virtual desktop infrastructure, VDI) yaklaşımında sunucu bilgisayar üzerinde, her bir kullanıcı için ayrı bir masaüstü sunulurken; *terminal sunumu* ismi verilen yaklaşımda, tüm kullanıcılar için toplam bir tane masaüstü sunucu yazılımı çalışmakta ve tüm kullanıcılar bu sunucuya bağlanmaktadır. Bir başka deyişle, kullanıcı ile uzak masaüstü sunucusu arasındaki ilişki, VDI yaklaşımında bire bir (one-to-one) iken, terminal sunumu yaklaşımında çoka bir (many-to-one) olarak karşımıza çıkmaktadır. Citrix XenDesktop, Microsoft Enterprise Desktop Virtualization, VMware View gibi ürünler bu grup altında toplanabilir.

5.2.3. Veri Depolama Sanallaştırması

Veri depolarında sanallaştırma, aynı veri yolu üzerinde farklı veri yolları varmış gibi davrandırma gereksiniminden çıkmış bir ihtiyaçtır. Bu ihtiyacı eş zamanlı yedekleme sistemleri takip etmiştir.

Sanal disklerde önemli olan bir veri yolu üzerindeki mantıksal bölüm tanımlayıcısı (Logical Unit Identifier, LUN) ya da mantıksal blok adresidir (Logical Block Address, LBA). Bu diskler aracılığı ile bir veri yolu üzerinde farklı adreslemelerde farklı diskler varmış gibi gösterilebilir. Bu işlem girdi-çıktı birimi üzerindeki adreslemelerin değiştirilmesi ile sağlanır. Geleneksel disk kontrol araçlarının yerine başlangıç ve bitiş adresleri mantıksal olarak gerçekleştirilir. Bu durumda bir disk birçok farklı yapıyı kullanır hale gelir. Bu duruma haritalandırma adı verilir. Haritalandırma mantıksal disk sürücüsü ana biriminde yer alır. Bu sayede bir disk üzerinde farklı yerlere yazılan veriler bu haritalandırma ile bulunabilir. Bütün haritalandırmalar mantıksal birimin ilk alanına yazılırlar.

Disk sanallaştırmasının en önemli özelliklerinden biri fiziksel yapılarla da sorunsuzca çalışabilmesidir. Bunun için iSCSI adı verilen bir protokol kullanılır. iSCSI protokolü mantıksal diski fiziksel ya da sanal makine üzerinde fiziksel bir disk gibi gösterebilir. Diskler yerel disk olarak algılanabilirler. Bu diskler formatlanmak zorunda değillerdir. Kümelemelerde biçimlendirilmemiş nisap (quorum) disk olarak da kullanılabilir.

Veri depolarında sanallaştırmanın birçok avantajı vardır. Verileri taşımak, verilerin kopyasını tutmak, fiziksele aktarmak oldukça kolaydır. Eskiyen medyalar üzerinden yeni medyaya veri taşındığında bu diski kullanan makine üzerinde ayar değiştirmeye gerek kalmaz. Önemli olan adresleme yapılarının doğru bir şekilde tanımlanmasıdır. Yönetimleri çok kolaydır, disk ekleme ve çıkarmak problemsizdir.

Dezavantaj olarak, her bir işletim sistemi için ayrı bir iSCSI protokolü gerektirir. Veriler için özelleştirme işlemi her bir uç kullanıcı makine için ayrı ayrı yapılmalıdır.

En bilinen açık kaynak kodlu ve genel kamu lisansı ile ücretsiz olarak dağıtılan veri deposu sanallaştırması yazılımı ise Openfiler'dır.

5.2.4. Veri ve Veritabanı Sanallaştırması

Veri tabanı büyüdükçe veri kayıtlarını paylaştırma hareketi onlarca yıldır kullanılan bir şeydir. Veri yönetimi çözümleri içerisinde kalan verinin paylaştırılması için kullanılan iki ana yol vardır:

i. Paylaşılan tüm veritabanları, bu veritabanlarının tamamını varsayan mimarlık, düğüm kümeleri, hepsi bir paylaşımı kullanırlar. İç-düğüm iletişimleri küme üzerindeki farklı düğümlerden ortaya çıkan güncel aktiviteleri senkronize etmek için kullanılır. Paylaşılan tüm veri yönetimi sistemleri tek haneli düğüm kümeleri için sınırlıdır.

ii. Paylaşım yapmayan veritabanı mimarlığı ki bunun içersindeki tüm veri içerden yönetilen paylaşımla açık iyi tanımlanmış veri bölge sınırlarıyla ayrıştırılmıştır. Paylaşım yapmayan veritabanları el yordamlı bölümlendirme gerektirmektedir.

Sanal bölümlendirmede mantıksal veri fiziksel veriden otonom bir şekilde üreterek ve büyük oranda veri bölümlemesini yöneterek soyutlandırılmıştır. Bunlar otonom bir şekilde elde edildiği için bölümleme yönetimi için gereksinim duyulan kaynaklar minimal seviyededir. Bu tarz büyük bölümlendirmeler şu şekilde sonuçlanır: Küçük olan bölümlemeler ve ilave bölümleri tanımlamak için yeniden bölümlendirme istemeyen sistemler donanım değiştirilse de randımanlı bir şekilde yönetilir ve dengeli yüklenirler. Bu sanal mimarlık hem "tamamı paylaşılmış" ve "paylaşımı yapılmamış" ile ilgilenmektedir. Mimarlar tüm veri bölümlendirmesini, çapraz bölümlendirme sorgusunu ve tam bölümlendirme taraması yapmadan hareket sürecini ölçeklendirebilmeye izin vermektedir.

5.2.5. Ağ Sanallaştırması

Ağ sanallaştırmasını sağlayabilecek yöntemler, aşağıda özetlenmektedir:

a. Protokol tabanlı yöntemler ve dış sanal ağlar

Protokol tabanlı yöntemler kullanıldığında elde edilen sonuç, dış sanal ağlar (external virtual network) olarak karşımıza çıkar. Bu yöntemlerle, çeşitli ağ bileşenleri, bir sanal ağ altında toplanır.

- **VLAN (Virtual Local Area Network)**. Türkçesi Sanal Yerel Alan Ağları olan VLAN, IEEE tarafından geliştirilmiştir. VLAN OSI 2. katmanda (Layer 2) çalışır. Adından da anlaşılabileceği gibi VLAN teknolojisi kullanılarak, bu teknolojiyi destekleyen cihazlar üzerinde mantıksal ağlar oluşturulur. Bu mantıksal ağlar aslında bölünmüş birer genel yayın alanlarıdır (broadcast domain).

  VLAN, yerel alan ağı üzerindeki ağ kullanıcılarının ve kaynaklarının mantıksal olarak gruplandırılması, farklı genel yayın alanlarına atanması

ve ağ cihazları üzerinde farklı kapılara (port) atanması ile uygulanır. VLAN kullanılan bir ağda, bir VLAN'da bulunan kullanıcılar sadece kendi genel yayın alanına sahip olacağından, birbirleri ile haberleşebilirler. Oluşturulmuş farklı bir VLAN'da bulunan kullanıcılar ile iletişim kuramazlar. Büyük ağlarda VLAN ihtiyacı işte bu sebepten dolayı ortaya çıkmış ve iletişim ağı mühendislerini büyük bir zahmetten kurtarmıştır. Ortamda OSI 3. katman çalışan (Layer 3) bir cihaz olması durumunda, bir VLAN'a üye ağ kullanıcısının farklı bir VLAN'a üye ağ kullanıcısı ile haberleşmesi sağlanabilmektedir. Artık günümüzde üretilen Layer 3 switch'ler, aynı zamanda yöneltici (router) modunda çalıştıkları için bunu yapabilmektedir. VLAN adaptasyonu sonrasında genel yayın (broadcast) trafiği azaltılır ve bant genişliği de artırılmış olur. Ayrıca ağ kullanıcıları daha kolay yöneltilebilir ve erişim izinleri (access list) çok daha kolay yapılandırılıp uygulanabilir.

VLAN kullanımı aynı zamanda ağ yatırımını da düşürmektedir. Örneğin, 48 kapılı bir ağ anahtarınız var ve bunun sadece 25 kapısını kullanıyorsunuz. Başka bir yerel alan ağı oluşturmanız gerekiyor ve 20 kişilik bir grubu ağa bağlayacaksınız. Yeni bir ağ anahtarı almak yerine elinizdeki 48 kapılı ağ anahtarının boş olan 23 kapısını başka bir VLAN oluşturup atayarak, yeni bir kapılı bir ağ anahtarı almaktan tasarruf elde edebilirsiniz.

VLAN'lar ağ üzerinde uygulanarak, 2. seviye anahtarlamanın getirdiği, genel yayın kontrolü, güvenlik ve esneklik gibi problemleri ortadan kaldırılır.

- **VPN (Virtual Private Network):** Genel iletişim altyapısını kullanarak, tünel açma protokolü (tunneling protocol) ve güvenlik yordamları aracılığı ile güvenli ve özel veri aktarımını sağlayan sanal özel ağ teknolojisine VPN adı verilir. VPN ağlarını bir şirket tarafından sahiplenilmiş veya kiralanmış özel hatlar olarak düşünebiliriz. VPN uygulamasının temel amacı, bir firmaya özel bir hat tahsis edilmesi yerine firmanın ayni hizmeti daha düşük fiyata herkes tarafından paylaşılan altyapıdan temin etmesidir. Telefon şirketleri ses mesajları için daha önceden paylaşımlı güvenli hatlar için yatırım yapmışlardır. Bir VPN ağı, aynı şekilde güvenli ortak paylaşımı, veri transferinin gerçekleştirilmesi için izin verir. Günümüzde şirketler VPN teknolojisini hem dış ağ (extranet), hem de geniş iç ağ (intranet) uygulamalarında tercih etmektedirler.

Sanal özel ağ teknolojisinde verinin herkese acık hatlar üzerinden gönderilmesinden önce şifrelenmesi, sonrasında da ulaştığı tarafta deşifre edilmesi söz konusudur. Bunun dışında sadece iletilen verinin değil, gönderinin ve alanın iletişim ağı adreslerinin şifrelenmesi ile daha fazla güvenlik sağlanabilir. Microsoft, 3com ve birkaç diğer firma PPTP teknolojisini geliştirmiş, daha sonra bu protokol Microsoft tarafından Windows NT işletim sisteminde desteklenmiştir. VPN yazılımları tipik olarak güvenlik duvarının bir parçası olarak kurulup servis verirler. Birçok güvenlik duvarı bu hizmeti sağlamaktadır.

VPLS (Virtual Private LAN Service): VPLS ya da Sanal Özel Yerel Ağ Hizmeti, günümüzün iletişim ağ ortamında sıkça kullanılan bir terim olup, bir VPN teknolojisidir ve IP tabanlı ağlar üzerinden, çok noktadan çok noktaya Ethernet tabanlı iletişim sağlama yöntemi olarak karşımıza çıkar. VPLS, genellikle "geleceğin iletişim ağı" olarak anılan gelecek teknolojiler arasında yer alacağa benzemektedir. Bugün artan popülerliğine rağmen, aslında VPLS sadece kısa bir süredir kullanımdadır ve bu terimin nasıl tanımlandığını anlamak dikkat gerektirir [32].

Eğer bir işletme, örgülü bağlantıya (meshed connectivity) ve iletişim ağını ölçeklendirebilmeye gereksinim duyuyorsa, VPLS iyi bir çözümdür. IP yolları bir sağlayıcıyla paylaşılmadığından dolayı, yönlendirmeyi (routing) kontrol etmek isteyen ve kendi ağlarını ve bağlantılarını yönetmek isteyen müşteriler için oldukça uygundur. Genellikle bu, küçük ve daha az karmaşık iletişim ağı ortamını yansıtır. İşletmeler, var olan yerel Ethernet arayüzlerinden faydalanabilir ve iletişim ağlarını Geniş Alan Ağlarına (Wide Area Networks) genişletebilirler. VPLS, örgülü olmayan ağların, Ethernet bağlantısına ihtiyaç duyulmayan, yüksek sayıdaki sitelerin bir ağ içerisinde birbirleriyle iletişim kurmaları gereken yerlerin veya IP yollarını duyurmak isteyen bir işletmenin gereksinimini karşılayamayabilir. Ethernet'in bazı coğrafi kapsam sınırlamaları olduğu için, belirli bölgelerde daha büyük ağları tamamlamak amacıyla kullanılabilinir; ancak coğrafi olarak dağılmış birden çok yerin gereğini karşılayamayabilir.

VPLS, işletmelerin bant genişliğini megabitlerden gigabitlere ölçeklendirmesine olanak sağlayarak, Ethernet'in tüm yararlarını sunar. Donanımların iyileştirilmesi kolay olduğu için, bant genişliği gereksinimleri kısa zamanda karşılanabilir. Daha yüksek hızda bir hizmete ölçeklendirmek, var olan donanımda küçük bir değişiklik yaparak kolay

olabilir. Çoğu işletmenin hali hazırda yerinde Ethernet donanımı mevcuttur, VPLS yapmak düşük maliyetli bir çözümdür. Ayrıca, yüksek hızlara ulaşmak, bakırdan fibere geçiş yapmayı gerektirmez. Hizmet, protokolden bağımsızdır, IP, IPX vb. protokolleri de destekler.

VPLS'in yararlarından biri de, yönlendirme esnekliği ve kontrolüdür. Ethernet'in özünde olan herhangi birinden diğerine bağlanabilmek yeteneği, sitelerin eklenmesini veya çıkarılmasını kolaylaştırır. Bir işletme, bir kere ağa bağlandığı zaman, ağ üzerindeki herhangi bir yere ulaşabilir. Bir Ethernet anahtarına benzer olarak, VPLS, yeni bir site çevrimiçi olduğunda, tablolarını günceller. Yeni bir siteyle iletişim kurabilmek için, ağ üzerinde var olan sitelerde bir değişiklik yapılmasına gerek kalmaz.

VPLS, kolay ölçeklendirilebilir mimarisine, esnekliğine ve karşılanabilirliğine bağlı olarak giderek daha popüler hale gelmektedir. Günümüzde kullanılan birçok teknolojide olduğu gibi, VPLS'in iyi bir çözüm olup olmadığına karar verebilmek için, işletmenin gereksinimleri göz önünde bulundurulmalıdır. Bazı durumlarda, çözümlerin bir karışımını oluşturmak gerekebilir.

b. Sanal cihaz tabanlı yöntemler ve iç sanal ağlar:

Sanal ağ anahtarları gibi sanal ağ cihazlarının kullanılarak sanal ağ arayüz kartlarının (VNIC) birbirlerine bağlanması ile iç sanal ağlar (internal virtual network) elde edilmiş olur. Böylelikle, aynı ortamdaki sanal sistemler arasında bir ağ elde edilmiş olur.

Sanal cihazlar arasındaki ağ trafiği, prensip olarak bellek üzerinde akar. Ancak yine prensip olarak sanal sistemlerin, çalışma anında farklı fiziki sistemlere taşınabileceği öngörülebileceğinden, iç sanal ağlarda oluşan trafiğin iki farklı fiziki sistem arasında, olağan ağ trafiğine dahil olarak akması gerekeceği göz ardı edilmemelidir.

Sanal cihaz tabanlı ağ kurulumları bu nedenle sanal ağ arayüz kartlarına ek olarak fiziki ağ sistemlerindeki tüm ağ aygıtlarının (anahtar, güvenlik duvarı, vb) birer sanal denginin kullanımını, ayrıca gerekli görüldüğünde, bir önceki kısımda da bahsedilen teknikler, özellikle VPN kurulması yolu ile güvenli iletişimin sağlanmasını gerekli kılabilmektedir.

5.2.6. Uygulama Sanallaştırması

Bu bölümde, uygulama sanallaştırması yöntemleri tanıtılmaktadır.

a. Emülasyonlar ile sanallaştırma

Emülasyon ile sanallaştırma dendiğinde ilk akla gelen bir yazılımın uyumsuz bir donanım üzerinde çalıştırılması olmaktadır. Örneğin, mevcut masaüstü bilgisayarınızı nostaljik Commodore 64'ünüze çevirmek ya da bir oyun konsolu haline getirmek (örneğin, Nintendo için zsnes[2] kullanmak) mümkündür. Ya da masaüstü bilgisayarınız üzerinde bir cep telefonunu klavyeniz ve fareniz ile kontrol edebilirsiniz. Bu tip donanım emülasyonlarının dışında işletim sistemi emülasyonları da oldukça yaygındır. Örneğin, eski Dos işletim sistemini günümüz işletim sistemleri üzerinde çalıştırarak eski oyunları yeniden oynayabilmek ya da Microsoft Windows işletim sistemine özel yazılmış uygulamaları Linux, MacOS X, FreeBSD, Solaris gibi diğer işletim sistemleri üzerinde çalıştırmak bu tip emülasyon yazılımları ile mümkündür. Bunlara örnek olarak Dosbox, Wine, Winelib verilebilir.

b. Çapraz-platform sanallaştırma (cross-platform virtualization)

Günümüzde genel olarak uygulamalar işlemci tipine ve işletim sistemine özel olarak derlenmiş çalıştırılabilir ikili dosyalar olarak bulunmaktadır. Buradaki zorluk kaynak kodu aynı bile olsa farklı platformlarda çalışabilmesi için kodun yeniden derlenmesi gerekliliğidir. Çapraz-platform sanallaştırma ile bir soyutlama katmanı işletim sistemi ile çalıştırılabilir uygulama arasına girmektedir ve bu şekilde yeniden derleme ihtiyacı kalmadan farklı platformlarda çalışabilmektedir. Soyutlama katmanı çalıştırılabilir dosyayı yorumlar ve üzerinde bulunduğu platforma göre ikilik dosyayı çalıştırır. Bu ara işlemler sebebiyle derlenmiş çalıştırılabilir dosyalara göre başarım dezavantajı bulunmaktadır ancak her işlemci ve işletim sistemi için kaynak kodunun değiştirilmesine gerek duyulmaması ve her biri için derleme ihtiyacının olmaması getirileridir. Bu tip sanallaştırmaya örnek olarak JVM'yi (Java Virtual Machine) verebiliriz. Aynı Java uygulaması JRE (Java Runtime Engine) kurulu tüm Linux, MacOS X ya da Microsoft Windows işletim sistemlerinde çalışabilmekte ve eğer donanıma erişim gibi bir ihtiyacı yoksa basit bir değişiklikle web üzerinden bir tarayıcı aracılığıyla bile çalıştırılabilmektedir.

c. Taşınabilir uygulamalar (portable programs) ve merkezden yönetilebilir uygulama servisi araçları ile sanallaştırma

Geleneksel olarak uygulamalar bir kurulum dosyası olarak edinilir. Kurulum ile birlikte ana çalıştırılabilir dosya ve gerekli yardımcı dosyalar belirli dizinlere kopyalanır. Uygulama ayarları ve yapılandırmaları ise işletim sistemi kayıt defteri

[2] ZSNES oyun emülatörü, http://www.zsnes.com.

gibi ortamlarda tutulmaktadır. Taşınabilir uygulamalarda ise uygulamanın kurulum ile birlikte oluşturduğu dizin yapısı korunur, gerekli ayar ve yapılandırmalar ise işletim sistemine yazılmadan tutulur. Böylelikle uygulama işletim sisteminden bağımsız olarak çalıştırılabilir ve taşındığı başka bilgisayarda da aynı ayarlar ile kullanılabilir. Birçok ücretsiz ya da açık kaynak uygulamanın taşınabilir sürümleri rahatlıkla bulunabildiği gibi bazı araçlar (örneğin, VMware ThinApp, Xenocode Virtual Application Studio, InstallFree vb.) yardımıyla kurulan uygulamalar taşınabilir hale de getirilebilmektedir.

Taşınabilir uygulamalara benzer mantıkta çalışan ancak bunun bir adım ötesine geçen, kurum içi kullanılan uygulamaların merkezden yönetilebilmesini ve çalıştırıldığı bilgisayarda bir iz bırakmamasını sağlayacak araçlar bulunmaktadır. Citrix XenApp, VMware ThinApp, Microsoft Application Virtualization, Novell ZENworks Application Virtualization bu araçlara örnek olarak verilebilir. Bu araçlar istemci bilgisayarlarında bir sanallaştırma katmanı yaratarak uygulamanın kullandığı yapılandırma ayarlarını üzerinde çalıştığı bilgisayarda değil bir sunucuda tutmakta ve merkezden yapılan ayar değişikliklerinin uygulamayı kullanmak isteyen tüm istemcilere yansımasını sağlamaktadır. Böylelikle bilgi işlem birimlerine uygulamanın güncellenmesi ve kaldırılması gibi konularda merkezi bir yönetim avantajı sağlandığı gibi lisans takibinin rahatlıkla yapılabilmesi ve aynı uygulamaya ait farklı sürümlerin çakışmalarının engellenmesi gibi konularda da faydalar getirmektedir.

d. Sanallaştırılmış uygulama sunucuları (virtual appliance) ile sanallaştırma

Günümüzde kurulumu ve yapılandırması güç birçok uygulama, ayarları yapılmış ve çalışır şekilde bir sanallaştırılmış uygulama sunucusu olarak edinilebilir durumdadır. Ağ ve ağ güvenliği yönetimi araçları, ortak çalışma olanağı sağlayan uygulama sunucuları, e-posta ve web sunucuları gibi birçok sanal sunucu çalışır durumda internet ortamından indirilebilir ve kullanılmaya hazır şekildedir. Bunlar içinde ücretsiz ve sınırsız kullanım hakkı olan araçlar olduğu gibi birçok ücretli aracın deneme sürümleri de yer almaktadır.

5.2.7. Bellek Sanallaştırması

Günümüzde yazılım başarımını darboğaza sokan bellek sınırlamaları, iletişim ağları sayesinde oluşturulan bir ortak bellek havuzunun paylaşımı sayesinde aşılmaktadır. Bu ortak bellek havuzundan faydalanabilen bilgisayarlar ve dolayısı ile bu bilgisayarlar üzerinde çalışan uygulamalar, genel başarımlarını yükseltmek,

bellek kullanım verimliliğini sağlamak ve sistemden daha fazla yararlanmak için istenilen miktarlarda belleğe erişim avantajlarına sahip olurlar.

Bu platformda yer alan sunucuların sahip oldukları yazılımlar, sunucuların ortak bellek havuzuna bağlanmasını ve sahip oldukları bellek kapasitelerinin bu platform üzerinde paylaşılmasını sağlar. Bu ortak bellek havuzunda paylaşılan hafıza, bir yönetim yazılımı ile yönetilir. Bu yönetim yazılımı veri hazırlama politikalarını belirler, ortak havuza verilerin eklenmesi, tahliye edilmesi kararlarını vererek istemcilerden gelen bellek ihtiyaçlarını yönetir.

Ortak bellek havuzlarına iki farklı yöntemle erişilir:

a. Uygulama Düzeyi Bellek Sanallaştırması

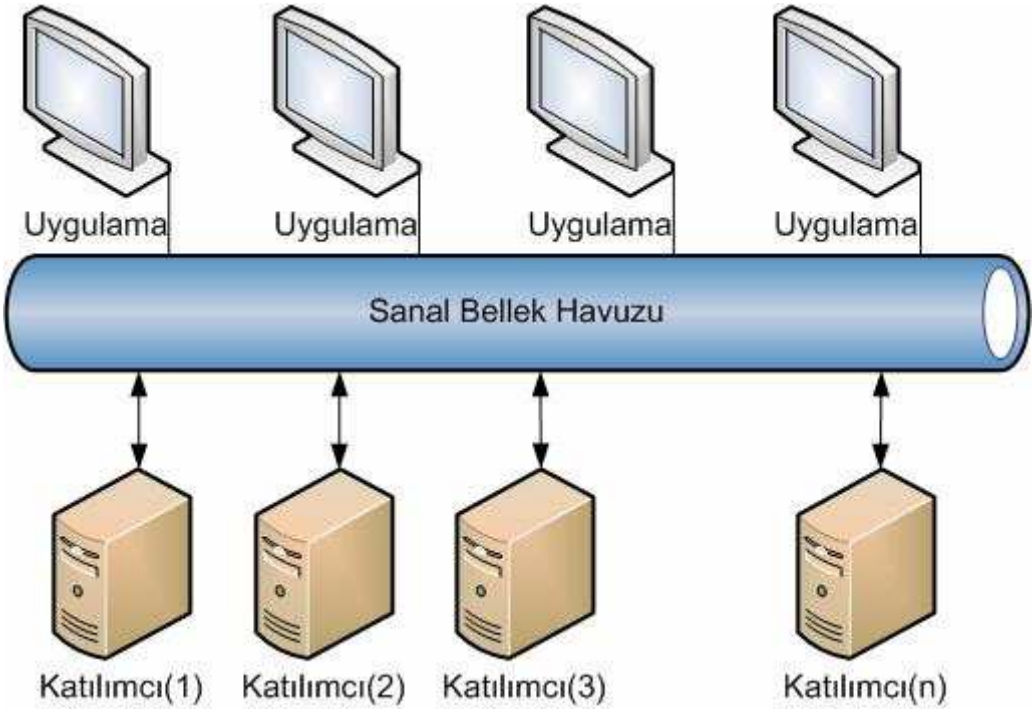
Bu yöntemde, uygulama düzeyinde yüksek hızlı paylaşımlı bir önbellek oluşturmak için ortak havuza bir arayüz (API) üzerinden erişilir (Şekil 5.10). Ortak havuzun iletişim ağı üzerinden erişilebilen bir dizin şeklinde tanımlanıp kullanılması da uygulama düzeyinde bir diğer yüksek hızlı bellek paylaşım yöntemidir.

b. İşletim Sistemi Düzeyi Bellek Sanallaştırması:

İşletim sistemi düzeyinde ise ortak havuz, sayfa önbelleği olarak tanımlanır. Bu yöntem yerel veya ağa bağlı depolama birimlerine oranla çok daha hızlı ve büyük kapasiteli bir kaynak sağlar. Burada bellek sanallaştırması uygulamaları, paylaşılan hafıza sistemlerinden farklıdır. Paylaşılan hafıza sistemleri, bellek kaynaklarının soyutlanmasına izin vermezler, kümelenmiş bir uygulama ortamı içinde yer almazlar, gerçekleştirilen bellek paylaşımı tek bir işletim sisteminin ürünüdür (Şekil 5.11).

Bellek sanallaştırması aynı zamanda hafıza tabanlı depolama yöntemlerinden de (örneğin, SSD) farklıdır. Hafıza tabanlı depolama yöntemi de bir kümelenmiş bilgisayar sistemi üzerinde hizmet verebildiği halde, üzerinde çalıştığı sabit disk ortamının fiziksel kısıtları nedeniyle daha karmaşık ve az verimli bir paylaşım sunar.

Bellek sanallaştırması teknolojisi, bellek yönetimi mimarileri ve sanal bellek tekniklerini izler. Her iki alanda gelişimin yolu ise, fiziksel kaynakların ihtiyaçlar doğrultusunda daha verimli kullanılabilmesi amacıyla mantıksal ve fiziksel kaynaklar arasında sıkı ilişkilerin daha esnek ve soyut hale getirilmesinden geçmektedir. NUMA ve SMP mimarileri çok işlemcili tekil sistemler üzerinde bellek kullanımını dinamik olarak yönetirken; bellek sanallaştırması ise, bir ağa bağlı birden fazla sistemin toplam hafızasını tek bir bellek havuzu olarak yönetebilmektedir.



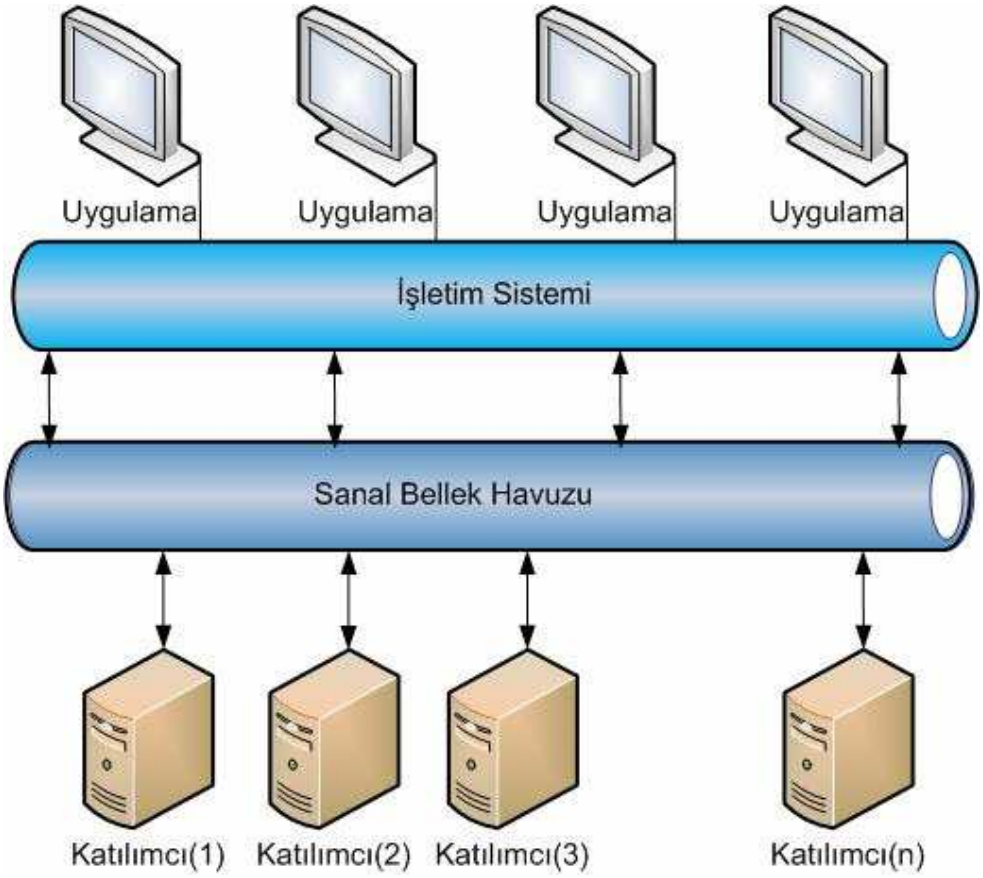
Şekil 5.10: Uygulama Düzeyi Bellek Sanallaştırması

5.3. Süreç Konusunda Öneriler ve Uyarılar

Sanallaştırma projelerinin teknik ekip ve yönetim tarafından iyice değerlendirilip karar verilmesi gerekir. Mevcut altyapının ne kadar sanal ortama geçiş açısından uygun olduğu iyi irdelenmelidir. Sanallaştırma altyapısına geçişin mevcut yatırımları tamamen atıl durumda bırakıp bırakmadığı araştırılmalıdır. Sanal platform için kapasite planlamanın mutlaka gündeme alınması ve gerekirse bu konuda danışmanlık hizmetinin de temin edilmesi gerekmektedir. Benzer projeleri başarıyla tamamlayan diğer kurum ve firma yöneticileri ve teknik ekipleri ile görüşmeler yaparak geri bildirimler alınmalıdır.

Henüz bazı fiziksel ortamlar sunucu, işletim sistemi veya özel ihtiyaçlar için sunucu üzerinde bulunan fiziksel kartlar nedeniyle sanala aktarılamamaktadır. Çok yüksek işlem hacmine sahip uygulama, veri tabanı yönetim sistemleri ve vb. hizmetler sanallaştırıldığında başarım açısından yetersiz kalabilir.

Sanal sistemlerde üzerinde çalışan uygulamaların sanallaştırma kaynaklı farklı sıkıntıları oluşabilir. Bilişim hizmetleri üreticilerinin sanal sistemlere ne kadar destek verdikleri mutlaka araştırılmalıdır. Bazı üreticiler kendi uygulamaları için yine kendilerine ait sanallaştırma çözümlerini pazarlama girişimlerinde bulunabilir ve farklı sanal çözümlere destek vermeyebilirler.



Şekil 5.11: İşletim Sistemi Düzeyi Bellek Sanallaştırması

Ayrıca, sanallaştırma kadar sanallaştırmayı yönetebilmenin de önemli olduğu unutulmamalıdır. Birçok sanallaştırma ürünü olduğunu düşünürsek bunların disk üzerindeki alanlarını ve dosya yapılarını anlayan, yönetebilen araçlar olmalıdır (örneğin, PlateSpin).

Her sanallaştırma ürünü farklı disk imajları kullanırlar. Bu yapı içerisinde sıkıştırılmış imaj bellek üzerinde açılır ve ihtiyaç oldukça kullanılırlar. Sanallaştırma yönetim araçları, sanal makineleri klonlama, yük dengelerinin takibi, otomatikleştirme gibi işler yaparlar. Bu ürünler birbirleri arasındaki geçişi de sağlarlar. Bu ürünlerin en belirgin özelliği, fiziksel bir makineyi sanala sanal bir makineyi de fiziksel bir ortama taşıyabilmesidir.

Birçok sanallaştırma ürünü, disk analizi de yapabilir. Bunun yanında ana bellek üzerindeki alanları da inceleyerek ve gerektiğinde diskler üzerine basarak, sorunlu durumlarda sistemlerin kaldıkları yerden çalışmaya devam edebilmeleri sağlanır. Ancak sanallaştırma yönetim araçları bu alanları bastıkları yerleri disk üzerinde silmezler; bu da adli anlamda önemli bir bilgidir. Bu bilgilerin ayrıca bir ürün tarafından temizlenmesi gerekir.

Sistemleri kendi aralarında taşımak genelde problem olabilir. Bunun sebebi de bellek depolamasının yanında dosya yapıları arasındaki problemdir. Yani bir sanallaştırma yapısının dosya kullanımı ile bir diğerininki birbirinden faklı olduğu için öncelikle ortak bir alana çevrilmesi gerekebilir.

Sanallaştırma sistemleri üzerlerinde çalıştıkları dosya sistemlerinin yeteneklerine bağımlıdır. Bu yüzden formatlanmamış diskler genellikle tercih edilirler. Bir dosyada 4 GB'tan büyük dosya taşıyamayan bir sistemde tüm sistem 4'er GB'lık parçalar halinde tutulmak zorundadırlar. Ortak disk alanlarında işlem yapılacaksa bunun için taşıyıcı sistemin dosya sistemi yetenekleri devreye girer ki bununla ilgili olarak disk küçültmesi ya da büyütülmesi (LVM, OCFS2 vb.) durumunda sanallaştırma diskleri üzerinde çalışan sistemler bunlardan etkilenmezler.

BÖLÜM 6.

UYGULAMA ALANLARI

Sanallaştırma sayesinde bilişim kaynaklarının yönetiminde ve esnekliğinde daha büyük bir başarıya ulaşılmıştır. Sanallaştırma farklı işletim sistemlerine sahip olabilen birden çok sanal makinenin birbirlerinden yalıtılmış şekilde aynı fiziksel makine üzerinde çalışabilmesine olanak sağlar. Bu nedenle öncelikle sunucu sanallaştırması olmak üzere birçok alanda kullanılabilmektedir.

6.1. Sanallaştırabileceklerimizden misiniz?

Sanallaştırmanın uygulanamayacağı bir ortam veya koşul yoktur. Ancak Sanallaştırmanın uygulanabilir olması mutlaka uygulamaya alınmasını gerektirmez. Bazı durumlarda sanallaştırmaya geçmek avantajlı olmayabilir.

Birden fazla sunucuda, kullanılan farklı uygulamaların kendi sunucularındaki mevcut kaynakların çok az bir dilimini tüketmesi, geriye kalan kaynakların boşta durması durumunda; uygulamalar farklı işletim sistemi ya da ara yazılım gerektiriyor olsalar bile, bunları tek bir sunucuda yan yana işletmek daha verimli olacaktır. Bu durumda sunucu sanallaştırması kullanılabilir.

Ayrıca, sanallaştırma, uygulama geliştiriciler için uygulamalarını farklı işletim sistemi konfigürasyonlarında kısa bir sürede test ederek karşılaştırmalarını yapabilmelerini sağlar.

Sanal makinelerin hayatımıza girmesiyle birlikte, farklı güvenlik yaklaşımlarının ve farklı bilişim sistemleri yönetim anlayışının oluşması da beklenmelidir. Sanal platformlara geçiş aşamasında mevcutta çalışan ve herkesçe kabul gören standart sistem yapılarından çok daha farklı bir yapıya geçildiği unutulmamalıdır.

Sanal platformların tercih edildiği durumlarda artık fiziksel ortama geriye dönüşün oldukça zor olduğu da göz ardı edilmemelidir. Sanallaştırma ile beraber ayrı ayrı bağımsız olarak çalışan sunucular daha az sayıda sunucuda çalışmaya başlamaktadır. Fiziksel yapıda her sunucu iş sürekliliği açısından kendi riskini taşırken sanallaştırma ile beraber bir sunucu birden fazla sunucunun riskini almaya

başlamaktadır. Bu risklere karşın yeni teknolojik çözümler olsa da, bunlar farklı maliyetler olarak karşımıza çıkabilmektedir.

Bir kurum veya kuruluş, bu bölümde bahsedilen kullanım amaçlarından herhangi birini elde etmek için, BT altyapısında sanallaştırma çözümlerine yönelik değişimlere gitmeye karar verebilir. Örneğin; bir kuruluş, hayati servis veya uygulamalara yönelik olarak süreklilik oranlarını yüksek seviyelere çıkartmak veya çevreci bilişim gibi toplumsal kazanımlara katkıda bulunmak veya felaketten kurtarma senaryosu hazırlamak isteyebilir. Tabi olarak, sanallaştırma çözümlerini uygulamanın bir maliyeti olacaktır ancak varılmak istenilen hedefe ulaşmak için bu tip giderlerin önde tutulmadığı durumlar olabilecektir.

Bununla birlikte, asıl amacın sanallaştırma çözümlerini kullanarak BT altyapısını yeniden yapılandırmak ve konsolide etmek (kısacası, kuruma ait veri merkezini sanallaştırmak) ve böylece toplam sahip olma maliyetindeki artışı durdurmak ve mümkünse düşürmek olduğu durumda, bu çözümleri uygulamanın maliyeti göz önünde tutulması gereken etkenlerden biri olacaktır. Bu maliyet ise, oluşacak sistemde yaşanabilecek başarım düşüşleri de dahil olmak üzere farklı şekillerde karşımıza çıkabilmektedir.

Tüm bunlar dikkate alındığında ise, sanallaştırmaya geçiş konusunda karar verebilmek için bazı ölçütlerin göz önünde tutulması gerektiği sonucu ortaya çıkmaktadır ve bu bölümde bu ölçütlerin önemli görülen bir kısmı ele alınmaya çalışılacaktır:

- Sunucu sanallaştırmasını uygulanacak sunucu sayısı ne kadar fazla (örneğin, birkaç yüz veya daha üzerinde) ise, sanallaştırmanın o oranda fazla yararının görüleceği açıktır. Çok az sayıda (örneğin, birkaç adet) sunucunuz varsa da, sanallaştırmaya geçiş için yapılacak edinim ve kurulum masrafları, elde edilecek yarar tarafından karşılanmayabilir.
- Sanallaştırmada, fiziksel sunuculardaki atıl bekleyen kaynakların diğer sunucular/uygulamalar ile paylaşımının en yüksek seviyeye ulaştırılması hedeflenmelidir. Bu kapsamda, aşağıda 3 başlıkta toplanan fiziksel sunucu sistemlerinin sanallaştırılması, sanallaştırmadan alınacak verim artışını sağlayacaktır ve sanallaştırmayı daha anlamlı kılacaktır:
    - Farklı kaynakları yoğun bir şekilde kullanan fiziksel sunucu sistemlerini aynı çatı altına toplamak (örneğin, çok işlemci az bellek kaynağı, diğer taraftan da çok bellek az işlemci kaynağı kullanan sunucuların sanal ortama taşınması gibi).

- Farklı zaman dilimlerinde yoğunluk yaşayan fiziksel sunucu sistemlerini aynı çatı altına toplamak (örneğin, bir uygulama ayın sadece 10-15'i, diğeri ise 25-30'u arasında yoğun kullanılan sunucuların sanal ortama taşınması gibi).
- Çok yoğun kaynak tüketmeyen fiziksel sunucu sistemlerini aynı çatı altına toplamak (örneğin, işlemci ve bellek oranlarını atıl kullanan sunucuların sanal ortama taşınarak birleştirilmesi gibi).

- Mevcut sunucular, özellikle işlemci ve bellek kullanımı açısından genelde yüksek doluluk oranlarında (örneğin, %70-80 veya üstü) çalışıyorsa, sunucuları sanallaştırmanın çok fazla bir yararı görülemeyebilir. Sanallaştırma, yukarıda değinilmeye çalışıldığı üzere, atıl kalmış kaynakları kullandırmaya başladığında daha anlamlı olacaktır.
- Henüz ömrünü doldurmamış olan sunucuların bir bölümü veya tümü, donanım yapısı olarak sanallaştırmaya uygun değilse, sanallaştırmaya hemen veya bir bütün halinde geçilmesi zorunlu değildir. Zaman içinde, ömrünü tamamlayan sunucular yenilenirken, sanallaştırmaya da kademeli olarak geçilebilir.
- Kritik bir BT kaynağına (uygulama, veri, vb.) ilişkin güvenlik politikası, o kaynağın fiziksel güvenliğe dayanıyorsa, o kaynağın dayandığı altyapının sanallaştırması güvenlik politikasına aykırı bir durum oluşturabilir.
- Veri merkezinizi sanallaştırmadan önce, sanallaştırma konusunda yeterli eğitimlerle donatılabilecek ve böylece sanallaştırılmış sistemleri yönetebilecek seviyede sistem yöneticilerin bulunduğuna emin olunmalıdır.
- Sunucu sanallaştırması ile, az oranda işlemci kaynağına gereksinim duyan sanal sunucuları aynı fiziksel sunucu üzerinde toplamak mümkün olabilecektir. Böylelikle, aynı işlemciyi paylaşabilecekler ancak bellek gereksinimlerinde bir değişiklik olmayacaktır. Bu nedenle, sunucuların sahip bulunduğu bellek kapasiteleri çok yüksek değilse, sanallaştırmaya geçtikten sonra başarım kayıpları yaşanabilir.
- Kullanıcılar, coğrafi olarak dağıtık bir yapı sergiliyorsa, ADSL gibi standart bir İnternet bağlantısına güvenerek masaüstü sanallaştırma gibi, son kullanıcıların merkezle sürekli iletişim içinde kalmasını gerektirecek

çözümleri uygulamak, iletişim hatlarında sorun yaşandığı zamanlarda büyük sorunlara neden olabilir.

- Tüm BT altyapısı sanallaştırılmak zorunda değildir. Kurumun ihtiyaçları göz önünde bulundurularak sanallaştırma kapsamına karar verilebilir.
- Sanallaştırılmış altyapı üzerinde çalışamayacak özel bir uygulama varsa, bu uygulama ve üzerinde oturduğu kaynaklar sanallaştırılmamalıdır.
- Bunların dışında, sanallaştırma uygulandıktan sonraki durum düşünülmelidir. Gerekli maliyetler ve giderler hesaplanmalı; öncesi ve sonrasına ilişkin mali portreler karşılaştırılmalıdır. Burada, kullanılacak sunucu sayısı, veri merkezinin elektrik tüketimi, soğutma işlemleri, sistemlerin bakımından ve yönetiminden sorumlu kişi/kişilerin eğitimi ve temini, kullanılacak olan yazılımların uyumluluğu ve lisanslamaları konularındaki maliyetler ve giderler hesaplanarak, sanallaştırmanın maliyet açısından ne getireceği tespit edilebilecektir.
- Ayrıca, aşağıdaki durumlardan biri veya birkaçı söz konusu olduğu durumlarda, söz konusu sanallaştırma çözümünün, gereksinimi bir teknik veya başarımla ilgili soruna neden olmadan uygulanabileceğine emin olma noktasına özen göstermek gerekecektir:
    - Altyapı katmanların sanallaştırılmasından etkilenebilecek özel gereksinimlere sahip bir uygulama varsa;
    - Kümeleme (clustering) gereksinimi olan bir veritabanı sunucusu varsa; fiziksel sunucuda bir hata ortaya çıktığında onun yerini alacak (fail-over) bir sunucu varlığı söz konusu ise;
    - Yüksek başarım veya yüksek servis kalitesi (QoS) gereksimi olan özel bir uygulama varsa;
    - Uygulamanın bellek veya veri deposu gereksinimi çok yüksek ise;
    - Standart dışı bir sunucu yazılımı, uygulama vb. kullanılıyorsa.

6.2. Sanallaştırmanın Uygulama Alanları

Sağladığı ekonomik tasarrufu, iş yükü tasarrufu, mekan tasarrufu gibi avantajlarıyla sanallaştırma kamu kurum ve kuruluşlarının Bilişim Teknolojileri birimlerinde, felaketten kurtarma alanında, test ve araştırma ortamlarında, adli

incelemelerde, bilgi teknolojileri güvenliği alanında, barındırma hizmetlerinde, bulut bilişimde, taşınabilir sistemler oluşturmak amacıyla kullanılabilir.

6.2.1. BİB'nin Yeniden Yapılandırılması

Teknolojik ömrünü tamamlamak üzere olan ya da başka nedenlerle sunucuların yenilenmesi gereği ortaya çıkmış BİB'ler, yenilenme sürecinde sanallaştırma yöntemini kullanarak fiziksel sunucu sayısını azaltabilir, mekansal olarak rahatlama sağlayabilir, yönetimi kolaylaştırabilirler. Yenilemeden önce verilen hizmet, sunucu tarafından zorlanmadan veriliyorsa, yenilenecek olan sunucu hizmet için çok daha yeterli olacak ve kullanılmayan kaynakları boşa gidecektir. Bu gibi durumlarda eski hizmetlerin yeni sunucularda toplanması ekonomik olarak avantaj sağlayacaktır. Daha az sayıda sunucu alınacağı için mekansal kazanım olacaktır. Sanal makinelerde çıkan sorunlar fiziksel makinelerde çıkan sorunlara göre daha hızlı yönetilebilecektir. Bu da yönetim kolaylığı sağlayacaktır.

6.2.2. Felaketten Kurtarma

Symantec Felaket Kurtarma Araştırması'nın Türkiye bulgularına[3] göre; sistem çökmeleri, veri kayıpları (%64) ve virüs (%76) gibi birtakım tehditler Türkiye'de yer alan şirketler için başlıca üç sorun olarak ifade edilmektedir. Araştırmaya katılan kurumların %70'i, bilgisayar sistem çökmeleri (yazılım ve donanım) yaşadıklarını belirtirken, %52'si ise bu gibi çökmelerin sonucunda kendi felaket kurtarma planlarını uyguladıklarını ifade etmektedirler. Araştırmaya katılan kurumların %70'i zararlı yazılım (malware) ve güvenlik saldırısı aktiviteleri gibi tehditlere maruz kaldıklarını belirtirken, %54'ü ise bu gibi durumların sonucunda kendi felaket kurtarma planlarına başvurduklarını vurguluyor.

Sanallaştırma yaklaşımları, felaketten kurtarma senaryolarının ortaya konulmalarını kolaylaştırmaktadır. Sanallaştırma teknolojileri kullanıldığında, felaketten kurtarma merkezinde kullanılacak olan donanımların, felaketten kurtarma planı yapılacak olan diğer donanımlarla aynı özelliklere sahip olmak zorunluluğu da ortadan kalkmaktadır.

6.2.3. Sınama ve Araştırma Ortamları

Kum havuzu (sandbox) oluşturma, bir uygulamanın kendisine verilen kısıtlı erişim yetkileri dışına çıkması engellenerek davranışının izlenmesi tekniğine verilen addır. Bu tekniğin genellikle bir işletim sistemi üzerinde sanal bir ortam oluşturulması

[3] Symantec Felaket Kurtarma Araştırması, http://www.pctime.com.tr/habergoster.asp?id=2630.

ve uygulamanın bu sanal ortam dışına çıkamayacak şekilde çalıştıran uygulamalarını görmekle beraber, sınanacak uygulamanın, üzerinde kurulacağı ortamı temsil edecek sanallaştırılmış kopyası üzerine kurularak davranışlarının analiz edilmesi de bir kum havuzu uygulaması olarak görülebilir. Birçok güvenlik ürünü zararlı içeriklerin tespitinde doğrudan üzerinde çalıştığı işletim sisteminde bir çeşit sanal ortam oluştururken, kurumlarda uygulamaların sanal makineler üzerinde test edildikten sonra gerçek ortamlarına alınıp alınmayacaklarına karar verilmesi de bu kapsamda değerlendirilebilmektedir.

6.2.4. Adli İnceleme

Sanallaştırma adli incelemelerde çeşitli alanlarda ve yöntemlerle kullanılabilmektedir. Sanallaştırma adli bakımdan fiziksel olarak taşıma, muhafaza, erişilebilirlik gibi güçlüklerin üstesinden gelebilmek için fiziksel olarak kişisel bilgisayarların ya da sunucuların taşınması (içerisinde bulunan bilgilere ihtiyaç duyulması halinde) yerine hızlı bir şekilde sanalının alınması ve sonrasında adli incelemelerde kullanılması olanağı sağlayabilir. Aynı zamanda donanım bağımsız çalıştırılabileceği için birçok işletim sistemi üzerinde çalıştırılıp gerekli bilgilere kolayca erişilebilecektir. Bilgisayar ya da sunucuların farklı şehirlerde incelenmesi gerektiğinde, fiziksel hiçbir taşıma işlemine gerek kalmadan, teknik olarak erişim olanağını da sağlayabilecektir.

6.2.5. Bal Küpü ve Bal Küpü Ağları Oluşturma

Saldırganların kullandıkları yöntemler ve araçların tespit edilmesi için (genellikle) İnternet erişimine açık ve mümkün olduğunca normal bir sunucu herhangi bir ek güvenlik önlemi alınmadan bırakılır. Bal küpü olarak adlandırılan bu sunucunun saldırganlar için rahatlıkla tespit edilebilmesi önemlidir. Bu şekilde tek bir sunucu yaratılmasının da ötesinde benzer mantıkta bir ağ yaratmak ve saldırganların bu ağ içinde ne şekilde davrandıklarını tespit etmek mümkündür. Bu amaçla yaratılmış ağlara ise bal küpü ağları denilmektedir. Sanallaştırmanın getirmiş olduğu olanaklar ile bu tip sunucular ve ağların yaratılması günümüzde çok kolaylaşmıştır. Tek bir fiziksel makine içinde bile bu tip sanal ağlar ve sunucu kümeleri çok rahatlıkla oluşturulabilmektedir [25].

Diğer yandan, bal küpleri sanallaştırma platformları üstünde çalışması durumunda güvenlik unsurlarına dikkat edilmelidir. Bu tür platformlarda çalışan bir bal küpünün bir saldırgan tarafından algılanamaması kritik bir öneme sahiptir [33]. Bir bal küpünü ele geçiren saldırganın işlemci ve bellek kullanım değerlerini inceleyerek bilgisayarın bir sanal bilgisayar olduğunu anlaması mümkün

olabilmektedir [34]. Kasım 2008'de Honeypots haber grubunda[4] sanal bilgisayarların bal küpü mimarisinde kullanılmasıyla ilgili bir tartışma gerçekleşmiştir. Bu tartışmada, sanal bilgisayarların gün geçtikçe yaygınlaşmasına paralel olarak ele geçirilen bir sanal bilgisayarın bal küpü olması yönünde verilecek bir kararın zorlaşması yönünde yorumlarda bulunulmuştur. Sanallaştırma çözümlerinin kullanımı hakkında tartışmalar olmasına devam etmekte olup tam olarak geçerli bir çözüme henüz ulaşılamamıştır. Bal küplerinin saptanması konusunda yapılan bir diğer çalışmada iki yöntemden bahsedilmektedir [35]. İlk yöntemde, yüksek etkileşimli bal küplerinde kullanılan ve saldırganın hareketlerini izlemeye yarayan Sebek yazılımının nasıl saptanacağı üzerinde durulmuştur. İkinci yöntemde ise düşük etkileşimli bal küpü Honeyd'nin öykündüğü servisler üzerinden bir saptama yapılmıştır. Honeyd, servisleri kısıtlı olarak öykündüğü için, saldırganın bu servisleri saptama imkânı bulunmaktadır. Çalışmada Honeyd'nin hatalı öykündüğü bir servisten hareketle bal küpü saptamasında bulunmuştur. Bu çalışma, benzeri saptamaların yapılabileceğine bir örnek teşkil etmektedir.

6.2.6. Barındırma Hizmetleri

VPS (Virtual Private Server), küçük ölçekli sunucu ihtiyaçlarını karşılamak üzere üretilmiş, kişi ya da organizasyonlara özel sanal sunucu teknolojisidir. VPS mimarisi, bir fiziksel sunucunun üzerinde birden fazla sanal sunucu barındırarak yatırım ve işletme maliyetlerini düşürmeye ve maksimum fiyat/başarım oranı sağlamaya yönelik bir yapıdır.

VDS (Virtual Dedicated Server) hizmeti ise, üzerinde özellikle yoğunlukları nedeniyle paylaşımlı barındırma servislerini kullanamayan web siteleri, orta ölçekli e-posta sunucuları ve yüksek trafikli forumlar gibi yoğun uygulamaları barındırmaktadır. Ayrıca, her VDS'in kullanımına özel ve tamamen adanmış (paylaşımsız) olarak ayrılmış belirli bir işlemci gücü, bellek kapasitesi ve sabit disk alanı gibi sistem kaynakları ile sağlanmaktadır. Bu sayede bir sunucu üzerinde çalışan tüm VDS sunucular, VPS sistemlerinden farklı olarak birbirlerinden tamamen ayrılmakta ve maksimum başarım elde edilmektedir. Tüm VDS sunucular kendi işletim sistemlerine sahiptir ve teknik olarak fiziksel bir sunucudan farklı hiçbir yönleri bulunmamaktadır. Barındırma hizmeti veren firmalar, web barındırma hizmeti kapsamında, çok sayıda web sitesini aynı sunucu üzerinde barındırmaktadırlar. Web uygulamaları aynı web sunucu programını, aynı veritabanı uygulamasını paylaşırlar.

[4] Honeypots haberlesme grubu, http://seclists.org/honeypots/2008/q4/0012.html.

Standart bir yazılım altyapısı paylaşıldığı için, web uygulamalarının bu standartlara uyması gerekmektedir. VPS ise tamamen kişi veya kuruma özel bir sunucu ortamı sağladığı için, ihtiyaca uygun donanım ve yazılım altyapısını kurum belirlemekte ve istediği gibi önceliklendirme ve değişiklik yapabilmektedir. İhtiyaçları doğrultusunda sunucu kaynaklarını arttırmak ya da azaltmak her zaman mümkün olabilmekte ve bu işlem sanal sistemlerde oldukça hızlı olmaktadır. Web barındırma ve sunucu hizmeti sağlayıcıların bu hizmetleri daha güvenli ve kişi ya da kuruma özel verebilmeleri için sanallaştırma platformu kullanmaları oldukça yerinde olacaktır.

6.2.7. Bulut Bilişim

Bulut Bilişimi, bilişim kapasitesinin İnternet üzerine kaydığı, kullanıcıların, ortak kaynak, yazılım ve bilgiye diledikleri zaman diledikleri yerden ulaşabildikleri bir yaklaşım olarak özetleyebiliriz. Bulut Bilişim tarafında sunulan servis tiplerini şöyle sıralayabiliriz: Son kullanıcılara hitap eden yazılım servisleri (GoogleDocs, Google Calendar, Yahoo Mail vb.); Bulut yapıları için yazılım geliştirmek isteyenlere sunulan platform servisleri (GoogleApps) ve sunucu, ağ cihazları, veri depolama alanları vb. olanaklara gereksinim duyanlara sunulan altyapı servisleri. Bulut Bilişim tarafından sunulan servislere erişim için özel bir kurulum gerekmez; İnternet'e erişim için kullanılan araçlar, bu servislere erişim için yeterli olmaktadır. Ayrıca, eğer bir ücretlendirme söz konusu ise, bu servisleri kullananlar, kullandıkları oranda ödeme yaparlar.

Sanallaştırma, Bulut Bilişim için oldukça önemli yapı taşlarından birini oluşturur. Öncelikle, bulut yapıları tarafından sunulan altyapı servisleri, tipik olarak sanallaştırılmış bilişim kaynakları olarak karşımıza çıkarlar: Sanal sunucu, sanal ağ anahtarı, sanal veri depolama alanı vb. Ayrıca, teknik anlamda bir zorunluluk olmamakla birlikte, Bulut Bilişimin kendi altyapısının büyüklüğü düşünüldüğünde, bu çaptaki bir altyapının (dev veri merkezlerinin) sanallaştırılmış olmasının pratik yararları açıkça görülebilecektir.

6.2.8. Taşınabilir Sistemler

Mobil sanallaştırma masaüstü sanallaştırmasının mobil cihazlara uygulanmış hali olarak özetlenebilir. Desteklenen mobil cihazlarda alt kısma bir mobil yönetici koyarak birden fazla işletim sistemi çalıştırmaya yarar. Bu yapı kullanıldığı zaman kullanıcılar iş ve kişisel uygulamalarını ayırabilir veya farklı müşteriler için tamamen farklı sistemler ile tek cihazdan hizmet sunabilir. Bu sistemlere örnek olarak VMware Mobile Virtualization Platform verilebilir. Bu sistem ARMv4'den ARMv7 'ye kadar olan tüm işlemcilerde çalışır ve popüler olan Android, Symbian OS, Linux,

Windows CE, eCos, uITRON gibi işletim sistemlerini destekler. Bunun yanında Citrix firması yazılan uygulamaları çeşitli mobil araçlar için yorumlayarak çalışabilir hale getirebilmektedir, ancak yorumlar bazı sistemlerde ve yerelleştirmelerde sorunlar olduğunu belirtmektedir.

Bunun yanında mobil platformlarda VNC'ye eşdeğer bir yapı da bulunmaktadır. Çoğu mobil platform üzerine kurulabilecek bir VNC sunucusu yardımı ile uzaktan erişilebilir hale gelebilmektedir. Bunun yanında bu platformlar VNC istemcisi olarak da çalışarak tam donanımlı bir masaüstü bilgisayarını da uzaktan kumanda etmek amacı ile de kullanılabilir.

BÖLÜM 7.

BİLGİ İŞLEM BİRİMLERİ VE SANALLAŞTIRMA

Bu bölümde, Bilgi İşlem Birimlerinin (BİB) sanallaştırmaya bakışı ve geçişi açısından Dünya'daki ve Ülkemizdeki durum, Ülkemizden sanallaştırmayı uygulayan kamu kurum örnekleri ile sunulmaya çalışılmaktadır.

7.1. BİB'ler Açısından Durum

1960'larda başlayan sanallaştırma fikrinin, sanallaştırmayı sağlayan yazılım ve destekleyen donanım ürünleri ile birlikte, bugün artık BT pazarında giderek daha fazla söz sahibi olmasını sağlayacak olgunluk seviyesine erişmiş olduğu görülmektedir. İlgili ürünlerin, satış ve kullanımlarındaki artış ve sanallaştırma uygulayan kurum ve kuruluşların sayılarındaki yükselme, bu gerçeği kanıtlamaktadır.

7.1.1. Dünya'da Durum

Dünyadaki gelişmeler, ekonomik zorluklar, teknolojilerin sürekli değişmesi, her geçen gün daha karmaşıklaşması, çalışanların, kurumların, bireylerin bilişim teknolojilerine olan gereksinimlerinin ve bağlılıklarının artması birçok yeni gelişmenin yanında zorlukları da getirmektedir. Yönetimsel zorluklar bunun en başlıca sonuçlarından birisidir.

Bu şekilde gelişen ve değişen bir dünyada çevik bir altyapı ihtiyacı kaçınılmazdır. Çevik bir altyapı denildiğinde ise, maliyetleri düşüren, riskleri yönetebilen ve hizmet kalitesini yükselten bir yapıdan bahsedilmektedir. İş stratejilerindeki değişime ayak uydurabilmesi gerekmektedir.

Çevik bir altyapıda şu bileşenlerden bahsedilmektedir:

- Bilgi (veya bilişim) altyapısı (Information Infrastructure),
- Sanallaştırma,
- Varlık yönetimi (asset management),
- Verimli enerji kullanımı (energy efficiency),
- Güvenlik,

- Esneklik (business resiliency),
- Sistem yönetimi.

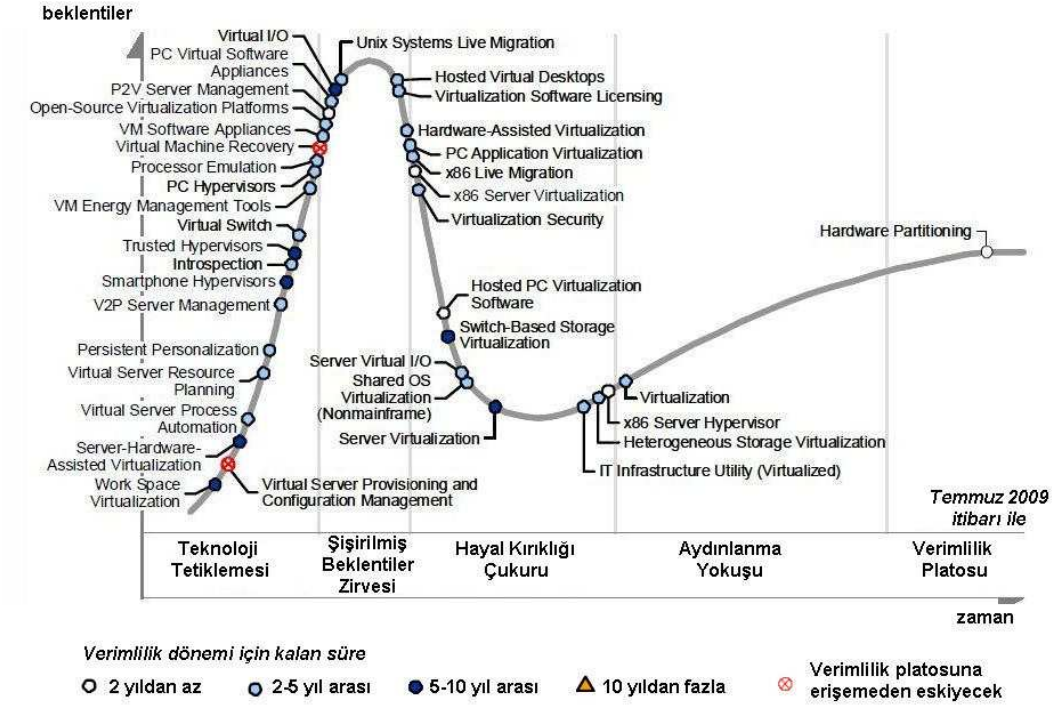
Sanallaştırma çevik altyapı için önemli bir bileşendir. İş ortamında çeviklik, esneklik, güvenlik, enerji verimliliği ve maliyet hassasiyetlerinin derecesine göre bakacak olursak farklı çözümler seçilebilir.

Sanallaştırma teknolojileri ve süreçleri konusunda Gartner Group tarafından Beklenti Döngü (Hype-Cycle) eğrisi yayımlanmıştır [36]. Herhangi bir yenilik veya teknolojik gelişim hakkında kamuoyunun beklentilerini gösteren eğri vasıtası ile, özellikle konu hakkında yatırım kararı alan kurum ve kişilere yol göstermesi hedeflenmektedir. Eğrinin dikey ekseni beklenti oranını yansıtırken yatay eksen temel olarak beş bölüme ayrılmış yakın zamanı göstermektedir. Zamanın ilk bölümü teknolojinin veya yeniliğin tetiklendiği ve beklentilerin oluşmaya başladığı dönemdir. İkinci bölüm beklentilerin en üst noktaya ulaştığı zaman aralığını göstermektedir. Daha sonra birtakım beklentilerin boşa çıktığı bir hayal kırıklığı dönemi başlamaktadır. Yeniliklerin olgunlaşmaya başladığı aydınlanma yokuşu döneminin ardından gerçek verimin alındığı verimlilik platosuna ulaşılmaktadır.

Şekil 7.1'de 2009 yılında hazırlanan Sanallaştırma Beklenti Döngü eğrisi sunulmuştur. Eğride de görüleceği gibi, sanallaştırma teknolojisinin uygulandığı alanların büyük bir bölümü henüz birinci ve ikinci aşamadadır. Başka bir ifade ile, beklentilerin çok üst düzeyde olduğu bir dönemde bulunmaktadırlar. Özellikle sanal masaüstü, donanım destekli sanallaştırma, sanal yazılım gibi alanlar beklentilerin yüksek olduğu alanlar olarak göze çarpmaktadır. Gartner Group raporuna göre birtakım sanallaştırma türlerinin henüz teknolojinin tetiklendiği bu ilk aşamada, son aşama olan verimlilik platosuna ulaşamadan eskiyeceği iddia edilmektedir. "Sanal makine hatadan kurtulma" bu tipte bir alan olarak belirtilmektedir.

X86 sunucu sanallaştırması, sunucu destekli masaüstü sanallaştırma yazılımı gibi uygulamaların iki yıl içerisinde; sanallaştırma güvenliği, donanım destekli sanallaştırma, yazılım lisanslamanın sanallaştırılması, sunucu sanal girdi-çıktı gibi birçok alanın ise 2 ila 5 yıl arasında verimlilik platosuna ulaşması öngörülmektedir.

Sanallaştırılmış BT altyapı araçları, heterojen depolama sanallaştırma ve x86 sunucu gözetimi gibi konular hayal kırıklığı çukuru aşamasını atlatarak aydınlanma yokuşu zaman dilimine geçmişlerdir. Yaklaşık 5 yıl içerisinde bu alanların verimlilik dönemine ulaşması beklenmektedir. Sanallaştırmanın tüm alanları arasında sadece donanım bölümlemesi verimlilik platosunda yer almaktadır.

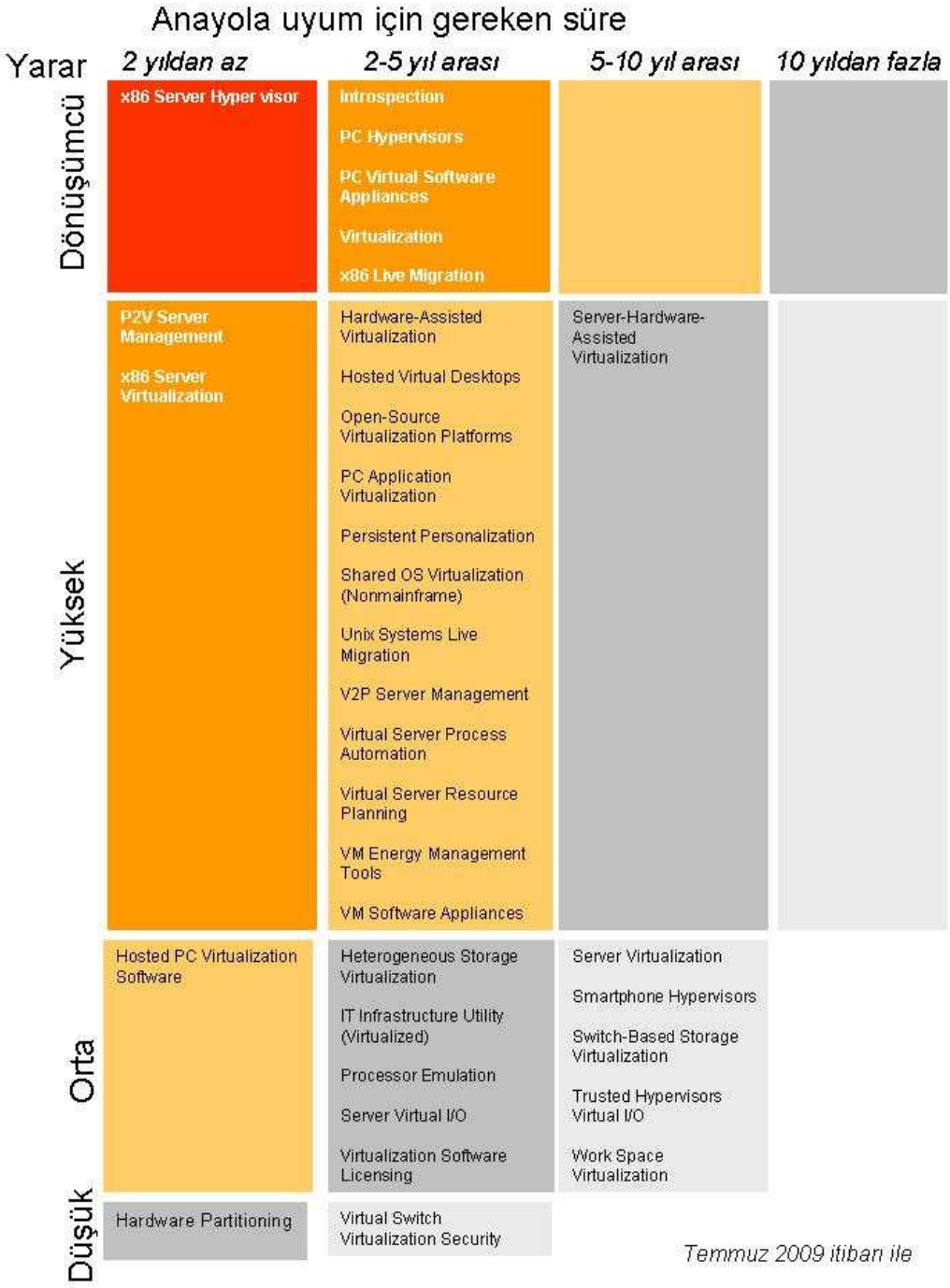


Şekil 7.1: Sanallaştırma Beklenti Döngüsü

Gartner'a göre, sanallaştırma beklenti eğrisi, teknolojinin anlaşılması ve piyasanın beklentisi üzerinde iki önemli dalgayı öne çıkarmaktadır: Sanallaştırmanın geçiş aşamasını ve olgunlaşmasını bir süreç olarak tanımlayan bu dalgalardan birincisi, BT teknik altyapısının konsolidasyonunu desteklemek üzere sanallaştırmanın kullanılmasına işaret etmektedir. X86 sunucu gözetimi, heterojen veri depolama sanallaştırması ve BT altyapısı için sanallaştırma araçlarının kullanımı ile sektördeki sanallaştırma anlayışının artması, getirilerin daha açık olarak görülebilmesini ve dolayısı ile hayal kırıklığı döneminden çıkılmasını sağlamıştır. Bu kapsamda iletişim ağı, güvenlik ve yazılım lisansları, anahtar konular olarak önemli rol oynamaktadır.

Sanallaştırma teknolojisinin anlaşılması ve beklentilerinin ikinci dalgası olarak, sanallaştırmanın olgunlaşmasının ikinci ve üçüncü aşamasına destek olacak alt uygulama alanları ve araçları açısından oldukça zengin bir kümeye sahip olması görülmektedir. P2V sunucu yönetimi, PC sanal yazılım araçları gibi ürünler henüz en yüksek beklenti periyodunda, bir diğer çoğunluğu başlangıç aşaması olan teknoloji

tetiklemesi periyodunda olmasına rağmen önümüzdeki birkaç yıl içerisinde verimlilik dönemine doğru büyüyeceği öngörülmektedir.



Şekil 7.2: Sanallaştırma Öncelik Matrisi

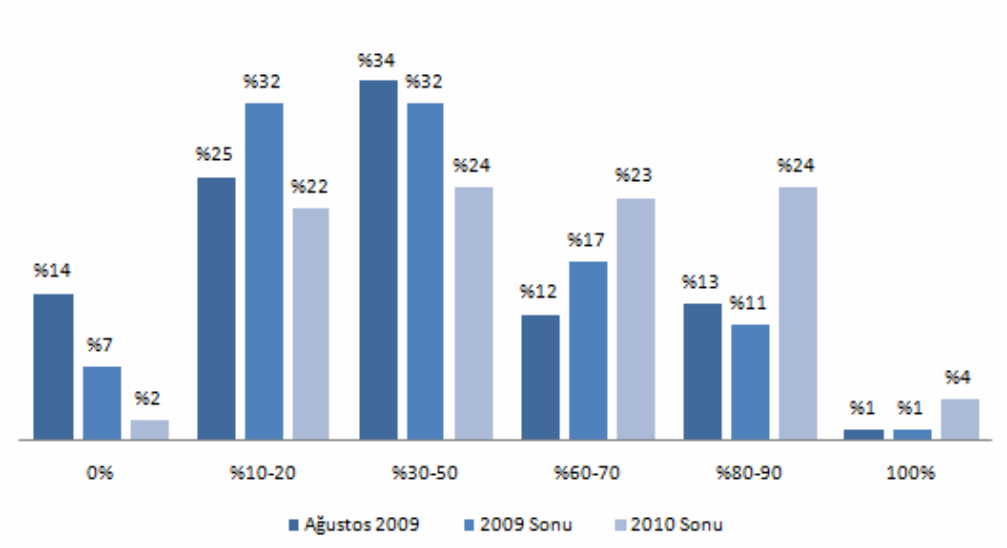
Gartner Group tarafından sanallaştırma konusunda ayrıca Öncelik Matris'i hazırlanmıştır (bkz. Şekil 7.2). Bu matris ile bir teknolojinin anayola uyumu, bir diğer ifade ile verimlilik dönemine geçişi için gerekli süre verilmektedir. Bu sayede karar vericilere sanallaştırma konusunda yatırım yapmaları esnasında rehberlik

edilmektedir. Firmaların genel olarak, matrisin sol üst çeyreğinde verilen ve iş süreçleri, gelir ve tasarruf konularında mevcut ve yakın gelecekte en etkin olabilecek teknolojilere yönelmeleri önerilmektedir. Tabloda da görüleceği üzere sanallaştırma konusunda günümüzde bu gruba x86 sunucu gözetimi, P2V sunucu yönetimi ve x86 sunucu sanallaştırması girmektedir.

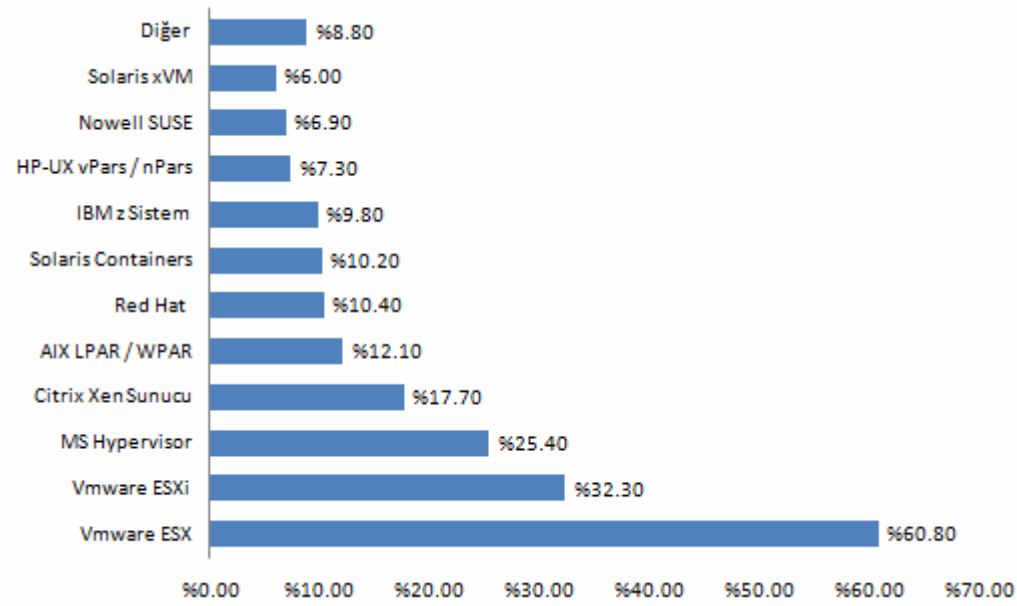
Yine Gartner Group tarafından senelik olarak ele alınan "yılın stratejik olarak tepede yer alan 10 teknolojik alanı" listesinde 2009'dan 2010'a geçişteki fark, sanallaştırma açısından ilgi çekicidir. 2009 yılına ilişkin listede en başta sanallaştırma görülürken, 2010 yılına ilişkin olarak hazırlanmış olan listede ise kullanıcı bilişimi (client computing), çevreci bilişim ve erişilebilirlik için sanallaştırma alanları yer almaktadır [37]. Bu sıralanan alanların her üçü de, sanallaştırmayı temel alan ve sanallaştırma üzerinden uzanılan yaklaşımlar içermektedir.

Sanallaştırmanın BİB'ler tarafından kullanılma (bir başka deyişle Sanal Veri Merkezine dönüşme) oranı ve durumu hakkında birçok araştırma yapılmış olduğu görülmektedir. Örneğin, 2009 yılının Ağustos ayında Centrify Corporation tarafından bağımsız bir kuruluşa yaptırılmış olan ve 500 civarında BT temsilcisinin katıldığı araştırma, en geniş örneklerden biri olarak sayılabilir [38]. Bu araştırmanın bazı önemli sonuçları şu şekilde özetlenebilir:

- Anketin yapıldığı sırada, katılanların %26'sı sunucularının en az yarısını sanallaştırdıklarını söylemelerine karşın; 2010 yılı sonuna kadar bu konumda olacaklarını belirtenlerin oranı ise %51'dir (Şekil 7.3).
- Anketin yapıldığı tarihte sanallaştırma uygulamakta olduklarını söyleyenlerin oranı %91 iken; 2010 yılı sonunda sanallaştırma uygulamakta olacaklarını belirtenlerin oranı ise %98'dir.
- Sanallaştırma için kullanılan ürünler büyük kısmı VMware ismini taşımaktadır. Bunu, Microsoft ve açık kaynak kodlu Xen projesine dayalı Citrix ürünleri izlemektedir (Şekil 7.4). Bunun yanında, ankete katılanların yalnızca %38'i tek markaya dayalı çözümleri kullanmakta olduklarını belirtmişlerdir. Yani, heterojen çözümlerin kullanımı oldukça yaygın olarak ortaya çıkmaktadır.

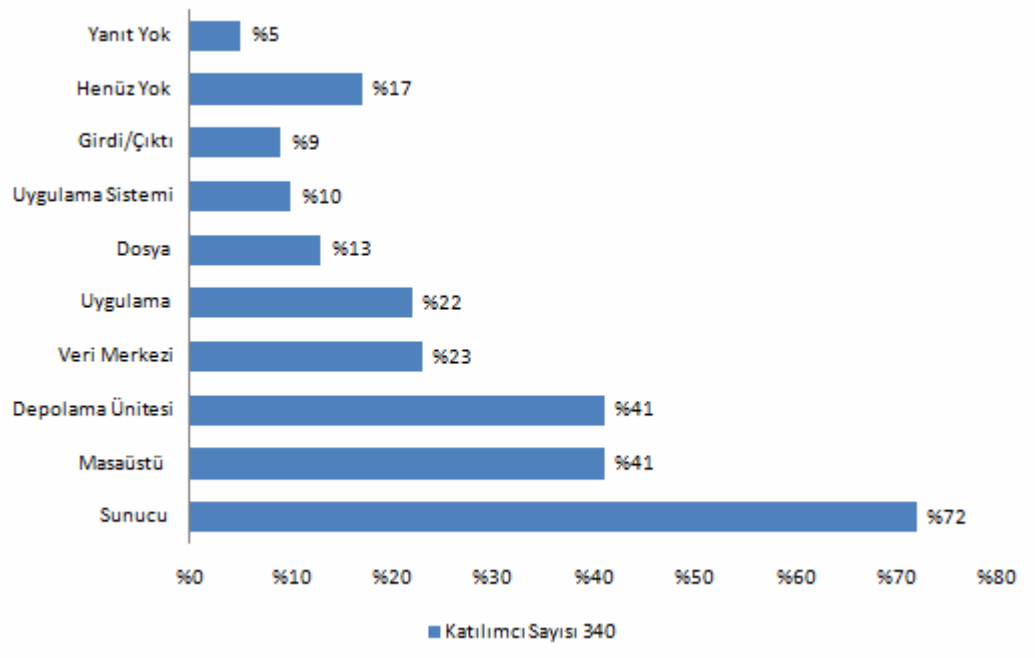


Şekil 7.3: Sunucuların Sanallaştırma Oranlarının Durumu ve Beklentiler



Şekil 7.4: Kullanılan Sanallaştırma Ürünü

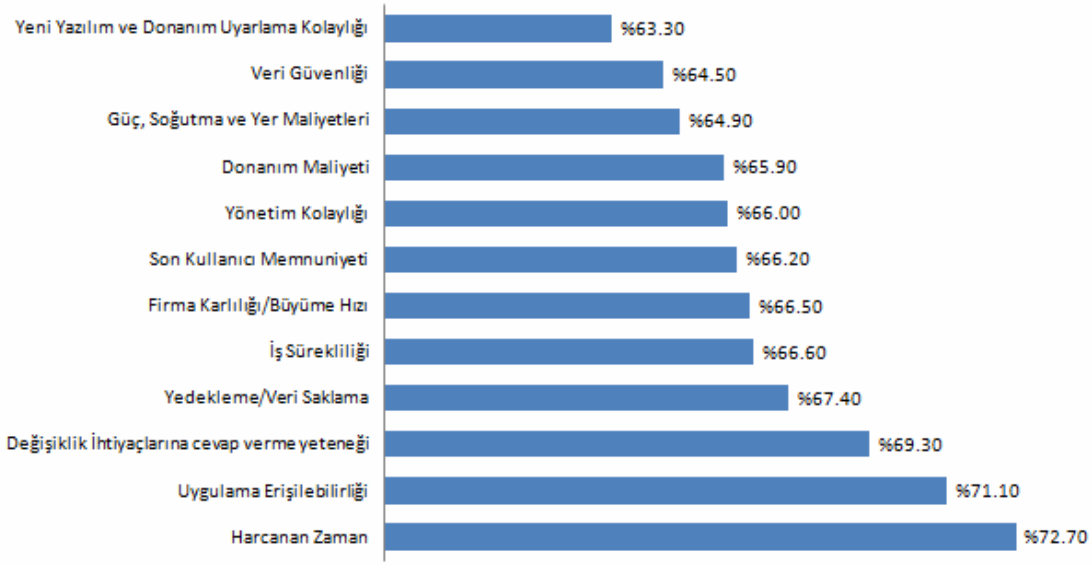
Bu araştırma daha çok sunucu sanallaştırmasını baz almasına rağmen, verdiği sonuçlar sanallaştırmanın ulaşmakta olduğu yönü göstermesi açısından önemlidir. Yine de, diğer sanallaştırma tiplerinin uygulanma durumu hakkında bilgi, IDG Araştırma Servisleri Grubunun ilgili çalışmasında görülebilmektedir [39]. 340 kişi ile yapılan bu anket çalışmasında, sunucu sanallaştırmasının ardından, masaüstü sanallaştırması, veri depolama sanallaştırması gibi diğer sanallaştırma tiplerinin de yaygın olarak kabul görmekte ve kullanılmakta olduğu görülmektedir (Şekil 7.5).



Şekil 7.5: Gerçekleştirilen Sanallaştırma Yatırımları

Bir başka araştırma ise, VMware tarafından 2009 yılının Eylül ayında, ABD ve Kanada'da bulunan 309 üst düzey veya BT yöneticisinin katılımı ile yapılan anket çalışmasıdır [40]. Bu çalışmanın sonuçları içinde şu bilgiler yer almaktadır:

- Ankete katılan kuruluşların önemli bir kısmı, sanallaştırmanın bir çok açıdan çalışmalarında iyileştirme sağladığını belirtmektedirler (Şekil 7.6).

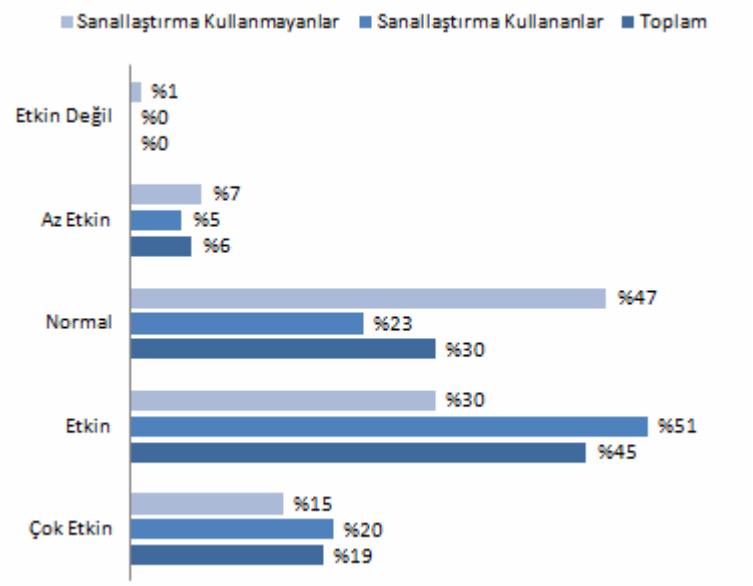


Şekil 7.6: Sanallaştırmanın İyileştirme Sağladığı Konular

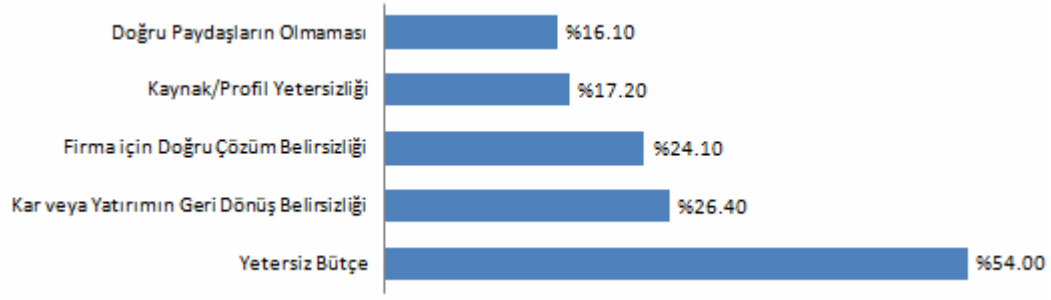
- Kendi BT çalışmalarını etkin bulanlar ile sanallaştırma kullananlar arasında bir bağ olduğu gözlenmektedir (Şekil 7.7).
- Sanallaştırmaya geçişte en büyük engel olarak, yetersiz bütçe kalemi görülmektedir. Bunu, sanallaştırmanın yararlarından ve yatırımın geri dönüşünden emin olamama, doğru sanallaştırma çözümü konusundaki kuşkular vb. izlemektedir (Şekil 7.8).

Ayrıca, ABD'nin bir eyaletinde kamu sektöründeki kurumlar üzerinde yapılan bir araştırmada da, en yüksek yatırım önceliğinin verildiği konunun sanallaştırma olduğu ve bunu az farkla altyapı yatırımlarının izlediği görülmüştür [41].

Sanallaştırma yöntemlerinin uygulanmasına (seçilen uygulama yöntemleri, yaygınlık, öncelik vb.) ilişkin olarak sektörlere göre bir farklılık bulunmadığı değerlendirilmektedir. Sektörlere göre dağılımı temel alan bir anket veya benzeri bir araştırmaya literatürde de rastlanılmamaktadır.



Şekil 7.7: Kendi BT Çalışmalarını Etkin Bulanlar



Şekil 7.8: Sanallaştırmaya Geçişte Engel Olarak Görülen Konular

7.1.2. Türkiye'de Durum

Türkiye'de kamu kurumlarında sanallaştırma çözümleri son dönemlerde merak edilen ve araştırılan bir konu haline gelmiştir. Birçok kamu bilgi işlem birimi bu konuda araştırmalar yapmakta ve farklı üreticilerin ürünlerini inceleme aşamasında bulunmaktadır. Hem sunucu hem de masaüstü sanallaştırması çözümleri teknolojik yeteneklerde hızlı bir şekilde geliştiği ve olgunlaştığı görülmektedir. Hızlı gelişen bu teknolojilerin Kamu kurumlarınca kullanılması ve yaygınlaşması tam tersine yavaş olduğu görülmektedir. Yönetimsel kararlılık ve teknik ekibin hazır bulunuşluk düzeyi sanallaştırma teknolojilerine geçişlerde önem kazanmaktadır. Henüz kamusal alanda bilişim hizmetleri sağlayan teknik birimlerin büyük bir oranı sanallaştırma teknolojilerini daha yeni gündemine almaya başlamıştır. Türkiye'de kamu BİB'nin şu an ağırlıklı olarak odaklandığı ve yatırım yapmayı hedeflediği nokta sunucu sanallaştırması kısmıdır. Ancak sınırlı sayıda olsa da bu konuda belirli mesafe kaydetmiş kamu bilgi işlem merkezleri de mevcuttur. Mevcut yatırımlarını korumak ve hatta bu yatırımlardan nasıl daha etkin faydalanıp aynı zamanda yönetim kolaylığı sağlamayı düşünen kamu bilişim yöneticileri çeşitli arayışlar içerisindedir. Sunucu sanallaştırması altyapısına geçen kurumlar masaüstü sanallaştırması konusunu incelemeye başladıkları görülmektedir.

Sanallaştırmanın Ülkemizdeki durumuna ilişkin olarak yapılmış olan bir araştırma literatürde bulunamamış; bu konuda fikir verebilecek çapta sağlıklı verilerin, BT sektöründe faaliyet gösteren firmalardan alınması da mümkün olamamıştır. Bununla birlikte, tarafımızca yapılan irdelemelerin sonucu olarak, Ülkemizde kendi veri merkezlerinin sanallaştırılması çalışmasını gerçekleştirmiş olan kurum ve kuruluşlarının sayısının henüz onlar mertebesinde kaldığı değerlendirilmektedir. Sayıca az olmasına karşın, ölçek bakımından Avrupa sıralamasında başlarda gelebilecek olan sanallaştırma çalışmalarının Ülkemizde yürütüldüğü ve sanallaştırmaya olan ilginin giderek artmakta olduğu görülmektedir.

7.2. Kamu BİB'lerinde Kullanım Örnekleri

Türkiye'de kamu kurumlarında son dönemlerde ciddi bir merak konusu uyandıran sanallaştırma konusu mevcut projeler incelendiğinde henüz istenilen olgunluk düzeyine gelmiş durumda değil gibi gözükmektedir. Birçok kamu bilgi işlem birimi bu konuda araştırmalar yapmakta ve farklı üreticilerin ürünlerini inceleme aşamasında bulunmaktadır. Henüz kamusal alanda bilişim hizmetleri sağlayan teknik birimlerin büyük bir oranı sanallaştırma teknolojilerini daha yeni gündemine

almaya başlamıştır. Ancak sınırlı sayıda olsa da bu konuda belirli mesafe kaydetmiş kamu bilgi işlem merkezleri de mevcuttur. Türkiye'de kamu BİB'nin şu an ağırlıklı olarak odaklandığı ve yatırım yapmayı hedeflediği nokta sunucu sanallaştırması kısmıdır. Mevcut yatırımlarını korumak ve hatta bu yatırımlardan nasıl daha etkin faydalanıp aynı zamanda yönetim kolaylığı sağlamayı düşünen kamu bilişim yöneticileri çeşitli arayışlar içerisindedir.

7.2.1. Örnek Çalışma: Kurum 1

Türkiye'nin önemli kuruluşlarından olan Kurum 1, faaliyetlerini tüm il ve ilçelere yaygınlaşmış 1000 civarında birimler aracılığıyla sürdürmektedir. Kurum 1, kurumsal bilişim hizmetlerini Yönetim Bilgi Sistemleri Birimi'nin bünyesinde yürütmektedir. Kurumun sunduğu bilişim hizmetlerinin genişlemesine paralel olarak, bilgi sistemleri altyapısının yeniden gözden geçirilmesi ve düzenlenmesi ihtiyacı doğmuştur. Bu ihtiyaç kapsamında; sunucu/istemci altyapısı içinde sorun çözüm sürecinin standart hale getirilmesi ve kısaltılması, daha güvenli bir sunucu/istemci altyapısı oluşturulması, sistemlerin yönetimini sağlayarak oluşacak arızalarda pro-aktif müdahale oluşturulması amaçlarına yönelik olarak kurumda sanallaştırma projesi başlatılmıştır.

Sanallaştırma yapılırken mevcut uygulamalar olduğu gibi taşınmayıp, güvenlik ve başarım politikaları yeniden gözden geçirilerek uygulamaların güncel sürümleri ile yeni kurulumlar yapılmıştır. Sanallaştırma ile hizmet seviyesi başarımında, erişebilirlikte ve ana bellek, işlemci kullanımlarında artış; sunucu sayısı ile paralel olarak altyapı ve bakım maliyetlerinde azalma sağlanmıştır. 10 tane tam dolu kabin sanallaştırma projesi sonrasında tek kabin içinde birleştirilerek daha yönetilebilir bir yapı oluşturulmuştur. Kurum 1, sağladığı tüm servisleri sanal ortama taşıyarak %100 sanallaşan ilk kamu kurumu örneğidir. Sanallaştırma ile daha yönetilebilir bir yapı kurmanın yanı sıra yedekli bir yapı oluşturulmuştur. Sanallaştırmada tercih edilen ürünün yüksek erişilebilirlik çözümü ile iş sürekliliği ve sistem kaynaklarının ihtiyaç olduğu zaman otomatik olarak dağıtımını yapan çözümleri ile kaynakların etkin kullanımı ve başarım artışı sağlanmıştır. Kurum 1, 2010 yılı planlarında yer alan hali hazırda ülke genelinde tüm birimleri kapsayacak olan masaüstü sanallaştırma projesi ilgili olarak araştırmalar yapmakta ve yeni ürünleri deneyerek testler gerçekleştirmektedir.

Kurum 1 olarak, sanallaştırma sayesinde elde edilen kurumsal katma değerler şu şekilde özetlenebilir:

- Kurumun tüm servisleri sanal ve yedekli bir ortama taşınmıştır.

- Ana bellek, işlemci kullanımlarında artış; altyapı ve bakım maliyetlerinde azalma sağlanmıştır.
- On tane tam dolu kabin sanallaştırma projesi sonrasında devre dışı bırakılmış ve tek kabin içinde yeni "blade" sunuculara aktarılarak daha yönetilebilir bir yapı oluşturulmuştur.
- Boşa çıkarılan sunucular geliştirilen yeni projelerde ihtiyaç duyulan veri paylaşımlarının sağlanabilmesi adına talepte bulunan kamu kurumlarına hibe edilerek kamu kaynaklarının atıl kalması engellenmiştir.
- Sunucu/istemci altyapısı içinde sorun çözüm süreci standardize edilmiş ve kısaltılmıştır.
- Daha güvenli bir sunucu/istemci altyapısı oluşturulmuştur, güvenlik altyapısı yeniden tasarlanmış, altyapı da yedekli bir şekilde donatılmış, yedekli yapı ile iş sürekliliği sağlanmıştır.
- Beş binden fazla kullanıcıya hizmet veren Kurum 1'de başarım artışı sağlanmıştır.

Kurum 1 sanallaştırma projesini hayata geçirirken örnek alabileceği başka kamu kurumlarının az olması nedeniyle ürün ve teknoloji tercihi yaparken zorlanmıştır. Bunun yanı sıra yapması gereken donanımsal ve yazılımsal tercihleri nasıl ölçeklendireceği konusuna netlik kazandırana kadar belli bir zaman kaybetmiştir. Bu sorunların çözümlerine yönelik olarak kapasite planlayıcı araçlar kullanmış ve gerçek yatırım ihtiyacını bu çalışmalar sonrasında belirleyebilmiştir.

Sanallaştırma projesini tamamlayan kurum bu geçiş sonrasında yedekleme altyapısını değiştirmek zorunda kalmış ve sanal ortamlar için farklılaşan yedekleme stratejileri belirlemek zorunda kalmıştır.

7.2.2. Örnek Çalışma: Kurum 2

Kurum 2, yeni gelen iş yüküyle beraber Türkiye'nin en önemli kamu kuruluşlarından biri oluşmuştur. İnternet tabanlı uygulamalarıyla ülkemize 7x24 çevrimiçi olarak hizmet vermektedir. Kurum 2, ülke çapında 500 civarında yerleşke ile hizmet vermeyi sürdürmektedir. Kurumda başlatılan sanallaştırma projesi, üst yönetimin desteği 2008 yılında başarı ile tamamlanmıştır. Bu proje ile beraber sistem altyapısında standardizasyon ve yönetim kolaylığı sağlanmıştır.

Kurum 2, sanallaştırma alt yapısına 2005 yılında işletim sistemi üzerine kurulan sanallaştırma yazılımı ile sanallaştırma teknolojilerini kullanmaya

başlamıştır. 2008 yılında mevcut sunucu altyapısının teknolojik ömrünü doldurması üzerine ve yeni ihtiyaçlar da göz önüne alınarak artan iş yükünü karşılamak amacıyla sistem altyapısına yatırım yapma ihtiyacı doğmuştur. Kurumun aldığı karar ile sanallaştırma projesine geçiş çalışmaları başlatılmıştır. AR-GE çalışmaları ve teknik şartname hazırlığı Kurum teknik personelince yapılmıştır. Türkiye'de Kamu Kuruluşlarında bu büyüklükte yapılan başka sanallaştırma projesinin olmayışından ve ilk olunmasından dolayı projenin her aşaması çok iyi hesap edilmiştir. Özellikle üst yönetimin projeye destek vermesi projenin başarı oranını arttırmıştır. O zaman için uygun bir Kapasite planlama yazılımı bulunmadığından planlama Sanal Makine (VM) başına bir çekirdek işlemci ve 4 GB ana bellek olarak tasarlanmıştır. Planlamaya göre, bu proje ile toplamda 320 VM alt yapısı kurulmuş olacaktır. Mevcut sunucular üzerinde çalışan servis ve uygulamalar güncel sürümlerine yükseltilmiş ve Kurum'un ihtiyaçlarını karşılayacak yeni yapıya göre tasarlanmıştır. Sanal altyapıya geçiş ile beraber işlemci ve ana bellek kaynakları değerlendirilerek başarımda, erişebilirlikte ve hizmet kalitesinde artış sağlanmıştır. Diğer yandan, altyapı ve bakım maliyetlerinin düşmesinin yanında yönetim kolaylığı sağlanmıştır. 200 adet civarında sunucuda çalışan iş yükünü sanal altyapıda 20 adet sunucuyla karşılayacak duruma gelmiştir. Ayrıca yeni iş gücü yükü de bu sanallaştırma sunucuları üzerinde tasarlanmıştır. Avrupa'da kamu kuruluşlarında en büyük sanallaştırma projesini gerçekleştirerek bu alanda ödül almıştır. Sanallaştırma projesi ile beraber yüksek erişilebilirlik çözümü ile iş sürekliliği ve sistem kaynaklarının ihtiyaç olduğu zaman otomatik olarak dağıtımını yapan çözümler sağlanmıştır. Kaynakların etkin kullanımı sayesinde başarım artışı sağlanmıştır. Kendi içerisinde yüksek erişebilirlik sağlandığı gibi aynı yapı, farklı bir yerleşkede Felaket Kurtarma Merkezine de kurulmuştur.

Sanallaştırma sayesinde, Kurum 2 olarak elde edilen kurumsal katma değerler aşağıda sıralanmıştır:

- Kurumun tüm servis ve uygulamaları sanal ortama taşınmıştır.
- Atıl kalan işlemci ve ana bellek kullanımlarında artış; altyapı ve bakım maliyetlerinde azalma sağlanmıştır.
- Mevcut sunucular sanallaştırma projesi sonrasında devre dışı bırakılmış ve 20 adet sunucuya aktarılarak daha yönetilebilir bir yapı oluşturulmuştur.
- Boşa çıkarılan sunucular test ve eğitim amaçlı laboratuvar ortamı oluşturulması için tasarlanarak atıl kalması engellenmiştir.

- Sunucu altyapısı içinde uzak/yerinde sorun çözüm ve destek süreci standart hale getirilmiştir.
- Daha güvenli ve erişebilir bir sistem altyapısı oluşturulmuş ve yedekli yapı ile iş sürekliliği sağlanmıştır.
- 20 bin civarında iç kullanıcıya ve uygulamalarıyla ülke geneline hizmet veren Kurumda başarım artışı sağlanmıştır.
- Kurum BT altyapısında 8 personel VCP sertifikası almıştır.
- Sanallaştırma altyapısında yaşanan sorunlara teknik personel ile kısa zamanda çözüme gidilmektedir.
- Kurum 2'nin tüm sistem altyapısı Kurum teknik personeli tarafından sistem kesintiye uğratılmadan sanal ortama aktarılmıştır.

Bunlarla birlikte, sunucu tarafında sanallaştırma yapılırken aynı zamanda iletişim ağı tarafında da kablolama altyapısına yönelik konsolidasyona gidilmiştir. Bu konuda uygun bir kapasite planlama yazılımı olmadığından kapasite planlama konusunda zorluklar yaşanmış; ancak kurumsal bilgi birikimine dayanılarak yazılım kullanılmadan kapasite planlaması yapılmıştır. Ayrıca, sanallaştırma yazılımı için nasıl bir destek alınacağı ile ilgili çeşitli zorluklar yaşanmıştır.

BÖLÜM 8.

SONUÇ VE ÖNERİLER

Sanallaştırma, verimlilik, esneklik ve çevreci bilişim gibi güçlü savlalarla ortaya çıkan güncel bir teknolojidir. Bu raporda, sanallaştırmanın ne olduğu, neden ve nasıl yapıldığı ile sanallaştırmaya geçiş ölçütleri tartışılmış, geçiş sürecinde kolaylık sağlayacak önerilerde bulunulmuştur.

Sanallaştırma, masaüstü, bellek, veri saklama alanı, sunucu ve işletim sistemi gibi çok değişik yapıların, gerçekte bulunan kaynaklardan bağımsız olarak kullanılabilmesini sağlayan bir yöntemdir. Tek bir sunucunun birçok sanal sunucu olarak gösterilmesi ya da saklama alanındaki verimsizlikleri ortadan kaldırması yönüyle donanım gereksinimlerini azaltan ve israfı önleyen bir teknolojidir. Donanım gereksinimlerinin azalmasını ve aynı işin daha az enerji kullanılarak yapılmasını sağladığı için sanallaştırma çevre dostu bir teknolojidir. Kullanıcıların, donanımın yeteneklerini tam kullanamadıkları masaüstü bilgisayarlar yerine, örneğin ince istemcilerle sunucu üzerinden çalışabilmesini sağlayan donanım seçeneklerini sunarak, kurumun bilgisayar alım maliyetlerini azaltması da olasıdır.

Sanal makineler kolay yedekleme ve kurtarma olanakları sunmakta, hizmet veren sunucunun kapatılmadan güncellenmesini sağlayarak hizmet kesintilerini önlemektedir. Bu yönüyle sanallaştırma sistemin güvenirliğini ve kesintisiz hizmet süresini artırıcı bir teknolojidir. Kurulacak yeni programların, sanal sunucular üzerinde denenmesi; sonrasında ise çok kısa süre içinde ve hizmet kesintisi yaratmadan hizmete sokulması sanallaştırma sayesinde mümkündür.

Kurumlar, sanallaştırmaya özel yönetim araçlarını kullanarak, daha az çaba ile tüm sanal sistemlerini yönetebilirler. İnce istemcilerin kişisel bilgisayar yerine kullanıldığı ortamlarda, kişisel bilgisayarlarda yaşanacak olağan sorunlar büyük ölçüde ortadan kalkacak ve böylece binlerce kişinin masaüstü bilgisayarları, sunucunun bulunduğu merkezden kolayca yönetebilir konuma gelecektir.

Günümüzde, sanallaştırma yazılımı olarak kendini ispatlamış bir çok seçenek bulunmaktadır. Bu ürünlerden bazıları, destek ve bakım hizmetleri ile birlikte ücretli lisanslarla sunulmakta ve hatta entegratör firmalar tarafından sunulan çözümler içinde kullanılmakta; bazıları ise genel kamu lisansı ile ücretsiz olarak sunulan açık kaynak kodlu projeler olarak karşımıza çıkmaktadır. Yurtdışındaki örneklerde olduğu

gibi, ücretsiz olarak sunulan bu ürünlerle birlikte ücretli destek ve bakım hizmetleri sunan BT firmaları, sanallaştırma desteği açısından Ülkemizde de önemli alternatifler haline gelmişlerdir. Diğer BT alanlarında olduğu üzere, sanallaştırma ürünlerinin seçiminde de, açık standartlarla uyumlu ürünlerin tercih edilmesi, ileride doğabilecek uyum sıkıntılarının mümkün olduğunca bugünden önüne geçilmesi açısından yararlı olabilecektir.

Sanallaştırma pek çok kurum için uygun bir çözüm seçeneğidir. Sanallaştırma, sunduğu olanaklarla kurumların verimliliğini artırma ve maliyetlerini düşürme olanakları sunsa da, kurumun sanallaştırmaya geçmeden önce bazı ölçütleri gözden geçirmesi ve tasarım kararları vermesi gereklidir. Uç bir örnek vermek gerekirse; ince istemciler gibi donanım araçlarıyla kişisel bilgisayarları tamamen ortadan kaldıran bir kurum, en ufak İnternet bağlantısı kesintisinde ya da sunucunun çökmesi durumunda kurum içindeki tüm çalışanların çalışamaz hale geleceğini göz önünde bulundurmalıdır. Kişisel bilgisayarlar, her ne kadar kaynak verimsizliği yaratsalar da, bir tanesinin bozulması diğer çalışanların çalışabilirliğini etkilemez. Bu nedenle, birbirinden konum olarak uzak mekanda bulunan sunucu ve istemciler için sanallaştırma kullanmayı düşünen kurumların, İnternet bağlantısının niteliğini ve kesinti olasılığını özenle incelemesi gerekmektedir.

Dikkat edilmesi gereken bir diğer konu da, sanallaştırılmış ortamlarda kullanılacak yazılımlara ait lisanslarla ilgilidir. Sanallaştırılmış ortamlara ilişkin özel lisanslama seçeneği sunmayan firmalara ait ürünleri satın alırken, bu ürünlere ait lisansların, sanal ortamlara değil, taşıyıcı fiziksel altyapıya göre hesaplanması gerektiği konusuna özen gösterilmesi gereklidir.

Sanallaştırma teknolojilerindeki ve uygulamalarındaki gelişmeler, sanallaştırılmış olan kaynakların bir araya getirilmesi; sunucu çiftlikleri üzerinde sanal kaynak havuzları oluşturulması; hatta yönetimsel olarak birbirlerine bağlı birimlerin veya firmaların veri merkezlerinin bu şekilde bir araya getirilerek daha büyük ve daha merkezi yapıların oluşması; hatta sanal kaynak barındırma ve erişim hizmetlerini sunan (sanal veri merkezi de denilen) yapıların oluşması sonuçlarını doğurabilmektedir. Bu yöndeki ilerleyiş, bulut bilişimin gelişmesine de katkı vermektedir.

Sanal veri merkezi örneğinde olduğu gibi, sanallaştırma teknolojilerinin, bilgilerin uzaktaki sunucularda tutulması ve erişilmesini de olağan ve kullanılır bir düzen haline getirmesi olasıdır. Ancak kamu kurumlarının bilgilerini uzakta ve

başkaları tarafınca barındırılacak konumlarda tutmaları, özellikle veri güvenliği açısından her kurumun kendi başına değerlendirmesi gereken bir konudur.

Sanallaştırma, sunduğu olanaklarla kamu kurumlarımızın BT birimleri için yeni ve cazip seçenekler sunmaktadır. Kamu kurumlarımızın kendi gereksinimlerini ve kısıtlarını belirleyip kendilerine en uygun sanallaştırma çözümlerini kullanmaları, sanallaştırma teknolojisinin kurumda başarıya ulaşma olasılığını artıracaktır. Sanallaştırma çözümlerinin kurumun yapısına uygunluğuna bakarak verilecek olan, sanallaştırmaya kısmen geçiş veya kademeli olarak geçiş veya bu aşamada sanallaştırma çözümlerini uygulamama kararları da alternatifler içinde değerlendirilmelidir. Bunların yanında, donanım üreten firmaların ürünleri tarafından sanallaştırma yöntemlerine verilmekte olan ve giderek yaygınlaşan desteğin, zaman içinde sanallaştırmaya geçiş konusunda yöneltici unsurlardan biri haline gelme olasılığının bulunduğu da düşünülmektedir.

Son olarak belirtmek gerekirse; sanallaştırma, sistem yöneticilerinden uçlardaki kullanıcılara kadar kurumun tüm BT çalışmalarında ciddi değişiklikler getiren, önemli bir geçiştir. Sanallaştırmanın başarılı olabilmesi için, sanallaştırma çalışmalarına başlamadan önce, tanıtım çalışmaları, eğitim seminerleri gibi faaliyetlerle, yönetim kademelerinden son kullanıcılara kadar BT ile ilgili herkesin desteğinin ve hatta inancının kazanılmaya çalışılması önemlidir.

KAYNAKÇA

[1] "Virtualization", Wikipedia, http://en.wikipedia.org/wiki/Virtualization, 12 Nisan 2010.

[2] David Bolton, "Definition of Virtualization", About.com Guide, http://cplus.about.com/od/glossar1/g/virtualization.htm, Kasım 2009.

[3] "Definition for Virtualization", ZDNet: Tech News, Blogs and White Papers for IT Professionals. http://dictionary.zdnet.com/definition/Virtualization.html, Son erişim: Nisan 2010.

[4] "Virtualization", Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions, http://www.webopedia.com/TERM/V/virtualization.html, Aralık 2009.

[5] Peter J. Denning, "Performance Modeling: Experimental Computer Science at its Best", Communications of the ACM, Kasım 1981.

[6] R. J. Creasy, "The origin of the VM/370 time-sharing system", IBM Journal of Research & Development, Vol. 25, No. 5, Eylül 1981.

[7] Rogier Dittner ve David Rule, "The Best Damn Server Virtualization Book Period: Including Vmware, Xen, and Microsoft Virtual Server". Syngress, ISBN 1597492175, 2007.

[8] Melinda Varian, "VM and the VM community, past present, and future", SHARE89 Sessions 9059-9061, 1977.

[9] "LPAR", Wikipedia, http://en.wikipedia.org/wiki/Logical_partition, 15 Nisan 2010.

[10] Fernando J. Corbató, Marjorie Merwin Daggett ve Robert Daley, "An Experimental Time-Sharing System", SJCC, 3 Mayıs 1962.

[11] Jason Nieh ve Özgür Can Leonard, "Examining VMware", Dr. Dobb's Journal, Ağustos 2000.

[12] R. Uhlig ve diğerleri, "Intel virtualization technology," Computer, Vol. 38, No. 5, Mayıs 2005.

[13] "Xen", Wikipedia, http://en.wikipedia.org/wiki/Xen, 10 Nisan 2010.

[14] Paul Barham ve diğerleri, "Xen and the Art of Virtualization", SOSP '03: ACM symposium on Operating systems principles, 2003.

[15] "z/VM: the newest VM hypervisor based on 64-bit z/Architecture", http://www.vm.ibm.com, Son erişim: Nisan 2010.

[16] Yeşim Çinioğlu, " Çevreci Yaklaşımın Ürünü Yeşil Veri Merkezleri ", BT Haber, Sayı 703, http://www.cevreciyiz.com/akademi/default.aspx?SectionId=278&ContentId=3651, 19-25 Ocak 2009.

[17] "Virtualisation: An easy win", Microsoft United Kingdom, http://www.microsoft.com/uk/publicsector/government/efficiency/virtualisation-an-easy-win.aspx, Son erişim: Nisan 2010.

[18] Steve Ranger, "Cloud, virtualization are new weapons in outsourcing arms race", Silicon.com, 15 Temmuz 2009.

[19] Steve Ranger, "Virtualisation and cloud: The new weapons in the outsourcing arms race", Silicom.com, 14 Temmuz 2009.

[20] Cenk Yapıcı, "IDC Veri Depolama", Sanallaştırma ve Yönetilebilir Servisler Konferans serisi,http://www.telepati.com/kasim09/konu5.htm, Kasım 2009.

[21] DDO Danışmanlık ve Temsilcilik, "Sunucu Sanallaştırması – Ne Zaman Anlamlı?", http://www.siberkult.com/blog/?p=143, Son erişim: Nisan 2010.

[22] Distributed Management Task Force, "Open Virtualization Format Specification",http://www.dmtf.org/standards/published_documents/DSP0243_1.0.0.pdf, 2009.

[23] Amit Singh, "A Taste of Computer Security", kernelthred.com, http://www.kernelthread.com/publications/security/sandboxing.html, Haziran 2004.

[24] "Software Restriction Policies", Microsoft, http://technet.microsoft.com/en-us/library/cc734043(WS.10).aspx, 30 Kasım 2007.

[25] John Hoopes, "Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting", Syngress, ISBN: 1597493058, 2008.

[26] Tuğba Akbal ve Bülent Örencik, "Veri Kaydı Güvenliği", Ağ Güvenliği Dersi Dönem Projesi, İTÜ, http://www3.itu.edu.tr/~orencik/AgGuvenligi2007 Sunumlari/akbal_verikaydi_rapor.doc, Nisan 2007.

[27] "VMsafe: A Security Technology for Virtualized Environments", VMWare, http://www.vmware.com/technical-resources/security/vmsafe/security_ technology.html, Son erişim: Nisan 2010.

[28] "ESX Server, Security Technical Implementation Guide", Defense Information Systems Agency, 28 April 2008.

[29] Ricky M. Magalhaes, "Security and Virtualization", http://www. windowsecurity.com/articles/Security-Virtualization.html, 30 Nisan 2008.

[30] Kevin Fogarty, “Desktop Virtualization: 5 Most Popular Flavors, Explained”, CIO, http://www.cio.com/article/504348, 07 Ekim 2009.

[31] B. Madden, “Desktop virtualization is more than VDI”, SearchVirtualDesktop. com, 8 Nisan 2009.

[32] AT&T, "Understanding VPLS", http://www.dmsstl.com/images/product-briefs /UnderstandVPLS.pdf, 7 Şubat 2008.

[33] Yavuz Gökırmak, Emre Yüce, Onur Bektaş, Murat Soysal ve Serkan Orcan, “IPv6 Balküpü Tasarımı”, EMO Elektrik-Elektronik, Bilgisayar ve Biyomedikal Mühendisliği Ulusal Kongresi, Aralık 2009.

[34] Kurt Seifried, “Honeypotting with VMware – basics”, http://www.seifried.org /security/ids/20020107-honeypot-vmware-basics.html, 15 Şubat 2002.

[35] Joseph Corey, “Advanced Honeypot Identification and Exploitation”. Phrack Magazine, Ocak 2004.

[36] "Hype Cycle for Virtualization", Gartner Group Research, G00168837, 21 Haziran 2009.

[37] Stephen Shankland, "Gartner: Brace yourself for cloud computing", http://news.cnet.com/8301-30685_3-10378782-264.html, 20 Ekim 2009.

[38] Frank Cabri, "Market Dynamics and Virtual Security Issues – Centrify Market Survey and Analysis", http://www.centrify.com/downloads/public/centrify_ ss050_market_dynamics_and_security_issues.pdf, Eylül 2009.

[39] Megan Santosus, "The Promise of Desktop Virtualization", IDG White Paper, http://sites.amd.com/us/Documents/promiseofdesktopvirtualization.pdf, 2008.

[40] "The Benefits of Virtualization for Small and Medium Businesses", VMware White Paper, www.vmware.com/files/pdf/VMware-SMB-Survey.pdf, 2009.

[41] Paul W. Taylor, "IT Industry Priorities in Public Sector", http://www.govtechblogs.com/fastgov/2008/08/it-industry-priorities-in-publ.php, 2008.