T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SANAL SUNUCU SİSTEMLERİNDE FELAKET KURTARMA YÖNETİMİ VE FELAKET KURTARMA PLAN ÖNERİSİ

YÜKSEK LİSANS TEZİ

Yasin AKILLI

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

HAZİRAN 2016

T.C.

İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

SANAL SUNUCU SİSTEMLERİNDE FELAKET KURTARMA YÖNETİMİ VE FELAKET KURTARMA PLAN ÖNERİSİ

YÜKSEK LİSANS TEZİ

Yasin AKILLI

Y1313.010043

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ali GÜNEŞ

HAZİRAN 2016

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1313.010043** numaralı öğrencisi **Yasin AKILLI** 'ın **"SANAL SUNUCU SİSTEMLERİNDE FELAKET KURTARMA YÖNETİMİ VE FELAKET KURTARMA PLAN ÖNERİSİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 07.06.2016 tarih ve 2016/16 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul..edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi :17/06/2016	
1)Tez Danışmanı: Prof. Dr. Ali GÜNEŞ	.....
2) Jüri Üyesi : Yrd. Doç. Dr. Metin ZONTUL	.....
3) Jüri Üyesi : Yrd. Doç. Dr. Ferdi SÖNMEZ	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans / Doktora tezi olarak sunduğum"Sanal sunucu sistemlerinde felaket kurtarma yönetimi ve felaket kurtarma plan önerisi" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (17/06/2016)

Aday / İmza

ÖNSÖZ

Tez konusunun belirlenmesi, bölümlerinin oluşturulması ve içeriğinin şekillendirilmesi ile yazım aşamasında eleştiri ve teşvikleriyle katkıda bulunan başta danışmanım Prof. Dr. Ali GÜNEŞ olmak üzere, Yüksek Lisans eğitimim süresince benden desteğini esirgemeyen İstanbul Aydın Üniversitesi Bilgi İşlem Daire Başkanı Birol ÇELİK, değerli desteklerinden dolayı İstanbul Aydın Üniversitesi Genel Sekreter yardımcısı Serkan YOLSAL ve son olarak varlığı ile hayatımın her anında bana güç veren biricik eşim Esra AKILLI ‘ya teşekkürü bir borç bilirim.

Haziran 2016 **Yasin AKILLI**

İÇİNDEKİLER

Sayfa

KISALTMALAR

IT:	Information Technology (Bilgi Teknolojileri)
DR:	Disaster Recovery (Felaket Kurtarma)
RTO:	Recovery Time Objective (Felaket Kurtarma Süresi)
RPO:	Recovery Point Objective (Felaket Kurtarma Noktası)
VM:	Virtual Machine (Sanal Makine)
FC:	Fiber Channel
ISCSI:	Internet Small Computer System Interface
CPU:	Central Processing Unit
RAM:	Random Access Memory
SLA:	Service Level Agreement
GB:	Giga Byte
GHZ:	Giga Hertz
FK:	Felaket Kurtarma
FKM:	Felaket Kurtarma Merkezi
FKP:	Felaket Kurtarma Planı
SERVER:	Sunucu
CLIENT:	İstemci
DRS:	Distributed Resource Scheduler

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

SANAL SUNUCU SİSTEMLERİNDE FELAKET KURTARMA YÖNETİMİ

VE

FELAKET KURTARMA PLAN ÖNERİSİ

ÖZET

Günümüz gelişen bilgi ve iletişim teknolojileri doğrultusunda işletmeler müşterilerine ya da kullanıcılarına bu teknolojiler üzerinden hizmet sunabilmek için sunucu sistemlerine ihtiyaç duymaktadırlar. Artan iş hacimleri, müşteri ve kullanıcı sayılarına paralel olarak fiziksel sunucu ihtiyaçları da artış göstermiştir.
İşletmeler gelişen bu durum karşısında artan fiziksel sunucu hizmetleri taleplerini karşılamak için yapacakları yeni yatırım giderlerinin önüne geçebilmek için sunucu sanallaştırma teknolojilerini kullanmaya yönelmiştirler. İşletmelerin iş yükünün büyük bir bölümünü üstlenen bu sunucu sistemlerinin önemi her geçen gün daha da artarak işletme devamlılığının en kritik maddelerinden biri haline gelmiştir.
İşletmeler bu durumu dikkate alarak sanal sunucu sistemlerinin hizmet sürekliliğinin sağlanması ve oluşabilecek teknik ya da doğal afet durumlarında hizmet kesintisi ve veri kaybı yaşanmaması için en etkin felaket kurtarma yöntemine ihtiyaç duymaktadırlar.
Bu Tez çalışmasında " fiziksel Sunucu sistemlerinin; gelişen teknoloji ve işletmelerde artan iş hacmine paralel olarak getirdiği zorluklar, sanal sunucu sistemlerinin; sunucu hizmetlerine getirdiği esnek ve kolay yönetim yapısının yanı sıra sanal sunucu sistemlerinde etkin felaket kurtarma yönetimi ve felaket kurtarma yönetimi için bir plan önerisinde bulunulması " araştırılmaktadır.

Anahtar Kelimeler: Sunucu Sistemleri, Sanallaştırma**,** Felaket Kurtarma**,** İş Sürekliliği**,** Felaket Yönetimi

DISASTER RECOVERY MANAGEMENT IN VIRTUAL SERVER SYSTEMS

AND

DISASTER RECOVERY PLAN SUGESTION

ABSTRACT

In accordance with the developing information and communication technologies of today's world, companies, to be able to provide services for their customers or users, are in need of server systems.
In parallel with the increasing amount of bussiness, customers and users; there is a considerable increase in the need of physical servers.
Companies, in order to supply the improved demands of physical servers and to avoid new expenses required, are generally heading for the ussage of virtual server technologies.
The perominence of these virtual systems, that assume the major part of the workload is increasing day by day, making the systems the most critical part of the companies.
Taking all these into consodiraiton, companies need a powerfull disaster recovery management to supply bussiness continutiy and to avoid data loss or lock of access in a possible disaster situtaion.
In this thesis; on one side the difficulities of using physical servers in parallel with the developing technologies and increasing workload, on the other side, the flexibility and easy management structure of virtual server systems are researched; along with active disaster recovery management strategies by giving a disaster recovery management plan sample.

Keywords: Server Systems, Virtualization**,** Disaster Recovery**,** Business Continuity**,** Disaster Management

1. GİRİŞ

Günümüz gelişen bilgi ve iletişim teknolojileri doğrultusunda işletmeler müşterilerine ya da kullanıcılarına bu teknolojiler üzerinden hizmet sunabilmek için sunucu sistemlerine ihtiyaç duymaktadırlar. İş yükünün büyük bir bölümünü üstlenen bu sunucu sistemlerinin önemi her geçen gün daha da artarak işletme devamlılığının en kritik maddelerinden biri haline gelmektedirler.

İşletmeler bu durumu dikkate alarak sunucu sistemlerinin hizmet sürekliliğinin sağlanması ve oluşabilecek teknik ya da doğal afet durumlarında hizmet kesintisi ve veri kaybı yaşanmaması için en etkin felaket kurtarma yöntemine ihtiyaç duymaktadırlar. Sunucu sistemlerinizi barındıran veri merkeziniz için iyi organize edilmiş bir felaket kurtarma yönetimi planı sunucu sistemlerinizde meyadana gelebilecek beklenmedik teknik ve doğal afetlere karşı koruma ve iş sürekliliğini sağlamanın en iyi yoludur.

Veri merkeziniz işletmenizin kalesi gibidir, işletmenizin müşteri ve personellerine hizmet sunarken kullandığı tüm sistemlerin altyapısı bu veri merkezlerinde bulunmaktadır. Donanım, Yazılım, Veri ve Uygulamalarınız gibi tüm kritik IT bileşenleriniz ise sunucu sistemlerinizi oluşturmaktadır.

Veri merkezinizi ve sunucu sistemlerinizi en gelişmiş donanımsal ve yazılımsal güvenlik çözümleri ile korur, hızlı çalışan optik networkler ile maksimum düzeyde kesintisiz hizmet sunan bir hale getirmeye çalışırsınız. Bu çalışmalar için ise çok ciddi zaman ve yatırım maliyet giderlerini gözealırsınız. Bunun yanı sıra veri merkezinizin kontrolü ve sistemlerin yönetilmesi için de insan kaynakları istihdamı gerçekleştirirsiniz. Böylelikler veri merkeziniz ve sunucu sistemleriniz işletmenizin en büyük gider kalemlerinden biri oluşturur.

Buna rağmen ne yazık ki veri merkeziniz ve sunucu sistemleriniz, kontrolünüz dışındaki donanımsal sunucu arızaları, yazılımsal ve uygulama bazlı problemler, donanım ve yazılım üretici firmala servis kesintileri, enerji kesintileri, yangın, sel baskını, deprem gibi doğal afetler ve benzeri sebepler yüzünde yine de tam olarak koruma altına alınmış değildir.
Kısacası risk altında olan şey tüm işiniz, yani veri merkeziniz ve sunucu sistemleriniz enaz firmanız kadar önemli ve bu riski hafifletmek tamamen sizin kuracağınız felaket kurtarma çözümleri ve iyi tasarlanmış bir felaket kurtarma yönetimine bağlıdır.

Felaket kurtarma yönetimi, daha önce planlanmış ve senaryosu test edilmiş ya da beklenmeyen sebeplerden dolayı oluşan felaketleri önlemede ve günlük iş sürekliliğinin sürdürülmesi için çok önemlidir. Kısacası firmanın devamlılığını sağlamada felaket kurtarma temel unsurdur. Asıl amaç IT için tüm kritik servisleri olabildiği kadar çabuk ve veri kaybı olmaksızın geri getirebilmek ve de firmayı oluşabilecek zararlardan korumaktır.

IT departmanınızın çevikliği ve uygulama alt yapınız bu süreci etkileyecek en önemli unsurlardır. Nasılki yangın söndürme ekipmanları yangından önce binalara kurulmalıdır aynı şekilde IT altyapınız için de eğitimleri alınmış ve testleri gerçekleştirilmiş olası felaket senaryonuz ile felaket kurtarma yönetim planınız önceden hazır olmalıdır.

Bu tez çalışmasında “ işletmeler için hem çok kritik hem de çok yüksek maliyetli olan veri merkezleri ve sunucu sistemlerinin sürekliliğini tehdit edecek olan teknik ve doğal afetlerden kaynaklı felaketler karşısında nasıl bir felaket kurtarma süreç yönetimi yapılması ” gerektiğine dair yapılan araştırmalar ve çalışmalar aktarılacaktır.

1.1 Çalışma Konusu

Bu tez çalışmasında "Sanal Sunucu Sistemlerinde Felaket Kurtarma Yönetimi ve Felaket Kurtarma Plan Önerisi" konu başlığı altında: Günlük iş süreçlerinde bilgi teknolojilerini yoğun olarak kullanan işletmelerin sahip oldukları veri merkezlerindeki sunucu sistemleri, sanallaştırma teknolojilerinin sunucu sistemlerine getirdiği yönetimsel kolaylıklar ve bu sunucu sistemleri üzerinden müşterilerine ya da personellerine sundukları ürün veya hizmetlerin kesintisiz olarak devamlılığının nasıl sağlanabileceği hakkında bilgiler sunulmuştur.

İşletme faaliyetlerinin sürdürülebilirliliği konusunda çok kritik bir öneme sahip olan bu sunucu sistemlerinde iş sürekliliğini kesintiye uğratabilicek beklenmedik ve acil durumlarda ortaya çıkan sorunlara karşı nasıl daha etkin ve en az kayıpla sonuçlanacak bir felaket kurtarma yönetimi yapılabileceğine dair araştırmalar ve çalışmalar yapılmış, ayrıca felaket kurtarma yönetimi için bir de plan önerisinde bulunulmuştur.

1.2 Tezin Amacı

Bu tez çalışmasının amacı: Günümüzde bilgi teknolojilerini kullanan işletmelerin sahip oldukları veri merkezlerinde müşterilerine ya da personellerine ürün veya hizmet sunmak için kullandıkları sunucu sistemleri mimarisi hakkında bilgiler sunmak, bu sunucu sistemleri için sanallaştırma teknolojilerinin getirdiği yönetimsel kolaylıkları ve yine bu sunucu sistemlerinde iş sürekliliğini kesintiye uğratabilicek beklenmedik ve acil durumlarda ortaya çıkan sorunlara karşı nasıl daha etkin ve hızlı bir felaket kurtarma yönetimi yapılması gerektiği hakkında fikir ve fayda sağlanma amaçlanmıştır.

Bunlarla beraber yine bu tez çalışmasında; aşağıda sıralanan maddeler amaçlanmıştır.

- IT yöneticileri ya da çalışanları için iş sürekliliği yönetimi ve felaket kurtarma yönetimi bilincinin oluşmasına katkı sağlamak.
- İş sürekliliğinin işletmeler üzerindeki olumlu ve olumsuz etkileri hakkında bilgiler sunmak.
- Veri merkezlerinde felaket kurtarma yönetimini planlamak isteyenler IT uzmanları için referans olarak kullanılabilecek bir örnek felaket kurtarma planı modeli oluşturmak.
- İş sürekliliği ve felaket kurtarma yönetimi ile ilgili akademik olarak yapılacak çalışmalara referans kaynak oluşturmak.

2. SUNUCU SİSTEMLERİ VE SANALLAŞTIRMA

Bu bölümde sunucu sistemleri, sunucu sistemleri çalışma mimarisi, fiziksel ve sanal sunucu avantaj-dezavantaj karşılaştırmaları ile sanallaştırma teknolojileri hakkında bilgilere yer verilmektedir.

2.1 Sunucu Sistemleri

Gelişen bilgi ve iletişim teknolojileri (Bilgisayar, Tablet, Cep Telefonu, Akıllı Telefon, İnternet, Mobil Uygulama, Web Tabanlı Yazılım uygulamaları gibi) doğrultusunda işletmeler müşteri ya da kullanıcılarına sundukları hizmetleri elektronik ortama taşımaya başlamışlardır.

Bu taşınmaya paralel olarak hem bu bilgileri üzerinde barındıracak depolama kapasitesine sahip hem de üzerinde sunacağı hizmetlere hızlı erişim sağlatacak güçlü işlemci ve bellek yapısına sahip sunucu bilgisayarlara ihtiyaç oluşmuştur.

Sunucular, Kişisel bilgisayarlara göre donanım sorunları daha az olan ve hizmet süresi bakımından 7/24 kapasitede çalışan, Bu çalışma durumuna göre özel soğutma mimarisine sahip, Birden fazla sunucu ile ortak çalışabilen ya da tek bir panel üzerinden de yönetim kapasitesine sahip bilgisayarlardır.

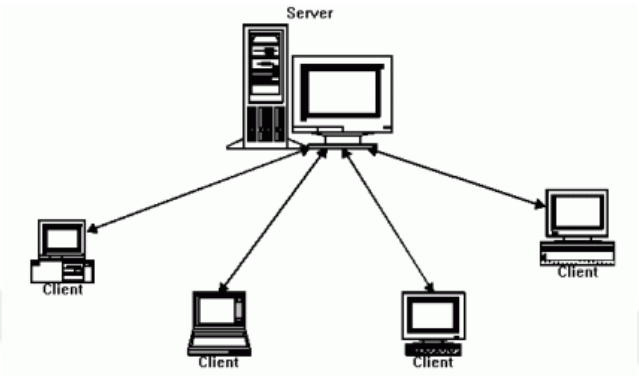
2.1.1 Sunucu sistemleri çalışma mimarisi

Sunucu sistemleri çalışma mimarisi, sunucu-istemci (client-Server) çalışma ve hizmet prensibine uygun olarak inşaa edilen teknolojilerdir.

Sunucu-istemci mimarisini kısaca açıklamakta fayda var. Sunucu-İstemci mimarisinde sunucunun görevi; istemci (kullanıcı, personel, müşteri ve istemci uygulama bilgisayarları) tarafından ihtiyaç duyulan verinin yönetilmesini ve işlenmesini kesintisiz bir şekilde yapmaktır.

İşte sunucu sistemleri bu şekilde tasarlanmış bir çalışma mimarisine sahip olarak üretilmekte ve geliştirilmektedir.

Aşağıdaki şekilde sunucu sistemlerinin temel çalışma prensibi olan sunucu-istemci (Client-Server) yapısı Şekil 2.1 ’de gösterilmektedir.

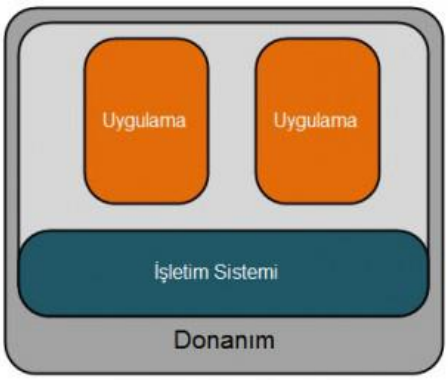


Şekil 2.1: Sunucu-İstemci Çalışma Mimarisi

2.1.2 Fiziksel sunucu sistemleri

Fiziksel sunucu adından da anlaşılacağı üzere tek bir donanım üzerinde yine tek bir işletim sistemi kurulabilen sunucu sistemleridir. Fiziksel sunucu sistemleri çalış

Günümüz gelişen bilgi teknolojileri ve farklı uygulama çeşitliliği gibi artan sunucu gereksinimlerine bakıldığında fiziksel bir sunucu üzerine sadece bir işletim sistemi kurmak ve kurulan işletim sisteminin üzerinde de sadece kısıtlı uygulamaların çalıştırılabiliyor olması yüzünden artık çok fazla tercih edilmemektedir.



Şekil 2.2: Fiziksel Sunucu Mimarisi

2.1.3 Fiziksel sunucu sistemleri avantaj ve dezavantajları

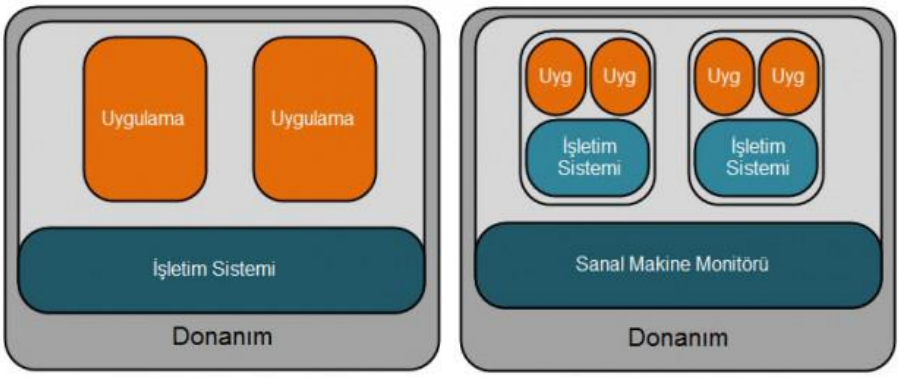
Fiziksel sunucu sistemlerinin kullanmasının getirdiği işletim sistemi ve uygulama bazlı getirdiği zorlukların yanısıra donanımsal ve maliyet bazlı bir takım dezavantajlarıda beraberinden getirmektedir.

Fiziksel sunucu sistemlerinin dezavantajları aşağıda sıralanmıştır.

- Sunucu donanım giderleri
- Sunucu yazılım giderleri
- Sunucu bakım ve onarım giderleri
- Sunucu Yazılım destek giderleri
- Sistem odası altyapı giderleri
- Enerji giderleri
- Soğutma giderleri
- Güvenlik ve izleme giderleri
- İnsan kaynağı
- Yönetim giderleri
- Sistem süreklilik giderleri

Yukarıdaki tüm maddeleri toparladığımız fiziksel sunucu sistemleri yüklü bir bütçe gider kalemi olmanın yanısıra yönetimsel zorlukları da birarada getirmektedir.

Fiziksel ve sanal sunucu mimarisi karşılatırılması Şekil 2.3'te gösterilmektedir.



Şekil 2.3: Fiziksel ve Sanal Sunucu Mimarisi

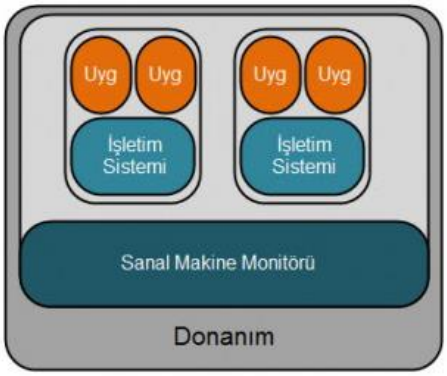
Fiziksel sunucuların genel avantajları aşağıda sıralanmıştır.

- Sadece bir işletim sistemine bağlı donanım ve yazılım kaynak kullanımı
- Yüksek seviyeli bilgi giriş-çıkış taleplerine cevap verebilme
- Yüksek donanım ve yazılım kaynağına bağlı sunucu ve işlem performansı, şeklinde belirtebilebilir.

2.1.4 Sanal sunucu sistemleri

Sunucu sanallaştırma, fiziksel sunucu üzerindeki donanımsal kaynakların (işlemci, ram, disk, network kartı vb.) ve yazılımsal platformların (işletim sistemi, uygulama, masaüstü vb.) sanallaştırma yazılımı katmanı (hyper-visor) ile soyut hale dönüştürerek birden çok sunucuya hizmet verebilecek şekilde bu kaynakların paylaştırılması şeklinde ifade edilebilir.

Bu sayede fiziksel sunucu üzerinde var olan kaynaklar tek bir işletim sistemi veya uygulamaya hizmet verme zorunluluğundan kurtarılmış ve sunucu kaynakları daha efektif olarak kullanıılması sağlanmıştır.



Şekil 2.4: Sanal Sunucu Mimarisi

Şekil 2.4 ’te de görüldüğü üzere bir fiziksel sunucu donanımı üzerinde birden fazla sanal sunucu ve işletim sistemi kurulabiliyor.

Sanal sunucu sistemleri sadece bir fiziksel sunucu üzerine birden fazla sanal sunucu kurulması ile ifadebiliecek bir konu değildir. Sanal sunucu mimarisinin bilgi teknolojileri alanında getirmiş olduğu birçok ciddi yetenek ve kolaylık bulunmaktadır.

Gelişen bilgi teknolojileri ve işletmelerin bilgi teknolojilerine bağımlılığı arttığı sürece büyüyen ve büyümeye devam edecek olan ver merkezlerinin en büyük yükünü sanal sunucu sistemleri üstlenmeye başlamıştır.

2.1.5 Sanal sunucu sistemleri avantaj ve dezavantajları

Sanal sunucu sistemlerinin işletmelere ve işletmelerin IT departmanlarına getirdiği temel avantajlar aşağıda sıralanmıştır.

- Kolay yönetim ve operasyon
- Verimli kaynak yönetimi
- Çoklu işletim sistemi uyumluluğu
- Etkin hata yönetimi ve izolasyonu
- Kesintisiz veri ve sunucu taşıma
- Sistem güncelleme test ortamı
- Esnek donanım değişiklik yönetimi
- Hızlı felaket Kurtarma yönetimi

2.2 Sanallaştırma

Sanallaştırma, fiziksel sunucu üzerindeki donanımsal kaynakların (işlemci, ram, disk, network kartı vb.) ve yazılımsal platformların (işletim sistemi, uygulama, masaüstü vb.) sanallaştırma yazılımı katmanı (hyper-visor) ile soyut hale dönüştürerek birden çok sunucuya hizmet verebilecek şekilde bu kaynakların paylaştırılması şeklinde ifade edilebilir.

Sanal sunucu sistemlerinde felaket kurtarma yönetimini detaylı olarak anlatmadan önce ilk olarak sanallaştırma fikrinin nasıl ortaya çıktığı ve bu fikrin günümüze kadar nasıl geldiğini anlamamıza katkı sağlayacak olan tarihsel gelişim süreçlerden kısaca bahsetmek gerekmektedir.

2.2.1 Sanallaştırmanın tarihçesi

Sanallaştırma fikrinin nasıl ortaya çıktığı ve sanallaştırma teknolojisinin geliştiğine dair bilgi sahibi olmamız için sanallaştırmanın tarihçesinden kısaca bahsetmek gerekmektedir.

Sanallaştırma çalışmalarına ilk olarak Oxford üniversitesinde zaman paylaşımı ve çoklu programlama fikrinin ortaya atılması ile başlanmıştır. Bu fikir kapsamında yapılan çalışmalar sonucunda Atlas projesi ismi ile sanallaştırma fikri somutlaştırılarak hayata geçirilmiştir.

1960 yılında Mancehter Üniversitesi öncülüğünde yürütülen Atlas projesi çalışmalarında ilk kez super-vizör (hiper-vizör veya bir çeşit sanal makine monitorü) ile sanal bellek kavramı ifade edilmeye başlandı. Ayrıca sanallaştırma fikri IBM firmasının 1960'lı yıllarda yaptığı çalışmalar sonucunda geliştirdiği M44/44X sistemlerinde de ortaya atılmıştır. Bu çalışmalar sırasında ise sanal makine kavramı ilk kez ifade edilmeye başlandı. Bu çalışma sırasında ilk kez sanal makine kavramı konuşulmaya başlandı (Cevat, 2010).

Yine IBM firmasının 1966 yılında geliştirdiği ve ilk tam sanallaştırma sistemleri olarak bilinen IBM CP-40 ile IBM CP-67 sanallaştırma modelleri oluşturuldu.1980 yılına kadar süren bu çalışmaların sonucunda IBM S/370 sanallaştırma modeli ilk donanım sanallaştırma teknoloji olarak hayata geçirilmiştir, yine bu çalışmanın paralelinde devam eden diğer bir projede ise IBM VM/370 isimli ilk sanal sunucu işletim sistemi de ortaya çıkarılmıştır (Cevat, 2010).

1990'lı yılların sonuna doğru gelişen bilgi ve iletişim teknolojileri doğrultusunda artan iş hacimleri, müşteri ve kullanıcı sayılarına paralel olarak fiziksel sunucu ihtiyaçları da artış göstermiştir.

İşletmeler gelişen bu durum karşısında artan fiziksel sunucu hizmetleri taleplerini karşılamak için yapacakları yeni yatırım giderlerinin önüne geçebilmek için sunucu sanallaştırma teknolojilerini kullanmaya yönelmiştirler.

Hem artan sunucu sistemleri maliyetleri hem de sahip olunan kaynakların daha verimli bir halde kullanılabilmesi ihtiyacı sanallaştırma teknolojisi üzeretecek firmalara olan ihtiyacı da bereberinde getirdi.

1998 yılında VMware şirketi bu amaç üzerinde kurulur ve 1999 yılında ise masaüstü bilgisayarlarla sanallaştırma teknolojilerini tanıştıran VMware Workstation ürününü pazara sürmüştür. Masaüstü bilgisayarlarda yakaladığı başarıyı sunucu bilgisayarlarda da yakalamak için çalışmalarına devam eder ve Linux çekirdek üzerinde geliştirdiği VMware GSX ile VMware ESX isimli sunucu sanallaştırma yazılımlarını 2003 yılında piyasaya sürer, sonrasından geliştirdiği vCenter ve vMotion teknolojileri ile sektörün öncüleri arasındaki yerini alır (Cevat, 2010).

Sunucu sanallaştırma yazılımları ile ilgili çalışmalar sürerken, fiziksel sunuculardaki işlemcileri üreten iki lider firma Intel ve AMD ise 2005 yılında sunucu sanallaştırma teknolojilerini desteklemek için kendi ürettikleri fiziksel işlemci mimarisinin (x86, IA-32) sanallaştırma yazılımlarına uygun şekilde yenileyerek sanallaştırma teknolojilerinin daha hızlı yayılmasını ve kullanılmasını arttırdı (Wikipedia Encyclopedia, 2016).

Günümüzde gelinen son noktaya bakacak olursak; sanallaştırma teknolojileri artık bilgi teknolojileri altyapıları için vazgeçilmez bir yere gelmiştir.

Sanallaştırma teknolojileri pazarına bakıldığında ise VMware, Microsoft, Citrix, IBM ve Oracle gibi teknoloji üreticileri bu pastadan ciddi pay almakta ve bu payı arttırmak için teknolojilerini rakiplerinin önüne geçebilmek adına geliştirmeye devam etmekedirler.

2.3 Sunucu Sanallaştırma

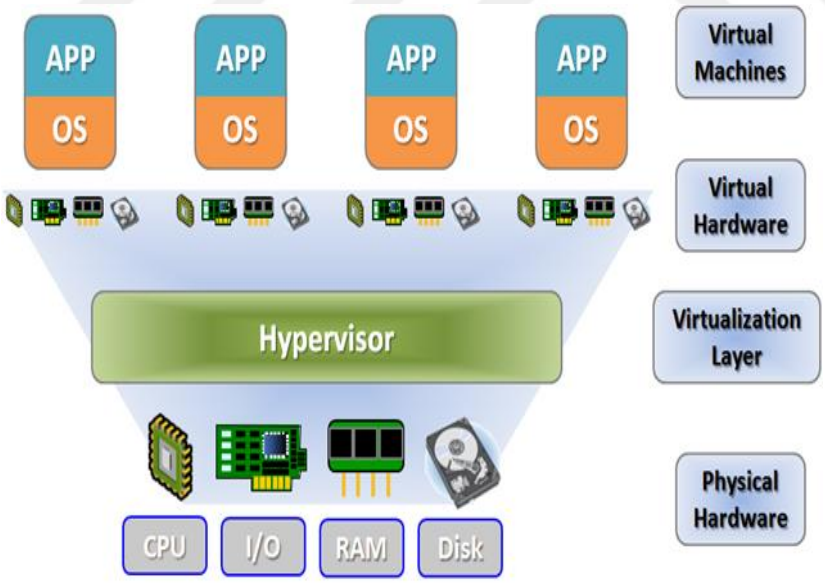
Sunucu sanallaştırma, fiziksel sunucu üzerindeki donanımsal kaynakların (işlemci, ram, disk, network kartı vb.) ve yazılımsal platformların (işletim sistemi, uygulama, masaüstü vb.) sanallaştırma yazılımı katmanı (hyper-visor) ile soyut hale dönüştürerek birden çok sunucuya hizmet verebilecek şekilde bu kaynakların paylaştırılması şeklinde ifade edilebilir.

Bu sayede fiziksel sunucu üzerinde var olan kaynaklar tek bir işletim sistemi veya uygulamaya hizmet verme zorunluluğundan kurtarılmış ve sunucu kaynakları daha efektif olarak kullanıılması sağlanmıştır.

IT yöneticileri için sanallaştırma denilince akla ilk gelen sunucu sanallaştırma tipidir. Sunucu sanallaştırma teknolojisi temel olarak tek bir fiziksel sunucunun sahip olduğu donanım kaynakları üzerinde kaynaklar dahilinde birçok işletim sisteminin kurulabilmesi ve paralel olarak birbirinden bağımsız aynı anda çalıştırılablimesi olarak tanımlanabilir.

Bir bilgisayar sisteminin kaynaklarını sanallaştırma fikri yıllardır üzerinde çalışılan bir konudur. Bu fikir işlemciler, bellek ve giriş-çıkış birimleri dâhil olmak üzere, bilgisayar sistemlerinin paylaştırılmasını ve kullanımının artırılmasını amaçlamaktadır. Sunucu sanallaştırmada, tek bir fiziksel platform üzerinde birden fazla işletim sistemi ve yazılım paketlerinin çalışması sağlanır (Buyya & Broberg, 2011).

Sunucu sanallaştırmada kurulan bireysel işletim sistemleri ile fiziksel donanım arasına yeni bir soyutlama katmanı eklenmektedir. Sunucu sanallaştırma ile soyutlama katmanı aynı anda birden fazla işletim sisteminin bir dizi donanım ile etkileşimini sağlamaktadır. Sunucu donanım kaynaklarını sanallaştırma teknolojisi şekil 2.5 'te gösterilmektedir.



Şekil 2.5 : Sunucu Sanallaştırma

Sunucu sanallaştırmaya ihtiyaç duyulmasının temel nedenleri inceleyecek olursak;

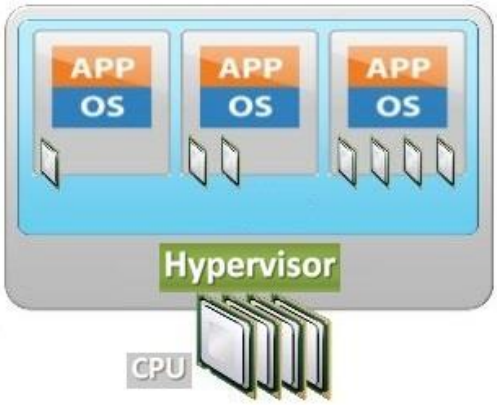
- Sunucu kaynaklarının verimli kullanılmaması
- Artan uygulama çeşitliliği
- Farklı işletim sistemleri uyumluluğu
- Kesintisiz hizmet sürekliliği
- Operasyonel kısıtlılık
- Artan donanım maliyetleri
- Artan altyapı ve enerji giderleri

Yukarıda belirtilen temel nedenlerden dolayı sunucu sanallaştırma teknolojilerine olan ihtiyaç her geçen gün daha da artmaktadır.

Günümüzde sunucu sanallaştırma teknoloji üreticileri ve ürettikleri sanallaştırma yazılımları incelendiğinde; Microsoft Hyper-V, VMware Virtual Center ve ESX(i) Server, Citrix XenSource, IBM zSeries, Oracle VM, Linux KVM ve Open Source Xen gibi üretici ve ürünler karşımıza çıkmaktadırlar.

2.3.1 İşlemci sanallaştırma

İşlemci sanallaştırma; fiziksel sunucunun sahip olduğu donanımsal işlemcilerin sanalllaştırma yazılım katmanı ile izole hale getirilip, bu sanallaştırma katmanı üzerinde oluşturulacak olan birden fazla sanal sunucu işletim sistemine kullandırılmasıdır, işlemci sanallaştırma Şekil 2.6 ’da gösterilmektedir.

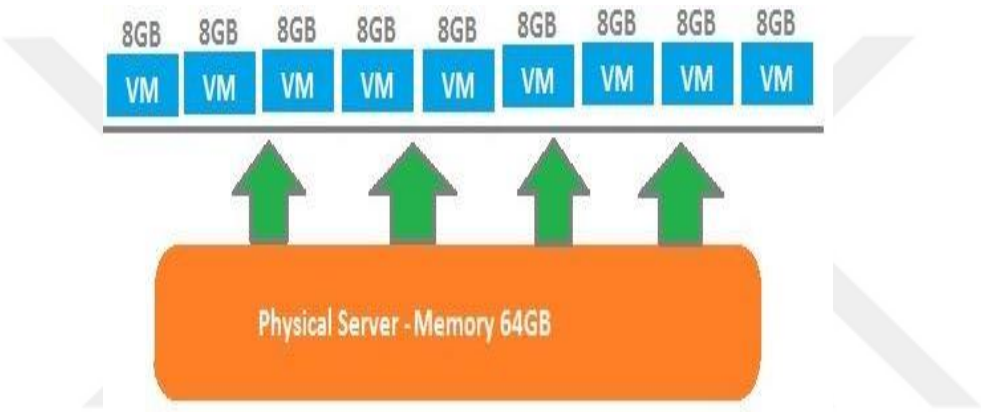


Şekil 2.6 : İşlemci Sanallaştırma

2.3.2 Bellek sanallaştırma

Fiziksel sunucu sanallaştırmanın yapılabilmesi için fiziksel sunucu içerisindeki 4 temel donanımın sanallaştırılması gerekmekktedir. Bu 4 temel donanımdan biri de bellektir.

Bellek sanallaştırma; fiziksel sunucunun sahip olduğu donanımsal belleğin sanalllaştırma yazılım katmanı ile izole hale getirilip, bu sanallaştırma katmanı üzerinde oluşturulacak olan birden fazla sanal sunucu işletim sistemine kullandırılmasıdır, bellek sanallaştırma Şekil 2.7'de gösterilmektedir.



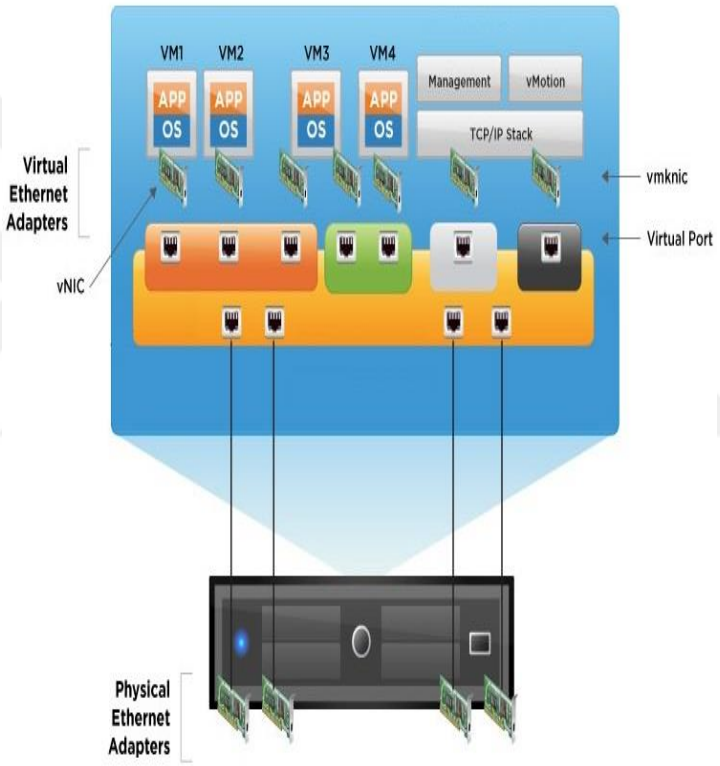
Şekil 2.7 : Bellek Sanallaştırma

2.3.3 Ağ sanallaştırma

Fiziksel sunucu sanallaştırmanın yapılabilmesi için fiziksel sunucu içerisindeki 4 temel donanımın sanallaştırılması gerekmekktedir.

Bu 4 temel donanımdan biri de Ağ'dır. Ağ sanallaştırma; fiziksel sunucunun sahip olduğu donanımsal belleğin sanalllaştırma yazılım katmanı ile izole hale getirilip, bu sanallaştırma katmanı üzerinde oluşturulacak olan birden fazla sanal sunucu işletim sistemine kullandırılmasıdır.

Ağ sanalllaştırma Şekil 2.8'de gösterilmektedir.



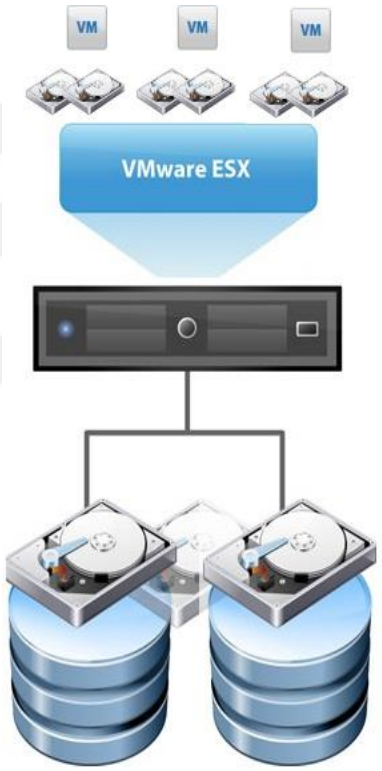
Şekil 2.8 : Ağ Sanallaştırma

2.3.4 Disk sanallaştırma

Fiziksel sunucu sanallaştırmanın yapılabilmesi için fiziksel sunucu içerisindeki 4 temel donanımın sanallaştırılması gerekmekktedir.

Bu 4 temel donanımdan biri de disk'tir. Disk sanallaştırma; fiziksel sunucunun sahip olduğu donanımsal belleğin sanalllaştırma yazılım katmanı ile izole hale getirilip, bu sanallaştırma katmanı üzerinde oluşturulacak olan birden fazla sanal sunucu işletim sistemine kullandırılmasıdır.

Disk sanallaştırma Şekil 2.9 'da gösterilmektedir.



Şekil 2.9 : Disk Sanallaştırma

2.4 Sanal Sunucu Sistemlerinin Avantajları

Sanallaştırmanın sunucu sistemlerine getirdiği birçok faydalar bulunmaktadır. Özellikle fiziksel sunucu sistemlerinde yaşanan birçok operasyonel ve yönetimsel sorunlar sanallaştırma teknolojisi ile ya ortadan tamamen kaldırıldı ya da basit bir hale dönüştürüldü.

Sanal sunucu sistemlerinin IT yönetimine kazandırdığı özelliklerden başlıcaları aşağıda sıralanmıştır bunlar;

- Fiziksel sunucu sayılarında azalma.
- Veri merkezi altyapı ihtiyaçlarında azalma (sunucu barındırma alanı, soğutma, yedekleme, enerji, ağ bağlantı cihazları vb.)
- Tek merkezden kolay sunucu yönetimi ve esnek yönetim kabiliyeti.
- Yeni sanal sunucuların, fiziksel sunuculara göre mevcut sunucu sistemine daha kolay ve hızlı eklenip yönetilmesi.
- Sunucularda donanımsal bağımlılığın ortadan kaldırılması.
- Verimli Kaynak yönetimi ve IT giderlerinde azalma.
- Çoklu işletim sistemi uyumluluğu.
- Etkin hata yönetimi ve hata izolasyonu.
- Kesintisiz veri ve sunucu taşıma.
- Sistem güncelleme test ortamı.
- Esnek donanım değişiklik yönetimi.
- Hızlı felaket kurtarma yönetimi.

Yukarıda saymış olduğumuz tüm bu özellikler sanallaştırma teknolijisinin sunucu sistemlerine ve IT yönetimine önemli faydalar sağladığı görülmektedir.

Yukarıda saymış olduğumuz bu özellikler hakkında aşağıda başlıklar halinde açıklamalar yapılmıştır.

2.4.1 Kolay yönetilebilirlik

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "kolay yönetilebilirlik" sunmasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, işletmelerin devamlılığını sağlayan veri merkezelerinin altyapısının hergeçen gün daha da büyüdüğü günümüzde bu sistemlerin kesintisiz hizmet vermesinin yanı sıra IT yöneticileri tarafından da kolay yönetilebilmesi de çok önemlidir.

Sanallaştırma teknolojisi kullanıldığı tüm sistemlerin yönetimini fiziksel sunucu yönetimine göre daha kolay hale getirmektedir. İstenildiği zaman tüm sanal sunucu sistemlerinin birer kopyası alınıp yönetimsel işlemler bu sunucular üzerinde daha rahat yapılabilir.

Bunun yanısıra, sanal sunucuların kullandıkları donanımsal kaynaklar dahil sahip oldukları tüm sistem özellikleri sunucular kapıtlamadan ve kullanıcılara kesinti yaşatmadan kolay bir şekilde değişitirilip yönetilebilmektedir.

2.4.2 Verimli kaynak yönetimi

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "verimli kaynak yönetimi ve IT giderlerinde azalma" sunmasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, IT altyapıları büyüdükçe hem bu yapıları tedarik etme maliyetleri hem de bu altyapıları yönetme zorlukları ortaya çıkmaktadır.

Günümüzde IT hizmetleri sağlayan ve kullanan işletmeler, başta veri merkezleri olmak üzere birçok alanda maliyet ve masrafları azaltmak için sanallaştırma teknolojilerini kullanmaktadırlar.

IT maliyetlerini ve masraflarını önemli ölçüde azaltan sanallaştırma teknolojisinin ortaya çıkardığı başlıca yararlar aşağıda sıralanmıştır.

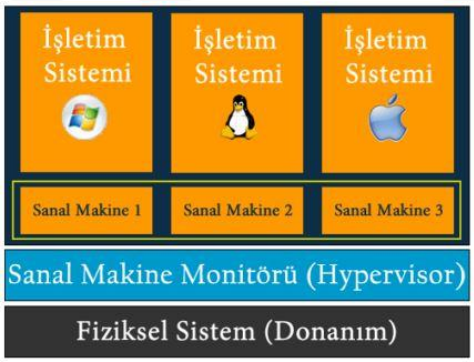
- Donanım kaynaklarının daha etkin ve verimli kullanılması.
- Donanım kaynaklarının bakım süreçlerinin hızlanması ve kolaylaşması.
- Fiziksel barındırma alanı, soğutma ve enerji tüketiminin azalması.
- Veri ve sunucu yedekleme ve geri yükleme işlerinin kolaylaşması.

IT yönetiminde kaynak optimizasyon çalışmaları önemli ölçüde yönetim ve işletim giderlerini azaltmaktadır. Sanallaştırılmış sunucu sistemlerinde bir fiziksel sunucu üzerinde aynı anda birçok işletim sistemini kurabilmek, çalıştırabilmek ve her işletim sistemi için birden fazla uygulama veya servis çalıştırılabilmek mümkündür. Böylekile sahip olunan fiziksel kaynaklar çok daha verimli ve etkin kullanılmış olacaktır.

2.4.3 Çoklu işletim sistemi uyumluluğu

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "çoklu işletim sistemi uyumluluğu" sağlamasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, fiziksel bir donanım üzerine sadece bir işletim sistemi kurabiliyor ve kullanabiliyorsunuz. Başka bir ifade ile "MS Windows Server" işletim sistemi kurduğunuz fiziksel sunucu üzerine "LINUX" işletim sistemi kurup aynı anda bu iki işletim sistemini kullanamazsınız.

Sanallaştırma teknolojisi ile beraber gelen çoklu işletim sistemi uyumluluğu hem marka bağımlılığını ortadan kaldırmış hem de aynı anda çoklu işletim sistemi çalıştırabilme imkanı sağlamıştır. Çoklu işletim sistemi uyumluluğu Şekil 2.10'da gösterilmektedir.



Şekil 2.10 : Çoklu işletim Sistemi Uyumluluğu

Sanallaştırma teknolojisi kullanılmadan önce fiziksel sunucularda iki farklı işletim sistemi kurulumu yapalıbiliyor fakat ikisi aynı anda o fiziksel sunucu üzerinde çalışamıyordu.

Sanallaştırma teknolojisi sayesinde bu problem çözüldü, artık tek bir fiziksel sunucu üzerine birçok farklı işletimi kurulup ve birbirilerini hiç etkilemeden aynı anda çalışalan sanal sunucular kuralabilir hale geldi.

2.4.4 Etkin hata yönetimi ve hata izolasyonu

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "etkin hata yönetimi ve hata izolasyonu" sunmasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, normal şartlarda bir fiziksel sunucuda problem oluştuğunda üzerinde çalışan sistem doğrudan etkilenir, servis ve hizmet kesintisi yaşanır.

Örneğin; bir fiziksel sunucunuz var ve üzerinde bir işletim sistemi kurulmuş durumda. Bu işletim sistemi üzerinde ise muhasebe ve personel giriş-çıkış sistemi uygulamarınızın çalıştığını varsayalım. Bu sunucuda muhasebe uygulumasından kaynaklı yazılımsal bir hata oluştu ve bu hatanın işletim sistemini çalışamaz duruma getirdiğini varsayalım.

Yaşanan bu durum karşısında personel giriş-çıkış sisteminde herhangi bir hata olmadığı halde muhasabe uygulamasının oluşturduğu hatadan dolayı olumsuz yönden etkilenip hizmet veremez duruma gelecektir.

Aynı fiziksel makinede çalışan sistemlerin birbirinden etkilenmesi beklenen bir durum olmasına rağmen sanallaştırma teknolojisi fiziksel makine üzerinde çalışan her bir sanal sistemin diğerlerin habersiz ve izole edilmiş bir şekilde çalışmasını sağlamaktadır. Dolayısı ile bir sanal makinede oluşan bir sorun diğer sanal makineleri etkilemez. Sorunlar otomatik olarak izole edilir. Diğer tüm sistemler ve servisler çalışmaya devam ederken oluşan sorun sistem yöneticileri tarafından giderilebilmektedir (Daş, 2012).

2.4.5 Kesintisiz veri ve sunucu taşıma

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "kesintisiz veri ve sunucu taşıma" imkânı sunmasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, normal şartlarda bir fiziksel sunucuyu başka bir ortama taşımak istediğinizde bu sunucunun elektrik enersini kesmeniz gerekmektedir. Bu durum beraberinde servis ve hizmet kesintisi de getirecektir.

Sanallaştırma teknolojisi ile gelen "vmotion" ve "storage-vmotion" özellikleri sayesinde sanal sunucular, veri kaybı ve hizmet kesintisi olmaksızın bir fiziksel sunucudan başka bir fiziksel sunucuya taşınıp çalıştırılabilir.

2.4.6 Sistem güncelleme test ortamı

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "sistem güncelleme test ortamı" sunmasıdır.

Bu maddeyi biraz daha detaylı inceleyecek olursak, normal şartlarda bir fiziksel sunucuda yeni yazılımsal güncelleme öncesi testler yapmak isteyebilirsiniz, ancak bu bu durum hem çalışan ortam için bir hizmet kesintisi riski oluşturmaktadır hem de operasyonel anlamda daha fazla efor ve zaman harcamayı da beraberinde getirmektedir.

Çalışan bir sisteme yeni bir uygulama veya servis ekleneceği zaman öncelikle bu servisin test edilmesi gerekmektedir. Test edilen servisin çalışan sisteme zarar vermemesi son derece önemli bir konudur. Bu nedenle çoğu sistem yöneticisi elindeki kaynakları kullanarak bir test ortamı oluşturmaktadır.

Fiziksel sunucular ile bir test ortamı oluşturmak oldukça maliyetli ve zahmetli bir iş iken sanallaştırılmış bir sistemde bu işlem son derece kolaydır. Sanallaştırılmış ortamda test edilmek istenen uygulamalar diğer sistemleri etkilemeden rahat bir şekilde test edilebilmektedirler (Daş, 2012).

2.4.7 Esnek donanım değişiklik yönetimi

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de "esnek donanım değişikliği yönetimi" sunmasıdır. Bu maddeyi biraz daha detaylı inceleyecek olursak, normal şartlarda bir fiziksel sunucuda donanım değişikliği yapma ihtiyacı ortaya çıktığında sunucu üzerinde bu işlemi yapabilmeniz için sunucunun elektrik enersini kesmeniz gerekmektedir. Bu durum beraberinde servis ve hizmet kesintisi de getirmektedir.

Fiziksel sunucu mimarisinde donanımsal arıza veya performan artışı için donanım değişikliği yapmak istediğinizde sunucuyu ve üzerindeki uygulamaları kapatmak zorunda kalırsınız. Bu durum hem hizmet kesintisi hem de donanım değişiminden kaynaklı operasyon sürelerinin uzaması gibi dezavantajları beraberinde getirmektedir.

Sanal sunucu sistemlerinde ise sunucularınızı cluster mimarisi ile dizayn ettikten sonra, donanımsal arıza veya performan artışı için donanım değişikliği yapmak istediğinizde ilgili sunucu üzerinden çalışan işletim sistemi ve uygulumalarınızı vmotion teknlojisi ile cluster içerisindeki diğer sunucu ortamına kesintisiz olarak taşıyabilirsiniz. Böylelikle hem sunucuyu kapatmayarak kesinti süresi zorluklarını yaşamaz hem de operasyonel kolaylıklara sahip olursunuz.

2.4.8 Esnek felaket kurtarma yönetimi

Sanallaştırma teknolojisinin sağladığı avantajlardan biri de hızlı felaket kurtarma yönetimidir. Bu maddeyi biraz daha detaylı inceleyecek olursak, normal şartlarda sadece fiziksel sunucular üzerinden hizmet veren bir veri merkezini olası bir teknik ve doğal afet durumunda kesintisiz bir şekilde devamlılığını sağlamak yüksek maliyetli yatırım ve yönetiim zorluklarını beraberinde getirmektedir.

Günümüzde kullanılan fiziksel sunucu/iş istasyonu sayısının çokluğu nedeniyle, birçok organizasyon fiziksel mekân, güç ve soğutma gibi sorunlar ile uğraşmak zorunda kalmaktadır. Artan enerji ve yerleşke talebi hem çevre için hem de şirketler için olumsuz sonuçlar doğurmaktadır (Menken, 2010).

Sanallaştırma teknolojisi kullanılarak sunucu sistemlerinin olası hatalara ve beklenmedik durumlara karşı dayanıklılıkları artırılabilmektedir. Örneğin, aktif hizmet veren bir fiziksel sunucu üzerinde bakım çalışması yapılması gerektiğini varsayalım. Bu çalışma sırısasında sunucuda kesintiye sebep olabilecek bir problem ile karşılaşıldığında o fiziksel sunucuda çalışan tüm sanal sunucuların ilgili kullanıcılara hizmet kesintisi olarak yansıtılmadan varolan farklı bir fiziksel sunucuya taşınması çok kolay ve hızlı bir şekilde yapılabilmektedir. Böylece IT yöneticileri tarafından amaçlanan iş sürekliliği sağlanmış olur.

Bunun yanısıra sanallaştırılmış sunucuların ve servislerin birer kopyalarını düzenli olarak almak, herhangi bir problem anında bir önceki problemsiz çalışma durumuna hızlıca geri dönüş yapılabilir.

Burada en önemli noktalardan biri ise sanal sunucu sistemlerinin dayanıklılığını ve iş sürekliliğini en üst seviyede tutabilmek için sanal sunucuları üzerinde taşıyan fiziksel sunucularında sürekli yüksek erişilebilir halde tutulmaları gerektiğidir.

Ayrıca “sanal sunucu sistemlerinin avantajarı” başlığı altında incelediğimiz ve aşağıda sıralanan tüm konular, sanallaşlaştırma teknolojilerinin esnek felaket kurtarma yönetimi için getirdiği kolaylakıları kapsamaktadır.

- Kolay yönetilebilirlik.
- Verimli kaynak yönetimi ve IT giderlerinde azalma.
- Çoklu işletim sistemi uyumluluğu.
- Etkin hata yönetimi ve hata izolasyonu.
- Kesintisiz veri ve sunucu taşıma.
- Sistem güncelleme test ortamı.
- Esnek donanım değişiklik yönetimi.
- Hızlı felaket kurtarma yönetimi.

Yukarıda belirtiğimi ve sanallaştırma teknolileririnin sunuculara kazandırğı, vmotion, storage-vmotion, snapshot ve DRS gibi daha birçok özellik esnek felaket kurtarma yönetimine katkı sağlamaktadır.

3. SUNUCU SİSTEMLERİNDE FELAKET KURTARMA YÖNETİMİ

Sunucu sistemlerinde felaket kurtarma yönetimini anlatmadan önce iş sürekliliği konusunda bir takım bilgiler vermek gerekmektedir. Bu tez e konu olan Felaket kurtarma yönetimi aslında iş sürekliliği kavramının bir parçasını oluşturmaktadır.

İş sürekliliği konusu kendi başına bir tez konusu olarak incelenebilecek kadar geniş bir konudur, ancak felaket kurtarma yönetimi ile ilgili bu tez i hazırlarken tez in önemini ve konu bütünlğünü tamamlaması açısından iş sürekliliği konusuna temel seviyede değinilecektir.

3.1 İş Sürekliliği

İş sürekliliği; bir işletmenin kritik iş süreçlerini ve servislerinin devamlılığını sağlamak, bu devamlılığı aksatacak bir kesinti olduğu zaman ise kabul edilebilir bir süre içinde tüm kritik iş süreçlerini ve servislerin yeniden çalışabilir hale getirmek için yapılan çalışmaların tümü olarak tanımlanabilir.

İşletmeler kullanıcı veya müşterilerine sundukları hizmet ve servislerin kesintisiz çalışmasını hedeflemektedirler. Bu hizmet ve servislerde yaşanacak kesintiler hem prestij hemde ciddi maddi zararları beraberinde getirmektedir.

Günümüzde hızla gelişen bilgi ve iletişim teknolojileri doğrultusunda işletmeler müşterilerine ya da kullanıcılarına hızlı ve kesintisiz hizmet sunmak için veri merkezilerine yatırımlar yapmaktadırlar. Bu veri merkezlerini ise en yüksek hizmet ve servis erişilebilirliliği sunan sistemler ile inşaa etmeye devam etmektedirler, yine bu sistemlerin enaz kesinti ile hizmet verebilmesi için tüm IT altyapısına da ciddi yatırımlar yapmaktadırlar.

İşletmeler için hem mali açıdan önemli bir gider kalemini oluşturan hem de iş yükünün büyük bir bölümünü üstlenen bu veri merkezleri işletme devamlılığının sağlanması için en kritik maddelerinden biri haline gelmektedir.

İşletmeler bu durumu dikkate alarak veri merkezinde hizmet veren sunucu sistemlerinin iş sürekliliğinin sağlanması ve oluşabilecek teknik ya da doğal afet durumlarında hizmet kesintisi ve veri kaybı yaşanmaması için en etkin felaket kurtarma yöntemine ihtiyaç duymaktadırlar.

Sunucu sistemlerini barındıran veri merkezleri için iyi organize edilmiş bir felaket kurtarma yönetimi planı sunucu sistemlerinizde meyadana gelebilecek beklenmedik teknik ve doğal afetlere karşı koruma ve iş sürekliliğini sağlamanın en iyi yoludur.

İstanbulda yaşanan deprem, Amerikada ikiz kule saldırısı ve ikitelli sel baskını gibi birçok doğal afet ve terör tehlikesi de iş sürekliliğini tamamen aksatacak etkenlerdir. Böyle durumlarda ise veri merkezinizin tamamını kaybetme riski ile karşıkarşıya kalabilirsiniz. Veri merkezlerinde yaşanabilecek donanımsal ve yazılımsal sorunlar ise doğal afet veya terör saldırısı kadar etkili olmasada yine iş sürekliliğini kısmi olarak aksatabilir (Taşkın & Sarıoğlu, 2012).

İşletmelerin ister doğal bir afet gibi tüm veri merkezini kaybetmeye neden olacak problemler, istersede teknik bir problemden kaynaklı hizmet ve servis kesintisine neden olacak riskleri önceden belirleyen, bu riskleri ve etkilerini analiz eden, olası problem anında nasıl önlem alınacağı ve de felaket kurtarma sürecinin nasıl yönetileceğini ortaya koyan bir iş sürekliliği yönetimine ihtiyacı bulunmaktadır.

3.1.1 İş sürekliliği yönetimi

İş sürekliliğini sağlamanın en önemli adımlarından biri de sürecin iyi yönetilmesidir. Sadece kriz yönetimi için gerekli altyapının hazırlanması ve teknolojik gereksinimlerin hazır olması yeterli değildir. İşletmelerde iş sürekliliğini aksatacak beklenmedik bir durum yaşandığında hazırlıklı olmak ve planlı bir şekilde hareket etmek çok önemlidir.

İş sürekliliği Yönetimi, bir felaket sonrasında operasyonların kesintiye uğraması sonucu, şirketlerin kritik iş süreçlerinin sürekliliğini sağlamayı amaçlayan planlar bütünüdür (Marsh, 2016).

İş sürekliliği planlaması yapılırken iş akışına olmusuz etki edecek küçük ya da büyük ölçekli tüm senaryolar gözönüne alınmalıdır.

Bu olumsuz etkiler sadece maddi zararlarla kalmayıp aynı zamanda işletmenin sektördeki imajını ve itibarınıda son derece olumsuz etkliyebilmektedir. Tüm bu riskler dikkate alınarak acil veya beklenmedik durumlara karşı iyi organize edilmiş bir iş sürekliliği yönetimi planı işletme için her zaman çok önemli bir yere sahip olacaktır. Her işletmenin kendi yapısına uygun bir iş sürekliliği yönetim planın olması artık önemli bir gerekliliktir. Bu plan kapsamında işletmenin devamlılığında sorumlu olan yönetici ve çalışanların bu konuda biliçlendirilmesi, beklenmedik bir durumda planlı ve iyi organize edilmiş bir şekilde harekete geçme bilincini de oluşturmak için gerekli eğitim ve çalışmaları da desteklemelidir. Burada esas amaç iş sürekliliğini aksatmaya sebep olacak problem küçük ya da büyük ölçekli olmasına bakılmaksızın işletmeninin olabilecek en az hasar ve kayıp ile bu problemi atlatması için gerekli eylemleri yerine getirmek ve günlük iş süreçlerinin devamlılığını sağlamaktır.

İş sürekliliği Yönetiminin Amacı;

- Beklenmedik durum ve iş sürekliliği planlama ve yönetimi stratejisi, organizasyonu ve sürecinin değerlendirmesi ve iyileştirilmesi,
- Beklenmedik durum ve iş sürekliliği planlamasının IT risk değerlendirmesi ve iş etki analizi ile uyumlu hale getirilmesi,
- Beklenmedik durum ve iş sürekliliği planlamasının iş hedefleri ve gereklilikleri ile uyumlu hale getirilmesi,
- IT yapısı için Beklenmedik Durum Planı hazırlanması veya iyileştirilmesi amacıyla yönlendirme,
- İş operasyonları için kriz yönetimi ve iletişim planları dâhil olmak üzere iş Sürekliliği Planlarının hazırlanması veya iyileştirilmesi amacıyla yönlendirme,
- Beklenmedik durum ve iş sürekliliği planları için test senaryolarının hazırlanması,
- Beklenmedik durum ve iş sürekliliği planları testlerinin gerçekleştirilmesi esnasında destek verilmesi,
- Beklenmedik durum ve iş sürekliliği yapısı dâhilinde görev ve sorumlulukların tanımlanmasıdır (Bilişim Derneği, 2016).

3.1.2 İş sürekliliği standartları

NFPA 1600 : A.B.D. National Fire Protection Association 2000 yılında risk değerleme (risk assessment), etki analizi (impact analysis), zararın hafifletilmesi (hazard mitigation) konularını içeren ve daha sonra American National Standards Institute (ANSI) tarafından iş sürekliliği planları için referans olarak gösterilen Standard on Disaster / Emergency Management and Business Continuity Programs (NFPA 1600)'ı yayımlamıştır (Akpınar, 2015).

PCI DSS (Payment Card Industry Data Security Standard) : Tüm büyük bankaların ve kredi kartı kurumlarının empoze ettiği ve kart ile ödeme sistemlerinde veri güvenliğinin tanımlandığı standarttır (Akpınar, 2015).

ISO27000 Serisi : International Organization for Standardization (ISO) tarafından geliştirilmiştir. Birçok büyük kurum enformasyon ve iletişim teknolojileri sağlayıcılarından ürün ve hizmetlerinin ISO27001 ile uyumlu olmasını talep etmektedir (Akpınar, 2015).

PAS 56 ve PAS 77 : 2006 (Publicily Available Specification) : British Standards Institution tarafından iş sürekliliği yönetiminin süreç, prensip ve terminolojisi; enformasyon teknolojileri sürekliliği ve kullanılabilirliği için geliştirilen çerçeve spesifikasyonlardır (Akpınar, 2015).

BS25999 : British Standards Institution tarafından PAS 56 temel alınarak geliştirilen ve iki bölümden meydana gelen uluslararası iş sürekliliği yönetimi standardıdır (Akpınar, 2015).

3.2 Sunucu sistemlerinde Felaket Kurtarma Yönetimi

Felaket kurtarma yönetimi: Günlük iş süreçlerinde bilgi teknolojilerini yoğun olarak kullanan işletmelerin sahip oldukları veri merkezlerindeki sunucu sistemleri, sanallaştırma teknolojilerinin sunucu sistemlerine getirdiği yönetimsel kolaylıklar ve bu sunucu sistemleri üzerinden müşterilerine ya da personellerine sundukları ürün veya hizmetlerin kesintisiz olarak devamlılığını sağlamak" olarak ifade edilebilir.

Başka bir deyişle; İşletme faaliyetlerinin sürdürülebilirliliği konusunda çok kritik bir öneme sahip olan bu sunucu sistemlerinde iş sürekliliğini kesintiye uğratabilicek beklenmedik ve acil durumlarda ortaya çıkan sorunlara karşı daha etkin ve en az kayıpla atlatmak için yapılan eylemler bütünü olarak ta tanımlanabilir.

İşletmelerin IT altyapısında karşılaşabileceği bir kriz veya felaket durumunda felaket kurtarma süreçlerinin başarılı bir şekilde yönetebilmesi için iyi organize edilmiş bir felaket kurtarma planına ihtiyacı bulunmaktadır. Kısacası firmanın devamlılığını sağlamada felaket kurtarma en temel unsurdur.

Felaket kurtarma yönetiminde asıl amaç sunucu sistemleri ve IT altyapı hizmetleri için tüm kritik servisleri olabildiği kadar çabuk ve veri kaybı olmaksızın geri getirebilmek, firmayı oluşabilecek zararlardan korumaktır.

IT departmanınızın çevikliği ve uygulama alt yapınız bu süreci etkileyecek en önemli unsurlardır. Nasılki yangın söndürme ekipmanları yangından önce binalara kurulmalıdır aynı şekilde IT altyapınız için de eğitimleri alınmış ve testleri gerçekleştirilmiş olası felaket senaryonuz ile felaket kurtarma yönetim planınız da önceden hazır olmalıdır.

3.2.1 Fiziksel sunucu sistemlerinde felaket kurtarma

Fiziksel sunucu sistemlerinde felaket kurtarma hem maliyetli hem de operasyon açısından oldukça zorlu süreçleri içerir. Birkaç yıl öncesine kadar güvenilir sanallaştırma yönetimi çözümleri olmadan felaket kurtarma yöntemleri aşağıdaki nedenlerden dolayı tatmin edici değillerdi.

- Yüksek maliyet
- Karmaşıklık
- Düşük güvenilirlik

Maliyet yüksekti; çünkü klasik yani manuel yöntemler de felaketten kurtulmak için var olan donanımsal ve yazılımsal sistem altyapınızı barındıran aynı özelliklerde ikinci bir veri merkezi kurmanız gerekiyor, yeni lisanslar almanız gerekiyor ve yeni personellere ihtiyaç vardı bu çok önemli bir handikap ve yüksek maliyet getiriyordu. Bu Maliyetler; server, lisans, sistem odası, personel masrafları vb. giderlerden oluşuyordu.

Sistemi anlamak güçtü karmaşıktı; çünkü tüm işletmenin kurtarılmasının temini için felaket kurtarma planınız tüm bireysel unsurları ve aktif kullanılan hareketli parçaları (Uygulamalar, hostlar, network ve storage) işin içine katılmak zorundaydı.

Güvenilirliği düşüktü çünkü otomatik değillerdi ve hiçbir kurtarma prosedürü test edilemiyordu. Test ler yapılmak istense bile sistemler kapatılıp test yapılabileceği için hem hizmet kesintisini hem de yüksek maliyetleri göze almak gerekiyordu.

Birçok firma RPO ve RTO değerlerine güvenemiyordu, IT departmanlarının bir felaket anında durumu kurtarmaya yetip yetemeyeceğine, veri merkezlerinin sistem altyapı ve güvenliği için ödenen sigorta giderlerinin gerçekten bu masraflara değer olup olmadığının şüphesi içindelerdi.

3.2.2 Sanal sunucu sistemlerinde felaket kurtarma

Disaster planlamasının başarılı olmasında sanallaştırma temel ve kritik bir önem taşır. Sanallaştırma Donanım ve Yazılım ‘ın karmaşıklığından soyutlanarak, sunucu sistmlerindeki süreçlerin standartlaşmasına imkân tanır, bu da kurtarma planınızı ve kurtarma süreçlerinizi daha güvenilir ve test edilebilir yapar.

Sanallaştırma teknolojileri; fiziksel sunucu sistemlerinde felaket kurtarma süreçlerinde yaşanan zorlukları çok ciddi oranda ortadan kaldırmış ve temel olarak aşağıda sıralan kolaylıkları beraberinde getirmiştir.

- Düşük maliyet
- Otomatik yönetim
- Güvenilirlik

Daha az masraflı felaket kurtarma; sanallaştırmanın sistemlere hızlı adapte edilmesi ve kopyalama teknolojisinin gelişimi ile felaket kurtarma daha az masraflı hale gelmektedir.

Sanallaştırma altyapısını kullanan sunucu sistemlerinde sistem kesintisi (failover) süreçleri daha kolay ve otomatik olarak süreç yönetimi yapılabilir hale gelmiştir. Daha düşük masraflı kopyalama (replikasyon) seçenekleri, düşük maliyetli veri depolama cihazları ya da bu işlemler için felaket kurtarma yönetim yazılımları gibi seçenekler artarak yaygınlaşıyor.

Tüm bu gelişmeler felaket kurtarmayı daha kapsamlı ve kolay yönetilebilir bir hale getirirken bunun yanısıra kritik IT cihazlarını ve sistemlerini aynı zamanda daha uygun maliyetlerde ve daha küçük veri merkezlerinde koruyabilir hale getirmiştir.

Otomatikleştirilmiş felaket kurtarma; Sanallaştırma ile fiziksel sunucu sistemlerindeki felaket kurtarma süreçlerinde yaşanan felaket kurtarma süreçlerin yönetimi, takibi, süreç adımlarının belirli bir düzen ve sıra ile uygulanması gibi zorluklar ortadan kalkmaya başlamıştır.

Sanal ortamlarda felaket kurtarma için kurtarma aşamasındaki her adımı önceden belirleyip, belli kriterler meydana geldiğinde yapılması istenen operasyonlar önceden belirlenip ilgili FKM yazılımları sayesinde otomatik hale getirilebilmektedir.

Örneğin; e-posta sunucunuzu yedekli çalışacak şekilde tasarladıktan sonra bu iki sanal sunucudan birinde belli bir süre aralığında iletişim kaybı (ping) yaşanırsa sunucu üzerindeki tüm hizmetleri diğer sunucu üzerine otomatik olarak taşınması için bir kurallar listesi oluşturabilirsiniz. Oluşturduğunuz bu kurallar listesindeki kural gerçekleştiği zaman felaket kurtarma yazılımı bu sistemdeki hizmetleri yedek sunucuya otomatik olarak yönlendirir. Böylelikle kullanıcılar için herhangi bir hizmet kesintisi yaşanmazken IT yöneticileri için de bu işlem otomatik ve zahmetsiz olarak yapılmış olacaktır.

Sanallaştırılmış sunucu sistemlerinde felaket kurtarma çözümleri otomatik olarak icra edilebilir ve istenen seviyede koruma tüm aşamaları ile sağlanabilir. Artık tüm firmalar için bir sanal ortamda kurtarma planı oluşturmak RPO ve RTO seçimi kadar kolay hale gelmiştir.

Güvenilir ortam koruması ve taşıması; IT yöneticileri sanallaştırma ile sunucu sistemleri için RPO ve RTO larına karşı daha güçlü bir garantiye sahip oldular. Sanallaştırma; hizmet kesintisiz ve veri kayıpsız bir şekilde kurtarma planlarını sıklıkla tekrar ve test etme olanağı sağlar. Otomatik olmayan kurtarma aşamaları artık otomatik kurtarma olarak değişti ve bu da kullanıcılardan kaynaklı hata riskini sıfıra indirdi denilebilir.

3.3 Felaket Kurtarma Yönetiminin Sınıflandırılması

Felaket kurtarma yönetimi, felaketin veri merkezi ve sunucu sistemleri üzerindeki etkilerine göre iki ana başlık altında sınıflandırılabilir.

Sunucu sistemlerinin tümünü barındıran veri merkezinizin tamamını kaybetmenize sebep olabilecek doğal aftlerin yanı sıra sadece sunucu sistemlerinin bir bölümünü veya bir kaç uygulamanızda hizmet kesintisine sebep olabilecek teknolojik problemlerde felaketin etkileri ayrı ayrı değerlendirilip, felaket yönetiminin de ona göre yapılabilmesi için bu sınıflandırma gerekmektedir.

İşletmelerin ister doğal bir afet gibi tüm veri merkezini kaybetmeye neden olacak problemler, istersede teknik bir problemden kaynaklı hizmet ve servis kesintisine neden olacak riskleri önceden belirleyen, bu riskleri ve etkilerini analiz eden, olası problem anında nasıl önlem alınacağı ve de felaket kurtarma sürecinin nasıl yönetileceğini ortaya koyan bir felaket kurtarma planına ihtiyacı bulunmaktadır.

Bu planı hazırlamaya başlamadan önce aşağıda sıralanan iki başlık altında felaket etki ve yönetiminin sınıflandırılması gerekmektedir.

- Doğal afetlerde felaket kurtarma yönetimi
- Teknolojik problemlerde felaket kurtarma yönetimi

Şimdi felaketin etki ve yönetiminin sınıflandırması için belirlediğimiz bu iki ana başlık altında konuları daha detaylı olarak inceleyelim.

3.3.1 Doğal afetlerde felaket kurtarma yönetimi

Deprem, sel, yangın, kasırga, çığ, tusunami, heyalan vb. doğal afetlerde sadece veri merkeziniz ya da sunucu sistemlerinizi kaybetmekle kalmaz bunun yanı sıra ürettiğiniz ürün veya hizmetlerin devamlılığını sağlayan techizat ve sistemleri de kaybetme riskiniz oldukça yüksektir.

Veri merkezleri ve sunucu sistemleri için en zorlu süreçler ve en uzun kurtarma sürelerinin yaşandığı felaket kurtarma yönetimi senaryoları doğal afetler sonucunda meydana gelen felaketlerdir.

Doğal afet durumunda veri merkezinizin ve tüm sistem altyapınızın tamamanı kaybetme riski ile karşı karşıya kalabilirsiniz. Böyle durumlarda felakat kurtarma süreçleri ve uzun kurtarma süreleri gibi zorlukların yaşanmasının yanı sıra yeniden bir veri merkezi kurulması gerektiği için çok ciddi bir maddi yatırımı da beraberinde getirmektedir.

İşletmelerin doğal afetler için yaptırmış olduğu bir sigorta anlaşması var ise bu süreçte oluşacak maddi zararları en az kayıp ile atlatmak için şanslı olacaktır. Eğer işletmenin bu konuda veri merkezi veya veri merkezini barındıran bina için doğal afet durumları için sigorta yaptırmamış ise ve bu maddi zararları karşılamakta güçlük yaşarsa kısa bir süre işletmenin tamamen iflas etmesi kaçınılmaz bir son olacaktır.

Doğal afetlerden sonra ayakta kalabilmiş şirketlerin bu konudaki tecrübeleri incelendiğinde bu afetlerin öncesinde aşağıda sıralanan süreçlerin felaketten önce hazırlandığı ve yapıldığı görülmektedir.

- Felaketlerin işletme üzerindeki iş etki analizleri çalışmaları yapılmış,
- Felaket senaryoları hazırlanmış,
- Felaket süreçleri için mali ihtiyaç ve kaynak analizleri yapılmış,
- İş sürekliliği yönetimi ve felaket kurtarma stratejisi planlanmış,
- İşletme yapısına en uygun felaket kurtarma çözümleri belirlenmiş,
- Felaket süreçlerinde personellerin sorumulukları belirlenmiş,
- IT yöneticileri ve personellerine gerekli eğitim ve bilinç kazandırılmış,
- Felaket kurtarma planı hazırlanmış,
- Felaket kurtarma plan ve senaryoları için belirli aralıklarla tatbikatlar gerçekleşitirilmiş,
- Felaket kurtarma ve yönetim süreçleri dökümanlaştırılmış.

Yukarıda sıralanan tüm felaket kurtarma süreçlerinin felaketten önce hazırlanmış olması olası felaket anında en az hizmet kesintisi, en az veri kaybı ve en az maddi zararlar ile atlatılmasına olanak sağlayacaktır.

Buradan yola çıkarak şu sonucu elde edebilmekteyiz: İşletmelerin ister doğal bir afet gibi tüm veri merkezini kaybetmeye neden olacak problemler, istersede teknik bir problemden kaynaklı hizmet ve servis kesintisine neden olacak riskleri önceden belirleyen, bu riskleri ve etkilerini analiz eden, olası problem anında nasıl önlem alınacağı ve de felaket kurtarma sürecinin nasıl yönetileceğini ortaya koyan bir felaket kurtarma yönetimi sistemine ihtiyacı bulunmaktadır.

Günümüzde doğal afetlerde felaket kurtarma strateji ve çözümleri noktasında genellikle farklı bir çoğrafi konumda kurulmuş felaket kurtarma merkezi ve bulut bilişim çözümleri kabul görmektedir.

Bu tez çalışmasının bir sonraki bölümünde "felaket kurtarma çözümleri" başlığı altında bu iki felaket kurtarma çözüm önerisi hakkında daha detaylı bilgiler ve araştırma sonuçları paylaşılacaktır.

3.3.2 Teknik problemlerde felaket kurtarma yönetimi

Bu bölümde Felaket kurtarma yönetiminin sınıflandırması bölümünün ikinci alt başlığı olan "teknik problemlerde felaket kurtarma yönetimi" hakkında bilgi ve araştırma sonuçları paylaşılacaktır.

Veri merkezlerinde veya sunucu sistemlerinde teknolojik problemlerde felaket kurtarma yönetimi, doğal afetlerde felaket kurtarma yönetimine göre daha kolay yönetilebilir, daha kısa sürelerde ve daha az zararla atlatılabilmektedir. Burada esas olan iyi organize edilmiş bir felaket kurtarma yönetimi ve planıdır.

Veri merkezlerinde veya sunucu sistemlerinde aşağıda sıralanan maddeler en temel teknolojik felaket faktörlerini oluşturmaktadırlar.

- Veri merkezinde elektrik kesintisi
- Sunucularda elektrik kesintisi
- Sunucular işlemci, hafıza, disk, anakart vb. donanım arızaları
- İşletim sistemi problemleri
- Uygulama ve servis kesintileri

Yukarıda belirtilen faktörlerden herhangi birinin yaşanması veri merkezi veya sunucu sistemlerinin tümünü etkilemek yerine sadece belirli bir hizmet veya uygulamada kesintilere yol açacaktır.

Teknolojik problemlerden kaynaklı durumlarda sistemlerin yeniden çalışabilir hale gelme süreleri ve felaket kurtarma çözümleri alternatifleri daha fazladır.

Günümüzde doğal teknolojik problemlerden kaynaklı felaketlerde, felaket kurtarma strateji ve çözümleri noktasında genellikle aşağıda sıralanan çözümler kabul görmektedirler.

- Sunucuların veya verilerin yedeklenmesi (Backup)
- Sunucuların kümelenmesi (Cluster)
- Verilerin başka bir kaynağa veya sisteme yansıtılması (Replikasyon)
- Verilerin ve sunucuların bulut ortamına taşınması (Cloud Computing)

Bu tez çalışmasının bir sonraki bölümünde "felaket kurtarma çözümleri" başlığı altında bu dört felaket kurtarma çözüm önerisi hakkında daha detaylı bilgiler ve araştırma sonuçları paylaşılacaktır.

3.4 Felaket Kurtarma Çözümleri

Felaket kurtarma tek başına bir çözüm ve ya süreç değildir. Felaket kurma içerisinde çözüm mekanizmaları da içermektedir. Bu bölümde işletmelerin veri merkezleri ve sunucu sistemleri için günümüzde gelişen bilgi teknolojilerinin sunduğu felaket kurtarma çözümleri, bu çözümler hakkında bilgiler ve yapılan araştırma sonuçları aktarılmıştır.

Veri merkezi ve sunucu sistemleri için iş sürekliliği stratejilerinin belirlenmesi ve felaket kurtarma yönetimi planlaması süreçlerinde işletmenin mali ve teknik yapısına en uygun felaket kurtarma çözümünü belirlemek en önemli süreç adımlarından biridir.

İşletmenin veri merkezi ve sunucu sistemleri mimarisi için en en uygun felaket kurtarma çözümü belirlenirken hem doğal afetler sonucunda meydane gelecek felaketler hem de teknolojik problemlerde meydana gelecek felaketler için en uygun felaket kurtarma çözümlerinin belirlenmesi gerekmektedir. Böylelikle her iki durum için hazırlıklı olunacaktır.

Günümüzde gelişen bilgi teknolojilerinin veri merkezi ve sunucu sistemleri için sunuduğu, IT yöneticileri tarafından genel kabul görmüş ve sunucu sistemlerinde en yaygın kullanılan felaket kurtarma çözümleri aşağıda sıralanmıştır.

- Kümeleme (Cluster)
- Yansıtma (Replication & Mirror)
- Yedekleme (Backup)
- Bulut Bilişim (Cloud Computing)
- Felaket Kurtarma Merkezi (Disaster Recovery Site)

Yukarıda belirtilen felaket kurtarma çözümlerini işletmenizin veri merkezi ve sunucu sistemleri için iyi bir iş-etki analizi sonucunda planlamanız durumunda bir felaket anında sistemlerinizi veri kayıpsız ve en az kesinti ile yeniden hizmet verebilir hale getirebilirsiniz.

Felaket kurtarma çözümleri olarak yukarıda belirttiğimiz teknolojileri bu tez çalışmasının bir sonraki bölümünde "felaket kurtarma çözümleri" başlığı altında daha detaylı olarak incelenecek ve yapılan araştırma sonuçları aktarılacak.

3.4.1 Kümeleme (Cluster)

Sunucu sistemlerinde felaket kurtarma çözümlerinin temel amacı, veri merkezindeki bilgilerin veya sistemlerin devamlı kurtarılabilir ve çalışabilir halde olmasını sağlamaktır.

Günümüzde işletmelerin her geçen gün artan bilgi teknolojileri ve sunucu sistemleri bağımlılıkları, bu teknoloji ve sistemler üzerinden kullanıcılarına ve müşiterilerine sundukları hizmet veya servislerin kesintiye uğraması artık 0 (sıfır) tahammül ve tolere noktasına gelmiştir (Çözümpark, 2015).

Bu sebep ile IT altyapı ve sunucu sistemlerinin hem kesintisiz çalışmasının sağlanması hem de bu iş için ayırılan kaynakların çok iyi planlanıp yönetilmesi, işletme mali yapısı ve IT altapısına en uygun felaket kurtarma çözümlerinin belirlenmesi görevi de IT yöneticilerine düşmektedir.

Veri merkezlerinde sanallaştırılmış sunucu sistemleri üzerinden sunulan hizmetlerin ve servislerin kesintsiz çalışması için en yaygın kullanılan ve en kolay yönetilebilen felaket kurtarma çözümlerinden biri de kümeleme (Cluster) teknolojisidir. Kümeleme (Cluster) işletmelerin veri merkezleri ve sunucu sistemleri üzerinden sundukları iş süreçlerinin sürekliliğinin sağlanması olarak kısaca tanımlayabiliriz.

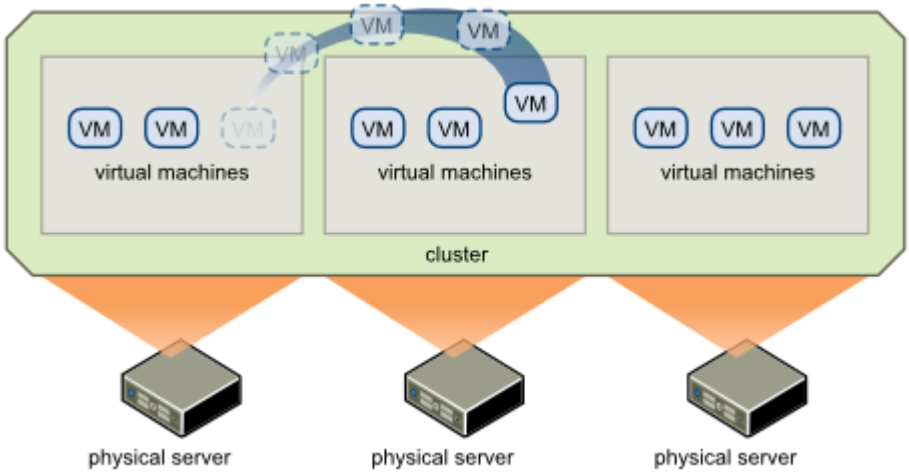
Kümeleme (Cluster), belirli bir amaç için, belirli bir konfigurasyon yapılarak bir araya getirilmiş, kümelenmiş, belli sayıda bilgisayarın, aynı görevi birlikte ya da yedekli çalışmasını sağlayan bir servistir. Kümeleme sisteminde birden fazla sunucu ile oluşturulduğu halde son kullanıcılar tarafından sadece tek bir sunucu gibi gözükecektir. Bir küme (Cluster) oluşturulurken en az iki ve daha fazla sunucuya ihtiyaç bulunmaktadır ve bir küme (cluster) içerisindeki her bir sunucuya "node" ismi verilmektedir. Birden fazla sayıdaki "node" lar bir araya gelerek kümeleri oluştururlar. Kümelerin içerisindeki node sayısı işletmelerin IT altyapı ve sundukları hizmetlere göre değişiklik gösterebilir, arttırılıp ve azaltılabilir (Kulaklı & Aslan, 2010).

Genel olarak incelendiğinde, kümeleme (Cluster) çözümlerinin iki temel amacı vardır bunlar aşağıda sıralanmıştır.

- Süreklilik (continuity)
- Yük dengeleme (Load Balancing)

Süreklilik; Sunucu sistemlerinin her türlü felaket ve arızalara karşı her zaman çalışır durumda kalmasını sağlamaktır. Kümeleme yapılarını geliştirmenin temel amacı kullanıcılara kesintisiz bir hizmet vermektir.

Yük dengeleme; kümelemenin en önemli teknolojisi olarak ifade edilir. Buradaki temel amaç eldeki sunuculardan olabildiğince tüm yetenek ve özelliklerinden yararlanmak ve iş süreçlerinin daha hızlı ve kesintisiz yapılabilmesini sağlamak için sunucu sistemlerine gelen yüklerin (iş isteklerinin) küme içindeki sunuculara eşit oranda dağıtılmasını sağlamaktır (Kulaklı & Aslan, 2010).



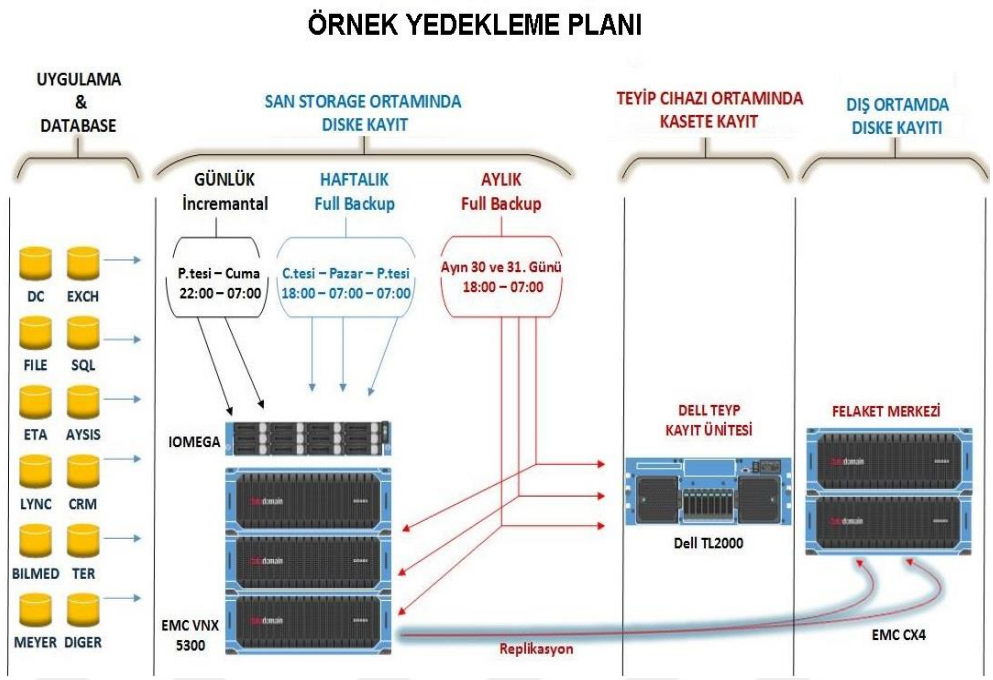
Şekil 3.1 : Kümeleme (Cluster) Mimarisi

Sunucu sanallaştırma katmanı üzerinde tasarlanmış bir kümele (Cluster) mimarisi örneği Şekil 3.1 ’de gösterilmektedir.

3.4.2 Yedekleme (Backup)

Veri merkezlerinde sanallaştırılmış sunucu sistemleri üzerinden sunulan hizmetlerin ve servislerin kesintsiz çalışması için en yaygın kullanılan ve en kolay yönetilebilen felaket kurtarma çözümlerinden biri de yedekleme (Backup) teknolojisidir. Veri yedekleme; veri merkezinizdeki bilgilerin veya sunucu sistemlerinin kurtarılabiliriliği ve kaybedilmesi durumunda tekrar elde edilebilmesi anlamına gelmektedir.

Yedekleme (Backup); sunucu sistemleri üzerinde çalışan yazılımların veya depolanan verilerin servis kesintisi, problem, donanımsal arıza, yazılımsal servis kesintisi ya da beklenmedik bir felaket durumunda müşteri ya da kullanıcılara sunulan hizmtelerin ve işlerin kesintiye uğramasını ve verilerin geri döndürülemez bir biçimde kaybolmasını engellemek amacıyla birden fazla kopya halinde bulundurulmasını sağlayan işlemler bütünüdür (Ulakbim, 2016).



Şekil 3.2 : Örnek Yedekleme Planı

Sanallaştırma teknolojisinin gelişimi ile beraber artık sanal sunucuların da yedeklerinin alınması ve geri dönülmesi çok kolay hale gelmiştir. Fiziksel sunucularda yedekleme işlemi çok zahmetli hemde geri dönülmesi durumunda kesinti yaşnaması ve yedek dosyaların test edilmesi çok düşük olduğu yedek dosyalarının çalışmaması gibi riskler ile karşı karşıya kalıyordu.

Sanallaştırma katmanı ile gelen anlık görüntü kopyası (snapshot) teknolijisi ile sanallaştırma katmanı üzerinde anlık olarak sanal sunucunun bir kopyası alınıp bir problem anında hızlı ve kayıpsız olarak anlık görüntü kopyasına çok hızlı geri dönülebilmektedir. Bu özellik daha çok sanal sunucu üzerinde günlük kritik operasyonlar öncesinde olası problem riskini azaltmak için kullanılan bir yöntemdir, tek başına bir yedekleme çözümü değidir.

Örneğin; bir işletmenin muhasebe departmanına ait kayıtlarının saklandığı yerde yangın çıktığını varsayalım. Eğer işletme bu verilerini başka bir yere de yedekliyorsa, yangın esnasında bütün verilerini kaybetse bile yedekleme sistemi sayesinde işletme için çok değerli olan bu veri kaybı engellenmiş olacaktır. Felaket durumlarında verinin herzaman hazır ve ulaşılabilir halde bulunmasının sağlandığı en önemli yöntemlerin başında gelmektedir (Kulaklı & Aslan, 2010).

Burada ayrıca dikkat edilmesi gereken bir konu var ki o da en az yedekleme kadar önemli bir konu, yedekleme yaptığınız alan yani yedeklenen dosyaları sakladığınız veri yedekleme üniteleri ve üzerlerinde veri disk mimarisidir.

Günlük iş süreçlerinize hizmet veren sunucularınızda herhangi bir problen yaşanmazken yedekleme ünitenizde yaşanacak bir problem de farklı bir teknik felakettir. Buradan şu sonuç çıkarılmaktadır; veri yedekleme planlaması yapılırken veri en az veri yedekleme kadar veri depolama sistemleride çok iyi planlanmalı ve tasarlanmalıdır. Veri depolama sistemleri ve üzerlerindeki veri diskleri için günümüzde en çok kullanılan disk koruma teknolojisi RAID (Reduced Array of Independet Disks) teknolojisidir.

Bu teknoloji veri depolama ortamlarından kaynaklanabilecek hatalar ve dolayısıyla felaket durumlarının en aza indirilmesini sağlamak için yapılmış bir veri saklama ve erişim teknolojisidir. RAID, diskler arasında veri kopyalama ya da veri paylaşımı için birden fazla sabit disk kullanılarak yapılan veri depolama stratejisidir. RAID kullanımının tek disk kullanımına göre yararı, veri bütünlüğünü, hata toleransını ve toplam disk kapasitesini artırmış olmasıdır (Ulakbim, 2016).

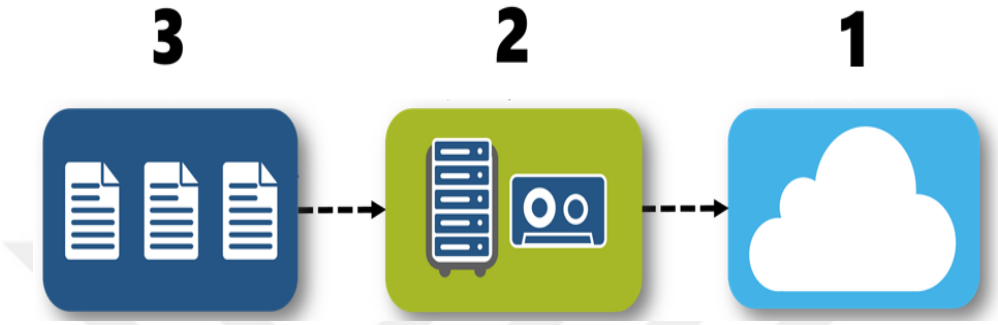
IT altyapı ve sunucu sistemleri üzerinden hizmet veren her işletme için iş sürekliliği ve felaket kurtarma yönetiminde veri büyük önem taşımaktadır.

İşletmeler için büyük öneme sahip olan bu verin yedeklenmesi için iyi planlanmış bir veri yedekleme planına ihtiyaç vardır. Veri yedekleme planı oluştururken aşağıda sıralanan kriterler göre hazırlanması veri yedekleme stratejinizin de belirlenmesine katkı sağlayacaktır.

- Veri yedekleme politikasının belirlenmesi,
- Veri yedekleme sıklığının belirlenmesi,
- Hangi verlerin yedekleneceğinin belirlenmesi,
- Yedeklenen verilerin geri yükleme sürlerinin belirlenmesi,
- Yedeklenen verinin kaç kopyasının olması gerektiğinin belirlenmes,
- Verinin nerede yedekleneceğinin tespiti (Merkez, Uzak konum vs.)
- Verilerin yedekleme ortamlarının belirlenmesi (Disk, Teyp, SAN vb.)

Veri yedekleme yöneticileri tarafından genel kabul görmüş yedekleme stratejisi 3-2-1 kuralıdır. Bu kuralı detaylandıracak olursak;

- 3 - Verilerinizin üç kopyasını alın
- 2 - iki farklı yedekleme ortamında saklayın (Disk, Teyp)
- 1 - Bir kopyasının ana veri merkezi dışında uzak bir bölgede saklayın.



Şekil 3.3 : Backup Stratejisi 3-2-1

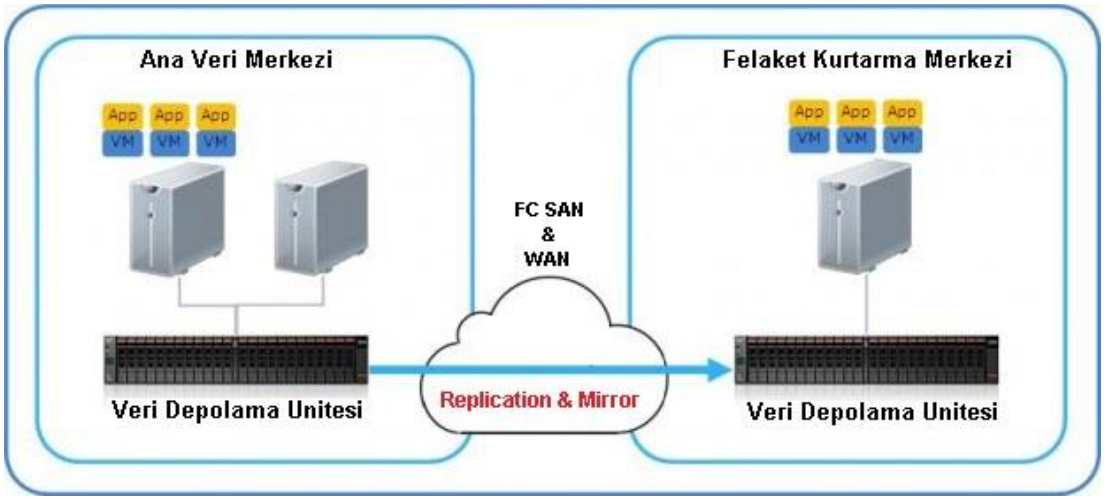
3-2-1 Backup stratejisi görsel olarak Şekil 3.3 ’te gösterilmektedir.

3.4.3 Yansıtma (Replication & Mirror)

Veri merkezlerinde sanallaştırılmış sunucu sistemleri üzerinden sunulan hizmetlerin ve servislerin kesintsiz çalışması için en yaygın kullanılan ve en kolay yönetilebilen felaket kurtarma çözümlerinden biri de yansıtma (Replication & Mirror) teknolojisidir.

Mirror kelime anlamı olarak (ikiz görüntü veya yansıma) şeklinde çevirebiliyoruz, yani bir verinin aynısının başka bir yere yansıtılması veya kopyalanması denilebilir. Daha bilindik bir ifade ile anlatacak olursak “Replikasyon” da diyebiliriz (Çözümpark, 2015).

Replikasyon; güvenilirliği, dayanıklılığı, erişilebilirliği arttırmak için yazılım ve donanım bileşenleri gibi kaynaklar arasında tutarlılığın sağlandığından emin olunarak, bilginin paylaştırılma sürecidir. Bir sistem ve ona ait disklerde bulunan verinin, başka bir sistem ile onun tamamen bağımsız disk setine kopyalanmasına veri replikasyonu ismi verilir (Doğdu & Nihat, 2009). Veri depolama yansıtma işlemi Şekil 3.4 ’te gösterilmektedir.



Şekil 3.4 : Veri Depolama Yansıtma

Veri merkezinde hizmet veren sunucular, personel veya müşterilerin kullandıkları uygulamalar, çalışma dosyaları ve daha birçok gereksinim için ihtiyaç duyduğumuz veri kullanım ve depolama alanları için günümüzde en yaygın kullanılan teknoloji veri depolama (data storage) sistemleridir (Çözümpark, 2015).

İşletmenin günlük tüm IT iş süreçleri ve hizmet veren sunucular bu veri depolama sistemleri üzerindeki disklerde depolanmakta ve bu sistemlerdeki veri alanları üzerinden çalışmaktadır. Bir felaket durumunda kurtarılması gereken en öncelikli sistemlerin başında bu veri depolama üniteleri gelmektedir.

Felaket kurtarma planlarının en kritik seviyeli işleri arasında öncelikle veri depolama üniteleri içerisindeki verilerin minimum kayıp ve kesinti ile felaket kurtarma merkezine veya başka bir veri depolama ünitesi üzerine yedeğinin alınması düzenli olarak sağlanmalıdır.

Veri depolama üniteleri hem fiziksel büyüklükleri hemde sahip oldukları disklerin hassasiyetleri nedeniyle çok fazla yer değişitirlmesi ve taşınması önerilmeyen sistemlerdir. Bu sebeple bu sistemler için en iyi yedekleme ve felaket kurtarma çözümü yansıtma (Mirror & Replication) çözümüdür.

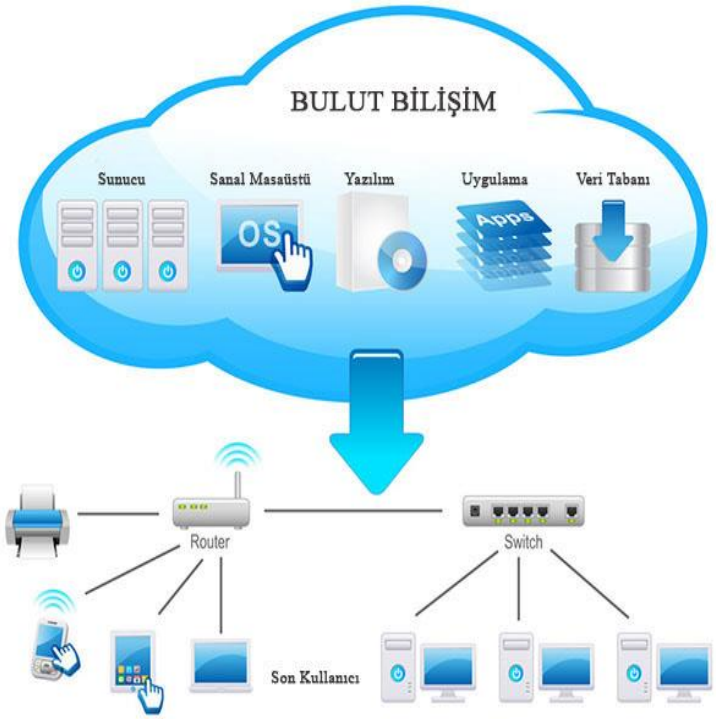
3.4.4 Bulut bilişim (Cloud Computing)

Günümüz gelişen bilgi teknolojileri ve geniş bant internet hizmeti ile beraber bulut bilişim (Cloud Computing) kavramı hayatımıza girmeye başladı.

Veri merkezlerinde sanallaştırılmış sunucu sistemleri üzerinden sunulan hizmetlerin ve servislerin kesintsiz çalışması için en yaygın kullanılan ve en kolay yönetilebilen felaket kurtarma çözümlerinden biri de bulut bilişim (Cloud Computing) teknolojisidir. Bulut bilişim teknolojisi Şekil 3.5 'te gösterilmektedir.

Gelişen sanallaştırma teknolojileri, geniş bant iletişim ağı, fiber kablo teknolojileri ve yüksek kapasiteli donanımların katkısı ile bulut bilişim güçlü ve ekonomik bir IT çözümü haline gelmiştir.

Bulut bilişim; işletmelerin IT birimlerine getirdiği yönetimsel ve mali kolaylıklar sayesinde, hem veri merkezi ve sunucu sistemlerinin yönetilmesi için sunduğu hizmetler hem de felaket kurtarma yönetimi için sunduğu çözümler ile IT yöneticileri ve veri merkezleri için vazgeçilmez bir teknoloji haline gelmiştir.



Şekil 3.5 : Bulut Bilişim Çalışma Yapısı

Bulut Bilişim; işletmelerin tüm Bilgi Teknolojileri Altyapısı, Donanım, Yazılım, Uygulama ve Sistem Yönetim gibi birimlerinin fiziksel temin ve barındırmanın yanı sıra kesintisiz hizmet sunumu gibi önemli rollerini üstlenerek işletmelere bulut servis Sağlayıcıları tarafından IT hizmetlerinin sunulmasıdır (Akıllı, 2015).

Sanallaştırma teknolojileri, bulut bilişimin en önemli yapı taşlarından biridir. Bulut bilişim servis sağlayıcıları tarafından sunulan hizmetler, klasik olarak sanallaştırılmış fiziksel sunucu kaynaklarıdır. Bulut bilişimi daha basit bir ifade ile belirtmek gerekirse sanallaştırılmış büyük fiziksel veri merkezleri de denilebilir.

Bulut bilişim; işletmenizin iş süreçleri için zaman ve mekân kısıtlamasını ortadan kaldırırken bir yandan da iş sürekliliği için oluşacak problemlerini yine sizin için ortadan kaldırıp kesintisiz hizmet sorumluluğu kendi üzerine almaktadır (Akıllı, 2015).

Bulut Bilişim; sadece bir sürekliliği ve felaket kurtarma çözümü değil aynı zamanda işletmeniz için size nerdeyse bütün sistem odası hizmeti sunuyor ve hangi katmanda ne kadar sorumluluk yüklendiğini belirtiyor. Sizden bu hizmet için kullandığınız kadar ödeme yöntemi ile işletmenize ayrıca maddi karlılıklar sağlıyor. Bulut Bilişim hizmeti temel olarak üç farklı tip çözüm ile sunulmaktadır;

- Genel Bulut (Public Cloud) :

Bir hizmet sağlayıcı tarafından hizmetlerin ve altyapının internet üzerinden kendi veri merkezi içerisinde müşterilere sunulduğu bulut (cloud) tipi'dir.

- Özel Bulut (Private Cloud) :

Hizmet ve altyapının müşteri özel ağı içerisinde kendi tarafından sağlandığı cloud tipi'dir. Yani kendi ortamımızdaki fiziksel sistem odamızdır diyebiliriz.

- Karma Bulut (Hybrid Cloud) :

Genel bulut ile özel bulut hizmetleri arasında ile Public cloud arasında noktadan noktaya bağlantı (site to site vpn) ile kullanılan bulut (cloud) tipi'dir (Akıllı, 2015).

3.4.5 Felaket kurtarma merkezi (Disaster Recovery Site)

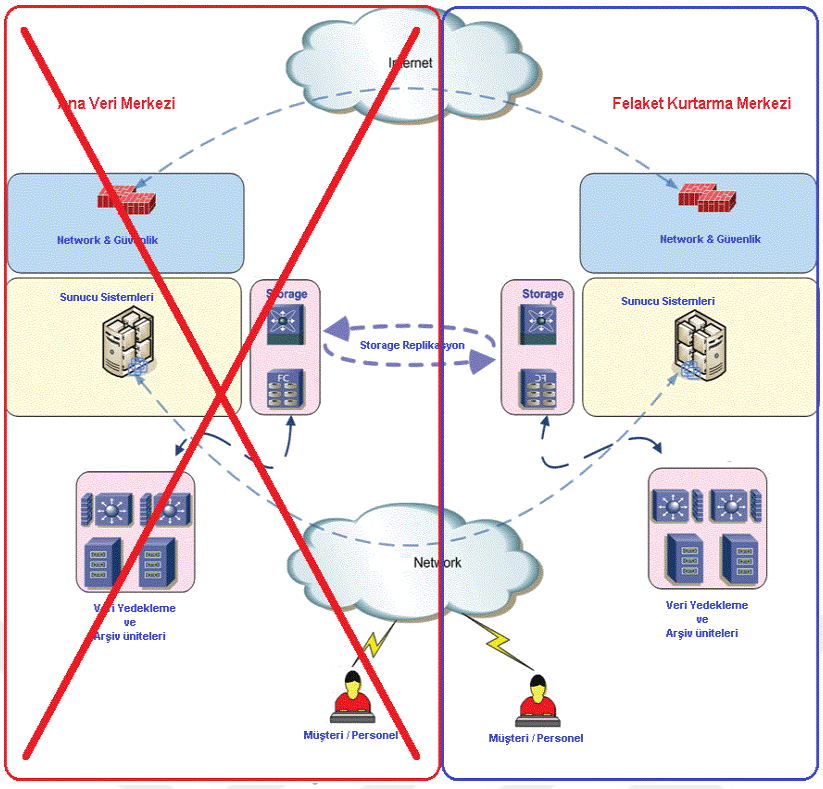
Felaket kurtarma merkezi ya da ana veri merkezinin birebir aynı özelliklerine sahip ikinci bir veri merkezi daha kurmak işletmeler açısından felaket kurtarma çözümleri arasında en yüksek maliyetli ve en çok yönetimsel iş yükü getiren çözümüdür.

Felaket kurtarma merkezi, ana veri merkezindeki fiziksel altyapı ve donanımsal sunucu kaynaklarının birebir aynısı olacak şekilde tasarlanır, ana veri merkezinden farklı bir coğrafi alanda konumlandırılırlar. Böylelikle bir felaket yaşanması durumunda tüm IT hizmetleri ve iş süreçleri en kayıp ve en az kesinti süreleri ile atlatılmış olacaktır.

Felaket kurtarma merkezleri oldukça maliyetli bir çözümdür, bu sebeple genelde büyük finans kuruluşları, telekom operatörleri, kamu kurumları ve büyük sanayi kuruluşları tarafından tercih edilen bir çözümdür.

İşletmelerin, iş sürekliliği ve felaket kurtarma yönetimi için felaket kurtarma merkezi (FKM) çözümünü tercih etmeleri durumunda bu çözümün işletmeye getireceği mali ve yönetimsel zorlukların neler olduğu temel başlıklar halinde aşağıda sıralanmıştır.

- FKM sunucu donanım ve yazılım giderleri
- FKM Sunucu bakım ve onarım giderleri
- FKM Sunucu Yazılım destek giderleri
- FKM Sistem odası altyapı giderleri
- FKM Enerji giderleri
- FKM Soğutma giderleri
- FKM Güvenlik ve izleme giderleri
- FKM İnsan kaynağı
- FKM Yönetim giderleri
- FKM Sistem süreklilik giderleri



Şekil 3.6 : Felaket Kurtarma Merkezi

Şekil 3.6' da da görüldüğü üzere felaket kurtarma merkezi, ana veri merkeziniz ile birebir aynı özelliklerde kurulmaktadır. Yine yukarıda sıralanan kriterler dikate alındığında felaket kurtarma merkezinin işletmeler için neden yüksek maliyetli ve yönetimsel zorluklar getirdiği daha net anlaşılmaktadır.

Felaket kurtarma merkezi çözümü yüksek maliyetli bir çözüm olduğu için günümüz global teknoloji üreticileri ve servis sağlayıcılar kendi bünyelerinde ortak kullanıma açık büyük veri merkezleri kurmaya başlamışlardır.

Kurdukları bu büyük veri merkezlerindeki IT altyapı ve sunucu sistemleri hizmetlerini, sanallaştırma ve bulut bilişim teknolojileri sayesinde orta ölçekli birçok işletmeye IT ve felaket kurtarma çözümü olarak sunmaktadırlar. Günümüzde Microsoft Azure, Amazon Cloud, VMware Cloud gibi global teknoloji firmaları bu hizmetleri sunmaktadırlar.

Ülkemizde de telekom operatorü ve büyük ölçekli teknoloji firmaları veri merkezi kiralama, bulut bilişim altyapı hizmetleri ve iş sürekliliği çözümlerini kurdukları büyük veri merkezleri üzerinden küçük ve orta ölçekli işletmeleri IT ihtayçlarını karşılamaktadırlar.

Türk Telekom veri merkezi, Turkcell veri merkezi, Sadece hosting gibi firmalar bu işin öncülüğünü üstlenmektedirler.

3.5 Türkiyede Gerçekleştirilmiş Felaket Kurtarma Projeleri

Bu bölümde Türkiye'de veri merkezi ve IT servisleri için felaket kurtarma projeleri geliştirmiş işletmelerin yapmış oldukları çalışmalar hakkında bilgiler sunulmaktadır.

3.5.1 Simit Sarayı

Simit Sarayı, veri merkezi ve IT servisleri için başarılı bir felaket kurtarma projesi yapmış işletmelerden biridir.

Projeye başlamadan önce Daikin'in çözmeye çalıştığı problemler nelerdi?

Simit Sarayı tüm üretim ve satış süreçlerinin kesintisiz çalışması için İstanbul merkez ofisi dışında farklı bir şehirde bulunan bir veri merkezinde sunucu kiralayarak felaket kurtarma merkezi ihtiyacını çözüyordu.

Felaket kurtarma senaryosu ve geliştirme platformu için esnek ve çevik bir altyapıya ihtiyaç duyuluyordu. Seçilecek çözümün maliyet avantajı getirmesi de bekleniyordu.

Simit Sarayı'nın proje sonrasında elde ettiği faydalar

Azure kullanımının en büyük faydası Simit Sarayı'na sağladığı esneklik oldu. SAP geliştirme ortamlarında ihtiyaç duyulan iş yükleri için altyapı dakikalar içinde sunulabilir duruma geldi.

Aynı şekilde Azure'un ölçeklenebilirliği de büyük fayda sağladı. Projenin hayata geçmesinden önce dosya sunucularında departmanlar için kota uygulanırdı fakat bulut entegre mimarisi sayesinde neredeyse sınırsız boyutta dosya sunucuların erişim mümkün oldu.

Düşük ve ön görülebilen maliyetlendirme ile Felaket Önleme Merkezi kuruldu. Bu felaket önleme ortamı aynı zamanda tüm yapının yüksek erişilebilirliğine de büyük katkı sağladı. Birden fazla lokasyon üzerinde dosyaların ve hizmetlerin barındırılmasından dolayı kesinti riski neredeyse sıfıra indi.

Burada Microsoft'un Azure için sunduğu SLA'ler de çok önemli. Güvenlik ve erişilebilirlik kriterleri IT departmanının ISO 27001 gibi süreçlere hazırlığında da fayda sağladı. Yıllık Felaket Kurtarma Merkezi maliyetlerinin %30- 40 arasında azalmasını bekleniliyor (Microsoft Azure, 2015).

3.5.2 Daikin

Daikin, veri merkezi ve IT servisleri için başarılı bir felaket kurtarma projesi yapmış işletmelerden biridir.

Projeye başlamadan önce Daikin'in çözmeye çalıştığı problemler nelerdi?

Daikin, felaket kurtarma merkezi ihtiyacını İstanbul merkez ofisi dışında bulunan bir veri merkezinde sunucu kiralayarak çözümlüyordu. Ancak, yerel bir sağlayıcıdan aldığı bu hizmette diğer birçok kullanıcının yaşadığı sorunları yaşıyordu. Kiralama maliyeti, bant genişliklerinde yaşanan sıkıntılar, esnek altyapı imkânının olmaması, taleplerin hızlı bir şekilde karşılanamaması, tedarikçinin ek maliyet ve taahhüt talepleri bu sorunlardan sadece birkaçıydı.

Daikin'in proje sonrasında elde ettiği faydalar

Azure ile tüm temel iş ihtiyaçları çok uygun bir maliyetle karşılanıyor. Azure'un ASR (Azure Site Recovery) Servisi ile Daikin, 10-12 saniye seviyelerinde RPO (Recovery Point Objective) değerlerine ve 3 dakika seviyesinde RTO (Recovery Time Objective) değerlerine sahip bir felaketten kurtarma çözümüne sahip oldu.

Azure'un Yedekleme Servisi ile Daikin, depolama alanı endişesi olmadan mevcut tüm verilerinin yedeklenmesi çözümüne sahip olurken, geriye dönük yedek saklama sürelerindeki sınırlandırmalardan da kurtuldu. Gelecekteki kapasite artırımları için sipariş, on-prem storage temini, kurulum vs. tüm iş yüklerinden kurtuldu (Microsoft, 2015).

4. FELAKET KURTARMA PLAN ÖNERİSİ

Tez çalışmasının bu bölümünde, işletmelerinin sahip olduğu veri merkezi, sunucu sistemleri ve IT servisleri için kendi işletmelerine özgü bir felaket kurtarma planı hazırlamak isteyen IT yönetici ve uzmanlarına bu süreçte nasıl başlamaları gerektiği, hangi kriteleri yerine getirmleri gerektiği ve felaket kurtarma planının yazılması sürecinde nelere dikkat edilmesi gerektiği gibi konularda katkı sağlamaktır.

İşletmelerin veri merkezi, sunucu sistemleri ve IT servislerinin devamlılığının sağlanması, veri merkezinin tümünü veya sunucu sistemleri ile IT servislerinin bir bölümünü çalışamaz duruma getirebilecek beklenmedik bir felaket durumunda, hem felaket kurtarma sürecini etkin yönetebilmek hem de en az maddi zarar ve hizmet kesintisi ile atlatmak için "Felaket Kurtarma Planı" hazırlamak isteyen veri merkezi ve IT yöneticilerinin felaket kurtarma planlanlama sürecinde dikkat edilmesi gereken en önemli kriterler hakkında bilgiler yine bu bölümde sunulmaktadır.

4.1 Felaket Kurtarma Planı

Bu bölümde; işletmelerin veri merkezi, sunucu sistemleri ve IT servislerinin devamlılığının sağlanması, veri merkezinin tümünü veya sunucu sistemleri ile IT servislerinin bir bölümünü çalışamaz duruma getirebilecek beklenmedik bir felaket durumunda, hem felaket kurtarma sürecinin etkin yönetebilmek hem de en az maddi zarar ve hizmet kesintisi ile atlatmak için "Felaket Kurtarma Planı" hazırlamak isteyen veri merkezi ve IT yöneticilerinin felaket kurtarma planlanlama sürecinde dikkat edilmesi gereken en önemli kriterler hakkında bilgiler sunulmaktadır.

Felaket kurtarma planı; veri merkezleri ve IT yöneticileri için artık bir seçenek olmaktan çıktı. Güvenilir IT servisleri her işletmenin devamlılığı için en önemli yapı taşlarından biri haline gelmiş durumda. Bilgi teknolojilerinin sürekliliğini garantilemek için işletmeler artık bir felaket kurtarma planı hazırlamak zorundalar.

Bilgi güvenliğinin ve IT servislerinin bu düzeyde öneme sahip olmasına rağmen şaşırtıcıdır ki bu konuda ülkemizde yapılmış ve yazılmış çok az çalışma var. Bu konuyla ilgili IT sektöründe kapsamlı ve tam anlamıyla oturmuş çalışmalar çok az sayıda, bu yüzden önerilen bu felaket kurtarma planı öneri çalışması IT yöneticisi ve çalışanlarına IT altyapı ve veri merkezleri için felaket kurtarma planı oluşturmada bir klavuz niteliği taşıması hedeflenmektedir.

Bu plan önerisinde herhangi bir felaket durumuyla karşı karşıya kalınması durumunda işletme için hayati önem taşıyan tüm bilgileri kayıtları ve sunucu sistemlerinizi kurtarmanızı sağlayacak etkin bir çözüm sunmaktadır.

Bu çalışma veri merkeziniz veya sunucu sistemleriniz için problem ve kesintilere sebep verebilicek durumlarla başa çıkabilmek için gerekli çalışmaları sunan, IT sektöründe genel kabul görmüş felaket kurtarma çözümleri ve felaket kurtarma yöntemleri de incelenerek oluşturulmaya çalışılmış bir felaket kurtarma yönetimi plan önerisidir.

Felaket kurtarma planının ilk basamağında kriz yönetimi planlama sorumluları ve müdehale ekibi yer almaktadır. Bu aşamada herhangi bir kriz durumunda üst düzey koordinasyon sağlanarak felaket kurtarma çalışmaları daha kolay yürütülebilir ve yönetilebilir hale getirilmiş olacaktır.

Dünya genelinde işletmeler iş sürekliliğini sağlayabilmek için giderek IT sektörüne bağımlı hale gelmektedir. Olası bir felaket durumunda direkt olarak IT sistemlerine ve IT altyapısına bağlı olan bu sistemler üst düzey çalışmaları gerektirir. Sonuç olarak denilebilir ki; iş sürekliliği planlaması direkt olarak iş süreçlerini de etkilemektedir.

İş sürekliliği olası bir felaket durumunda firmanın yürürlüğe sokacağı iş ve işlemler dizisini kapsar. İş sürekliliği planlaması kritik servislerin olası bir felaket durumunda hasar görmemesi veya durmaması için gerekli çalışmaları içerir ve bu sürecin mümkün olduğunca en az zararla atlatılmasını hedefler.

Felaket kurtarma planı ise içerisinde planlama, gelistirme ve test etme çalışmalarını barındırır. Olağan dışı bir felaket durumunda temel iş fonksiyonlarının etkili ve yeterli bir şekilde sürdürülmesini sağlar.

Günümüzde büyük veya küçük tüm kurumların iyi bir "Felaketten Kurtarma Planı" (FKP) olması gerekir. Bu plan mümkün olduğunca kapsamlı olmalı, kritik iş süreçlerinin felaket sonrası devamını, diğer önemli süreçlerin en kısa sürede başlatılabilmesini ve devamında kurumun normal işleyişe dönebilmesini sağlamalıdır. Bu plan aynı zamanda veri yedeklerinin de saklanmasını ve geriye dönülebilmesini öngörmeli ve veri kaybının olmamasını sağlamalıdır (Doğdu & Nihat, 2009).

4.1.1 Giriş

Bu bölümde felaket kurtarma planlama sürecine nasıl başlanılması gerektiğine dair yapılan çalışma ve araştırmalar ışığında bilgiler aktarılmıştır.

Günümüzde veri merkezi, sunucu sistemleri ve IT servislerini kullanan işletmeler incelendiğinde; küçük ölçekli, orta ölçekli, büyük ölçekli, ulusal ölçekli ve uluslararası ölçekli olmak üzere neredeyse her ölçekte işletmelerin olduğunu görmekteyiz. Durum böyle olunca da işletmenin ölçeğine göre veri merkezi, sunucu sistemleri ve IT servisleri de farklılık göstermektedir.

Böyle farklı ölçeklerdeki veri merkezi, sunucu sistemleri ve IT servisleri için felaket kurtarma çözümleri ile felaket kurtarma planları da farklılık gösterecektir.

Uluslararsı ölçekli bir işletme ile küçük ölçekli bir işletmenin felaket kurtarma planlarının aynı olması beklenemez, ayrıca uluslararası ölçekli bir işletmeninin felaket kurtarma planının küçük ölçekli bir işletme için felaket kurtarma planı olarak uyarlanması doğru bir sonuç vermeyecektir.

Felaket kurtarma planı, küçük ölçekli işletmeden uluslararası işletmeye doğru veri merkezi, sunucu sistemleri ve IT servisleri bazında farklılık göstereceği için tek bir felaket kurtarma plan şablonu oluşturma mümkün ve doğru bir yöntme değildir. Bu sebepten dolayı IT yöneticisi ve iş sürekliliği uzmanları kendi veri merkezi, sunucu sistemleri ve IT servisleri için işletmelerine özgü bir felaket kurtarma planı oluşturmaları gerekmektedir.

IT uzmanlarının birçoğu maalesef döküman hazırlama alışkanlığına sahip değildirler. Yine IT uzmanlarının birçoğu felaket kurtarma planı gibi çok detaylı ve onlarca sayfadan oluşan bir dökümanı hazırlanmakta ise daha çok başka birileri tarafından hazırlanmış dökümanlardan kopyala-yapıştır yöntemi ile Felaket kurtarma planı oluşturmayı tercşh etmektedirler. Bu şekilde hazırlanmış bir Felaket kurtarma planının da işletmeye gerçek anlamda fayda sağlamasını beklemek doğru olmayacaktır.

Farklı bir işletmenin kendine özgü oluşturduğu felaket kurtarma planını kopyala-yapıştır yöntemi ile alıp bir felaket kurtarma planı hazırlamak yerine, kendi işletme yapınıza uygun analizleri yapıp en uygun felaket kurtarma süreçlerini tanımlayarak ve felaket kurtarma çözümlerini tercih ederek hazırlayacağınız size özgü bir felaket kurtarma planı, size daha etkin felaket kurtarma yönetimi sağlamanının yanı sıra işletmenize ise çok daha fazla fayda sağlayacaktır.

Kendi işletmenize özgü bir IT felaket kurtarma planı hazılamak , kapsamlı, ettkin ve doğru organize dilmiş bir IT Felaket Kurtarma Planına sahip olmak için için aşağıda sıralan tüm süreçlerin eksiksiz olarak tamamlamanız bu süreçte size oldukça katkı sağyalacaktır.

- Felaket kurtarma yönetim planının amaç ve kapsamının belirlenmesi
- Veri merkezi sunucu sistemleri donanım ve yazılım envanterinin oluşturulması
- Sunucu sistemleri ve IT servisleri için felaket iş-etki analizlerinin yapılması
- Sunucu sistemleri ve IT servisleri için RTO ve RPO değerlerinin belirlenmesi
- İşletme IT altyapısına en uygun felaket kurtarma çözümlerinin belirlenmesi
- Felaket kurtarma operasyon ekipleri ve sorumluluklarının belirlenmesi
- İş kritik sunucu sistemleri ve operasyon kurtarma önceliklerinin tespit edilmesi
- Olası felaket Senaryoları ve kesinti problemlerinin belirlenmesi
- Felaket kurtarma yönetim ve operasyon sorumlusu personellerin belirlenmesi
- Felaket kurtarma çözümleri ve süreçleri için maili bütçe hazırlanması
- Felaket kurtarma merkezinin hazırlanması, iletişim ve ulaşım planlanmsı
- Destek alınacak tedarikçiler ve teknik destek firmaların belirlenmesi
- Peryodik olarak felaket kurtarma planın test edilmesi

4.1.2 Hazırlık ve planlama

Bu bölümde veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli ve ilk adımı olan "Hazırlık ve Planlama" sürecine dair yapılan çalışma ve araştırmalar ışığında bilgiler aktarılmıştır.

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin ilk ve en önemli adımlarından biri felekat kurtarma planı "Hazırlık ve Planlama" süreci" dir. İşletme yapınız ve IT servisleriniz için etkin ve doğru planlanmış bir felaket kurtarma planı sunucu sistemlerinizde meyadana gelebilecek beklenmedik teknik ve doğal afetlere karşı koruma ve iş sürekliliğini sağlamanın en iyi yoludur.

Veri merkezi, sunucu sistemleri ve IT servsileri için Felaket kurtarma planı oluşturmak isteyen IT yönetcileri hazırlık ve planlama süreçlerinde neler yapmalıdır, bu konular iki bölüm olarak incelenecektir. İlk olarak hazırlık aşamasında neler yapılması gerektiği ile başlayalım.

Hazırlık ?

İşinizin devamlılığı için veri merkezini sizin için en kritik yerdir ne var ki bazen elde olmayan sebeplerden kontrolümüzün dışında IT servisleriniz ulaşılamaz ya da sınırlı ulaşılabilir hale gelebilirler.

Bu durum nadirde görülse, işinizi büyük ölçüde aksatabilir, piyasanızı, müşterilerinizi ve hatta güvenirliğinizi etkileyebilir. İşletmenizi bu tehditlerden alanları korumak için iyi bir felaket kurtarma çözümü geliştirerek ortadan kaldırabilirsiniz.

Akıllıca kurulmuş bir sanal altyapı üzerine iyi kurulmuş ve iyi planlanmış bir felaket kurtarma çözümü iş süreçlerinizin devamlılığını kontrol altında tutmak için gerekli RTO ve RPO değerlerini size sağlayabilir.

Felaket kurtarma planlarınız hasarsız bir şekilde test edilebilir ve tipik felaket kurtarma gereklilikleri dışında IT departmanınıza fayda sağlayabilir. Felaket kurtarma planınızın çalışması ve kesin başarısı için altyapınız en kritik yere sahiptir. Sanallaştırılmış bir altyapının en güvenilir ve en az masraflı platform olduğu bilinmektedir.

En kritik uygulama ve verilerinizi belirleyin; en kıymetli uygulamalarınız hangileri güvenlik gerektiren? ya da iş sürekliliğinizi etkileyecek olanlar. Hangi bilgiler müşterileriniz için kesinlikle olmazsa olmaz, iç hesaplarınız finansman ve diğerleri gibi.

Kritik sistem ve uygulamalarınızı sanallaştırın; bu sadece sizin iş yoğunluğunuzu ve masraflarını azaltmakla kalmaz aynı zamanda ortamınızı Felaket kurtarma planlaması için daha müsait hale getirir. Sanal ortamlar çok daha kullanışlıdır ve taşınması çok daha kolaydır. Sanallaştırma, bireysel unsurları ve hareketli parçaları koruyarak karmaşıklığı giderir bu da planlamayı kolaylaştırır ve felaket kurtarma aşamasında yalınlık ve yönetilebilirlik katar.

RTO ve RPO değerlenizi gerçekçi olarak belirleyin; hangi bilgileri kaybedebilirsiniz? Ne kadar süreyle? kritik uygulamalarınız için ne zaman geri online olacaksınız? hedeflerinizin ulaşılabilir, gerçek ve doğruluğundan emin olun. Otomatik olarak planlanmış felaket kurtarma sistemleri çok güçlü olabilir ancak sihirli değnek gibi de görülmemelidir. Örneğin Exchange, Oracle, SQL ve SAP içeren 100 Sanal makine 30 dakika içerisinde failover edilip yeniden dönülemez. Sınırlarınızı ve sürelerinizi (RTO ve RPO) belirlemek için farklı durumlarda testlerinizi yapın ve sonuçları gözlemleyin.

Veri yedekleme ve geri yükleme prosedürlerinizi oluşturun; Failover (felaket durumunda sistemi ve hizmetleri üzerine alma) ve failback(felaket bittikten sonra sistemi ve hizmetleri eskiye geri döndürme) süreleri nelerdir belirleyin. Ortaya çıkan sonuç sizin koruma düzeyiniz ve geri yokleme hızınız ve masraflarınızla uyumlumudur anlarsınız.

Veri ve sistem yedeklerinizi güncel tutun; felaket kurtarma merkezi, veri yedeklme sistemleri ve veri depolama sistemlerinde mümkğn oldukça sık verilerinizi yedekleyin. Bu sayede bir felaket durumunda daha az veri kaybı ve sistem kesintisi yaşamış olursunuz. Ayrıca RTO değerlerinizi en az eforla karşılamış olursunuz.

İş ve operasyon süreçlerini otomatikleştirin; Yolunuzu insan hatalarının kesmesine izin vermeyin. Otomatik felaket planları yaparsanız uygun otomasyon sayesinde Felaket kurtarma işlemleriniz haftalar yerine dakikalar içerisinde yapılabilir hale getirilmiş olur. Bu sistem kullanıcıların işlemin birçok sürecini yönetime zorluğunu ortadan kaldırır ve işlem aktiviteleri olarak planlar. Network ve sanal makine konfigürasyonun önceden yapılması, uygulamaları yeniden başlatma gibi işlemleri kendiliğinden otomatik olarak yapar.

Risk yönetimini doğru planlayın; IT servislerinde yaşanan birçok kesinti felaket sebepli değildir, aksine planlanmış prosedürlerdeki aksama yüzündendir. IT sistemleri ve servisleri üzerinde yapılacak güncelleme ve yükseltme gibi işlemlerin nasıl yapılacağını önceden belirleyen prosedürler hazırlayın ve bu prosedürlere uygun işlem yapılmasını sağlayın.

Sorumluluk verin; felaket kurtarma planı içerisindeki herkese bireysel sorumluluklar verin. İlgili personellerin her zaman hazırda bulunup hemen kontrole geçmesini sağlar hale getirin.

Felaket sonrası normale dönüş planınızı hazırlayın; yaşanan bir felaket ve sonrasında yapılan bir felakat kurtarma, tam bir felaket kurtarma planı oluşturmaz. Felaket kurtarma bittikten sonra sistemleri eski orjinal çalışma ortamlarına geri döndürülmesi (failback) sürçlerininde planlanması gerekmektedir.

Çözüm ortağınızı seçin; felaket durumunda size IT altyapı ve sunucu sistemleri ile ilgili tedarik ve destek süreçlerinde yardımcı olacak firmayı önceden belirleyin. Bu size falaket anında hızlı geri kurtarma ve kolay kriz yönetimi katkısı sağlayacaktır.

Felaket kurtarma için maili kaynak planlaması yaptırın; işletmeniz için maliyet-etkin ve fiyat-performans kritelerine en uygun felaket kurtarma çözümünü tercih edin mali açıdan planlamayı da iyi yapın ki geri dönüşe işeminde yapılan masraflara değsin.

Yukarıda maddeler halinde incelediğimiz “Hazırlık” süreçlerinde yapılan işlemler; veri merkezi, sunucu sistemleri ve IT servislerimiz doğru ve etkin bir felaket kurtarma planlaması için en uygun hale getirme çalışmaları olarak tanımlayabiliriz.

Bir diğer bölüm ise “Planlama” sürecidir. Bu süreçte ise işletme organizasyonu, veri merkezi, sunucu sistemleri ve IT servisleri için en uygun felaket planlama kademesi ve felaket kurtarma çözümlerini belirlemek için yapılan çalışmalardır.

Planlama ?

Günümüzde IT felaket kurtarma planlaması, bilgi teknolojilerindeki diğer trentlerin arkasında kalmış durumda, kamu işletmeleri her ne kadar güvenli olduklarını düşündükleri sistemlere sahip olsalar da IT felaket kurtarma planları bilgiyi geri dönmede ve veri kaynaklarını depolama metodlarını tasarlamada yetersiz kalabilmektedirler.

Bilgi işlemin tüm iş süreçlerinize entegre olması ve teknolojiye güven konusu göz önüne alındığında felaket kurtarma planı görüşü bazı işletmelerde hala “olmasada olur” düşüncesinin olduğu görülebilmektedir.

Böyle düşünce yapısına sahip işletmelerde iş süreçleri ve işletme yapısındaki hızlı değişimler IT felaket kurtarma planını tasarlanırken temel olarak dört noktaya yenilikler getirilmesi gerekiyor. Bu dört nokta aşağıda sıralanmıştır.

IT felaket kurtarma planı ve iş sürekliliği planı terimlerinin doğru tanımlanması, aralarındaki fark ve benzerliklerin belirlerlenmesi.

İş sürekliliği planları; iş sürekliliği planları sadece felaket değil işletmenin günlük normal işleyişi ve devamlılık süreçlerinin belirlendiği stratejilerdir ve felaket sonrası iş operasyonlarının çalışır hale gelmesini sağlar.

IT felaket kurtarma planları; IT felaket kurtarma planları özellikle IT servislerini yeniden başlatmayı hedefler. Şu durumda denilebilir ki; felaket kurtarma planı iş sürekliliği planını destekler niteliktedir. Felaket kurtarma planlarının hedefleri ve amaçları iş sürekliliği planlarınınki ile çelişmemelidir.

Hangi olayların IT servisleri için felaket olarak kabul edeceği ve felaketlerin niteliklerinin belirlenmesi.

Eğer IT hizmeti aldığınız bir üretici veya tedarikçi iş ortağı firmanız herhangi bir şekilde size servis sağlayamadıysa bu durumda kullanıcıları bir IT felaketiyle karşı karşıyadır. IT felaketleri bir dosyanın yanlışlıkla silinmesinden tutun da veri merkezinin bulunduğu binayı etkileyecek bir kasırgaya kadar çeşitlilik gösterebilir.

IT felaketleri veri merkezindeki destekleyici altyapı hasarlarından (kablolama, güç kaynağı vb.) da kaynaklanabilir. Bu olaylar IT servislerini sağlayan sistemlerinizin çalışamaz hale gelmesine neden olabilir. Olay bu boyuta geldiğinde de artık IT servisleri hizmet sunamaz hale gelir ve bir felaket olayı ortaya çıkmış olur.

Felaket kurtarma planının kullanım amacının tanımlanması ve işletme üzerindeki etkilerinin belirlenmesi.

Unutulmamalıdır ki felaket kurtarma beliri bir donanım ya da yazılım sistemi için değil, tüm bilgi işlem servislerinin kurtarılması için kullanılır.

Örneğin; internet erişimi, telekomunikasyon, veri depolama ve işleme gibi IT servisleri diğer ilgili departmanlara ekstra yeterlik sağlayarak değer katar. Bu servislerin tüm özelikleriyle işletmeye yarar sağlaması için diğer kaynaklardan gelen içeriklerin eşleşmesine de bağlıdır. (donanım, yazılım, veri, insan kaynakları)

Bu içeriklerin herhangi bir felaket anında zarar görmesi durumunda felaket öncesi koşullara geri dönmek bazen mümkün ya da uygun olmayabilir.

IT felaket kurtarma planı'ın sadece bir işlem veya operasyon olmadığı, bir süreçler bütünü olduğunun bilinmesi.

Felaket kurtarma planlaması sadece bir basitleştirme ya da IT servislerinin kesintilerini azaltma işi değildir. IT Felaket kurtarma planının amacı sadece IT servislerini kolay geri yüklenebilir hale getirmek değildir ya da görevi sadece IT servisleri için problemleri azaltma değildir. Tüm bunlar önemli kriterler olduğu halde tek başlarına birer IT felaket kurtarma planınını oluşturmazlar.

Örneğin; Yedekleme teknolojisi uzun zamandır felaket kurtarma planının önemli bir parçası olarak görülüyor ancak yedekleme tamamen ayrı tek başına bir yapı değildir.

Veri merkezleri ve IT servisleri için felaket kurtarma planı veri koruma seviye ve stratejilerine göre genel olarak 4 kademede (Tier) incelenebilir, bu kademeler ilk olarak aşağıdaki tabloda gösterilmiştir.

Bilişim sektörünün en önemli elemanlarından biri olan veri merkezleri için de bazı standartlar mevcut. Bunlar arasında en çok kabul gören ise TIER sertifikaları. "Uptime Institute" tarafından verilen bu sertifikalar veri merkezlerini; uygulama, yönetim ve tasarım konusunda değerlendiriyor. Değerlendirme sonunda belli değerleri yakalayan firmalar da derecelerine göre TIER sertifikası almaya hak kazanıyor (Itadvisor, 2012).

Çizelge 4.1 : Felaket Kurtarma Planı Kademeleri

Felaket Kurtarma Planı Kademeleri		
Kademe Seviyesi		**Veri Koruma Metod ve Çeşitliliği**
Kademe 0: (Tier 0)		FKP (Felaket Kurtarma Planı) Yok - Veri Yedekleme Yok
Kademe 1: (Tier 1)		FKP + Off Siste Veri Depolama ve Yedekleme Var
Kademe 2: (Tier 2)		FKP + Off Siste Veri Depo. Veri Yedek. + Donanım ve altyapı yedekliliği
Kademe 3: (Tier 3)		FKP + Kademe 2 + Yedekli Veri Merkezi
Kademe 4: (Tier 4)		FKP + Kademe 3 + Aktif 2. Veri Merkezi

Kademe 0 (Tier 0) :

Tek alanlı data merkezini tanımlar yedekleme yada felaket kurtarma işlemlerine ihtiyaç duyulmayan yapıdır. Bu basamakta firmaya ait kayıtlı bir bilgi yoktur, dökümantasyon yoktur ve bir beklenmedik durum riski yoktur.

Bu basamakta olan işletmeler herhangi bir felaket durumunda verilerini asla kurtaramazlar. İşletmenin kurtarılma zamanı tahmin edilemez, birçok durumda tam anlamda tüm alanlarda uygulama ve sistemlerde tam bir kurtama sağlanamaz.

Kademe 1 (Tier 1) :

Bu kademedeki veri merkezine ve IT servislerine sahip işletmeler; bir felaket kurtarma planı olan, bilgilerini ana veri merkezi dışında (offsite) bir depolama alanında saklayan, yedekleyen ve bu süreçleri devamlı takip eden işletmelerdir.

Bu işletmelerde düzenli olarak veri ve sistem yedeklemesi yapılır, veriler ana veri merkezi dışında (offsite) bir veri depolama ünitesinde depolanır. Böylelikle bir felaket durumunda veri merkezini kaybetmeleri halinde, veri merkezlerindeki tüm donanımları kaybetmiş olmalarına rağmen en azından işletme verilerini kaybetmemiş olurlar. Tekrar yeni bir veri merkezi kurduklarında yedekledikleri işletme verilerini geri yükleyebilecek bir yedekleme platformuna sahiptirler. Ancak bu kademedeki veri merkezlerinin Kurtarma süreleri de donanımların tekrar tedarik edilmesi ve yeni altyapı için düşünülen binanın hazırlanma süresine bağlıdır.

Kademe 2 (Tier 2) :

Bu kademedeki veri merkezine ve IT servislerine sahip işletmeler; Kademe 1 deki yapının yanı sıra, veri merkezindeki kritik iş süreçlerine hizmet veren IT servisleri için yedek sistemler, donananım ve altyapı kaynaklarını bir felaket anında kullanmak üzere hazırda bulundururlar.

Bu işletmelerde düzenli olarak veri ve sistem yedeklemesi yapılır, veriler ana veri merkezi dışında (offsite) bir veri depolama ünitesinde depolanır. Bir felaket durumunda veri merkezini ve kritik IT servislerini kaybetmeleri halinde, daha önce hazırda bulundurdukları sistem, donanım ve altyapı kaynaklarını devreye alıp, bu sistemler üzerinden hizmetlerin devamlılığını sağlarlar.

İşletmeler açısından kademe 1 e göre daha masraflı bir çözümdür ancak hem kurtarma süreçlerini hızlandırır hem de işletme devamlılığını en az zararla sağlanmış olur. Bu kademede kurtarma süreleri genekde 24-48 saat aralığında tamamlanır.

Kademe 3 (Tier 3) :

Bu kademedeki veri merkezine ve IT servislerine sahip işletmeler; Kademe 2 deki tüm özelliklerini bünyesinde barındırır, bunun yanı sıra veri merkezindeki kritik iş süreçlerine hizmet veren IT servisleri ve kritik veriler için, yedek bir veri merkezine sürekli veri aktarma işlemleri yapılır.

Sürekli veri saklama ve belli peryotlarda verinin yansıtılması (replication) gibi işlemler için özel tasarlanmış yazılım ve cihazlar kullanılır. Bu sayede daha hızlı veri yedekleme ve kritik bilgilerin offsite veri merkezine de daha hızlı aktarılması sağlanır. Bu işlemler klasik veri yedekleme aşamalarından daha hızlı ve düzenlidir.

Yine bu kademede felaket kurtarma merkezlerinde daha önce tüm donanım ve yazılım altyapısının hazır ve aktif çalışır halde hazır olması gerekmektedir. Bir felaket anında zarar görmemesi istenen tüm bilgiler bu sistemlerde kullanıma hazırdır.

Kademe 4 (Tier 4) :

Bu kademedeki veri merkezine ve IT servislerine sahip işletmeler; Kademe 3 deki tüm özelliklerini bünyesinde barındırır, bunun yanı sıra ana veri merkezindeki kritik iş süreçlerine hizmet veren IT servisleri ve kritik veriler için, ana veri merkezinin aynı özelliklerinde aktif ikinci bir veri merkezine sahiptirler. Böylelikle her iki veri merkezi arasında sürekli veri yedekleme aktarma işlemleri yapılır.

Bu kademedeki yapılar iki alan arası elektronik veri taşıma yapabilen iki farklı veri merkezine sahiptir ve geri yükleme alanındaki bilgilerin aktif olarak yönetimi gerekliliklerini karşılar. Bu geri yükleme alanındaki bir işlemci tarafından yönetilir ve iki yönlü geri yükleme desteklenir.

Bu işletmelerde düzenli ve sürekli olarak veri ve sistem yedeklemesi yapılır, veriler ana veri merkezi dışında (offsite) bir veri depolama ünitesinde de depolanır. Aynı zamanda sürekli bir bilgi aktarımı ya da ana veri merkezi ve ikinci veri merkezi arasında yüksek veri iletişim bant genişliğinde desteklenen bir bağlantı vardır.

Bu kademedeki veri merkezlerinde ayrıca aktif-aktif sunucu kümeleme (Cluster) mimarisi ile iş yükü iki alan arasında paylaştırılabilir. İki alanda da ulaşılabilir şekilde kritik bilgilerin kopyaları ile bu iki alan arasında sürekli bir bilgi aktarımı vardır.

Yine bu kademde de çok yüksek maliyetler gerekmektedir. Ülkemizde ve dünya genelinde Kademe 4 seviyesinde veri merkezlerine genelde banka ve telekom operatorleri gibi büyük işletmeler sahiptir. Bu kademe de veri kaybı ve hizmet kesinti süreleri yok denecek kadar düşüktür.

4.1.3 İş-etki analizi

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemleri ve IT iş servislerinin felaket anında işletmenin ve iş süreçlerinin devamlılığı üzerindeki olumsuz etkilerinin analizlerinin felaket yaşanmadan önceden yapıldığı "felaket iş-etki analizi" dir.

Bu bölümde iş-etki analizi hakkında yapılan çalışma ve araştırmalar ışığında bilgiler aktarılmıştır.

Dünya genelinde işletmeler iş sürekliliğini sağlayabilmek için giderek IT sektörüne bağımlı hale gelmektedir. Olası bir felaket durumunda direkt olarak IT sistemlerine ve IT altyapısına bağlı olan bu sistemler üst düzey çalışmaları gerektirir. Sonuç olarak denilebilir ki; iş sürekliliği planlaması direkt olarak iş süreçlerini de etkilemektedir.

İş sürekliliği olası bir felaket durumunda firmanın yürürlüğe sokacağı iş ve işlemler dizisini kapsar. İş sürekliliği planlaması kritik servislerin olası bir felaket durumunda hasar görmemesi veya durmaması için gerekli çalışmaları içerir ve bu sürecin mümkün olduğunca en az zararla atlatılmasını hedefler.

Felaket kurtarma planı ise içerisinde planlama, gelistirme ve test etme çalışmalarını barındırır. Olağan dışı bir felaket durumunda temel iş fonksiyonlarının etkili ve yeterli bir şekilde sürdürülmesini sağlar.

Kapsamlı bir felaket kurtarma çalışmasındaki ana işlemler şu şekildedir:

- Kritik uygulamaların belirlenmesi,
- Veri ve sistem yedekleme prosedürleri,
- Veri ve sistem kurtarma prosedürleri,
- Uygulama ve test prosedürleri,
- IT altyapı ve sistem ihtiyaçları için kurulum-destek firmalarının belirlenmesi ve gerekli anlaşmaların yapılması.

Felaket durumuna hazırlanmanın en önemli bölümünü işletmenizin karşılaşabileceği riskleri belirlemek oluşturur. Aşağıdaki tabloda işleyişi engelleyen bazı temel IT sorunları listelenmiştir. Bunların dışındaki diğer risk türleri ise; kasıtlı müdehaleler, altyapı sorunları ve doğal afetler olarak sınıflandırılabilir. Neredeyse dünyadaki her işletme hepsi olmasa da bu sorunların birçoğu ile karşılaşır.

Çizelge 4.2 : Felaket Türleri

Felaket Türleri			
A	**B**	**C**	**D**
Donanım Arızaları	Bilgisayar Virüsleri	Elektrik Kesintileri	Yangınlar
Yazılım Hataları	Bilgisayar Korsanları	Klima Arızaları	Sel Baskınları
Ağ Bağlantı Hataları	İnternet Kesintileri	Güç Kaynağı Arızaları	Depremler
Veri Bozulma ve Silinmeleri	Test ve Güncelleme işlemleri hataları	kablolama Arızaları	Terör Saldırıları

Etkili bir FK planı kaybolan bilgilerinizi en hızlı şekilde kurtarmanızı garantiler. Yedekleme sistemlerinizi peryodik olarak test ettiğinizden, uygun kaynak ve personelle stratejilerinizi yeniden yapılandırdığınızdan emin olmalısınız.

Felaket kurtarma planınız; herhangi bir doğal afette ya da teknik bir felakette tüm sistemlerinizi ve verilerinizi en kısa zamanda eski çalışır haline geri çevirebilecek nitelikte olmalıdır.

Bir felaket kurtarma planı oluşturduğunuzda kötü bir durumla karşı karşıya kaldığınızda başınıza gelebilecek tüm olayları önceden belirlemiş olursunuz.

Bu araştırmada felaket kurtarma planlaması, felaket kurtarma aşamaları, kapsamlı bir felaket kurtrma planı ihtiyacı, tasarlama dizayn etme aşamaları açıklanacak ve son olarak bir plan önerisinde bulunulacaktır.

Aşağıdaki Çizelge 4.3 ’te işletmenin veri merkezinde müşteri ve personellere hizmet veren sunucu sistemlerine ait yapılmış örnek bir iş-etki analizi gösterilmektedir.

Çizelge 4.3 : Örnek Sunucu İş-Etki Analizi

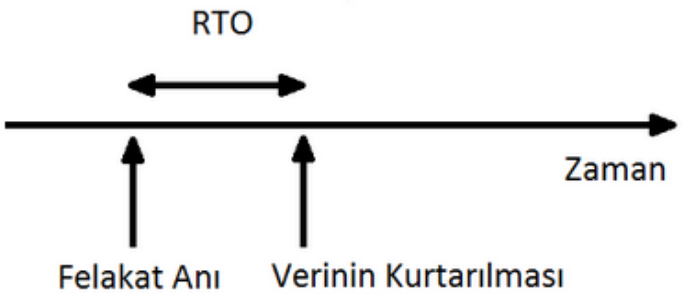
Sistem	Etki Alanı	Kurtarma Seviyesi
Active Directory	Tüm Kullanıcı hesaplarının oluşturulduğu, DNS ve DHCP hizmetlerinin sunulduğu ana sunucudur.	1.Öncelikli
File Server	Tüm Kullanıcılara dosya paylaşımı hizmeti veren sunucudur.	1.Öncelikli
Exchange Server	Tüm Kullanıcılara e-mail hizmeti veren sunucudur.	1.Öncelikli
Terminal Server	Muhasebe gibi önemli birimlerin sisteme erişimi için hizmet veren sunucudur.	1.Öncelikli
SQL Server	Kullanıcılara hizmet veren birçok uygulamanın Database lerinin çalıştığı sunucudur.	1.Öncelikli
AYSIS	Öğrenci, akademisyen ve personellerin kullandığı otomasyon hizmetini veren sunucudur.	1.Öncelikli
ETA	Muhasebe departmanının kullandığı otomasyonun hizmet vermesi için çalışan sunucudur.	1.Öncelikli
CRM	Çağrı Merkezi tarafından müşteri ilişkileri yönetiminde kullanılan yazılımın çalıştığı sunucudur.	1.Öncelikli
LYNC	Kullanıcıların kendi aralarında mesajlaşmalarını sağlayan otomasyonu çalıştıran sunucudur.	1.Öncelikli

4.1.4 Felaket kurtarma süresi (RTO)

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemkeri ve kritik iş servisleri için “felaket kurtarma süresi (RTO)” lerinin belirlenmesidir.

Bu bölümde felaket kurtarma süresi (RTO) hakkında yapılan çalışma ve araştırmalar ışığında bilgiler aktarılmıştır.

Felaket kurtarma süresi (RTO); veri merkezi ve IT servislerinin felaket durumunda ne kadar süre içerisinde kurtarılıp, sunucu ve servislerin tekrar çalışabilir hale getireleceğini ifade eder. Yani bir sistem için kabul edilebilir en fazla kesinti süresi ve tahammül sınırı olarakta ifade edilebilir. Ayrıca Şekil 4.1 'de çizim olarak ta gösterilmektedir.



Şekil 4.1 : Felaket Kurtarma Süresi (RTO)

Felakek kurtarm süreri (RTO); İşletmenin çalışamaz durumda bulunan bir süreci tekrar çalışır duruma getirmek için öngördüğü süredir. Amaçlanan bu sürenin "Kabul Edilebilir En Fazla Çalışılamaz Durumda Bulunma Süresi"nden daha kısa olması gerektiği açıktır (Dinç, 2014).

Felaket kurtarma süresi (RTO) kavramının daha anlaşılır olması için iki farklı örnek ile konuyu daha anlaşılır kılmak mümkün olacaktır.

İlk örnek; bir bankanın veri merkezindeki elektronik para transferi (EFT) hizmeti sunan sunucuda hizmetleri kesintiye uğratacak bir sorun yaşandığını ve sunucunun EFT işlemi için müşterilere hizmet veremez duruma geldiğini varsayalım. Böyle bir durumda felaket kurtarma süreniz ne kadar uzarsa EFT işlemleri gerçekleşmediği için hem çok büyük maddi zarar yaşanırken hem de müşteri memnuniyeti açısından bakıldığında banka prestij kaybı yaşanacaktır.

İkinci örnek; bir işletmenin veri merkezinizde personel, kullanıcı ve müşterileri ile yazılı iletişimini sağlayan elektronik posta sistemi (e-mail) sunucusunda hizmetleri kesintiye uğratacak bir sorun yaşandığını ve sunucunun e-mail işlemi için personel ve müşterilere hizmet veremez duruma geldiğini varsayalım.

Böyle bir durumda felaket kurtarma süreniz ne kadar uzarsa işletme birimleri ve müşetriler arasında iletişim problemi o kadar fazla iletişim problemi yaşanacak, bu sepepten dolayı günlük iş akışı ve iş süreçleri aksayacak, günlük iş süreçlerine ait işlem sürelerini uzayacak, çalışan ve müşteri memnuniyeti açısından olumsuz bir izlenim oluşacak ve işletme imajı açısından güven kaybı yaşanacaktır.

Yukarıdaki her iki farklı örnek te görüldüğü üzere işletmenizin veri merkezi ve IT servisleri için felaket kurtarma planlaması yapılırken felaket kurtarma süresi (RTO) çok önemli bir kriter ve doğru planlama gerektiren önemli bir süreçtir. İşletmenizin veri merkezindeki sunucu sistemleri ve tüm kritik IT servisler için;

- Felaket kurtarma süreleri (RTO) belirlenmeli
- İş sürçleri üzerindeki etki analizleri yapılmalı
- Felaket kurtarma planına eklenmeli
- En etkin ve hızlı kurtarma çözümleri belirlenmeli
- Yetkin kurtarma ekibi oluşturuşmalı
- Sorumlu kurtarma ekibine gerekli eğitimler verilmeli

Yukarı da sıralan tüm adımlar eksiksiz olarak yapıldığı taktirde bir felaket durumunda bu sunucu sistemleri ve IT servisleri en az veri kaybı ve kesinti ile hizmet devamlılığı sağlanmış olacaktır.

Aşağıda Çizelge 4.4 ’te örnek olarak bir üniversitenin veri merkezinde hizmet veren sunucu sistemleri ve IT servisleri için hazırlanmış olan bir felaket kurtarma süresi (RTO) çalışması gösterilmektedir.

Çizelge 4.4 : Felaket Kurtarma Süresi (RTO)

Sunucu Sistemleri ve İlgili Departmanlar	**Kabul Edilebilir Minimum Kurtarma Süresi (Saat)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdehale önceliği)**
Tüm Kullanıcılar **(DC, EXC, FILE SRV)**	45 Dakika	2.000	1.öncelikli
Muhasebe **(ETA)**	1 Saat	20	1.öncelikli
Öğrenci İşleri **(AYSIS)**	1 Saat	33.000	1.öncelikli
Personel Dairesi **(UBIS)**	5 Saat	7	2.öncelikli
İnsan kaynakları **(UBIS)**	6 Saat	5	2.öncelikli
Yazılım geliştirme **(SQL)**	6 Saat	5	2.öncelikli
Çağrı Merkezi **(CRM)**	12 Saat	22	2.öncelikli

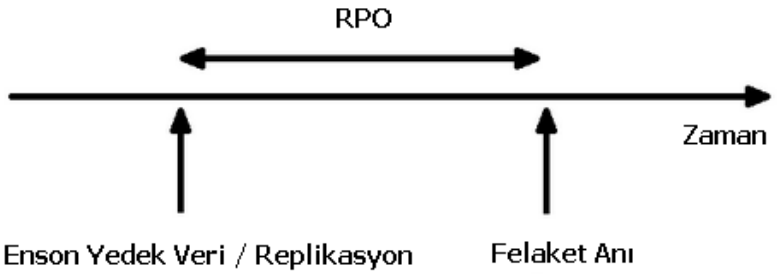
4.1.5 Felaket kurtarma noktası (RPO)

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemkeri ve kritik iş servisleri için “felaket kurtarma noktası (RPO)” nın belirlenmesidir.

Bu bölümde felaket kurtarma noktası (RPO) hakkında yapılan çalışma ve araştırmalar ışığında bilgiler aktarılmıştır.

Felaket kurtarma noktası (RPO); Bir sürecin kesintiye uğradığı zaman noktası ile sürece tekrar işlerlik kazandırıldığı zaman noktası arasında geçen süredeki azami kayıp veri miktarıdır (Akpınar, 2015).

Felaket kurtarma noktası (RPO); veri merkezi ve IT servislerinin hizmet veremez duruma gelmesine sebep verecek beklenmedik bir felaket durumunda zarar gören sistem veya servislerin en son hangi tarihli yedek veya replikasyon sisteme geri dönüleceği olarak ifade edilebilir. Ayrıca Şekil 4.2 'de çizim olarak ta gösterilmektedir.



Şekil 4.2 : Felaket Kurtarma Noktası (RPO)

Felaket kurtarma noktasını (RPO) başka bir ifade ile tanımlayacak olursak, felaket anından zarar gören sunucu sistemleri ve IT servislerinin yeniden çalışabilir duruma getirilebilmeleri için felaket anından önce geri ye doğru ne kadar süre iler veri kaybına tahamülümüz var bunun belirlenmesidir.

Örnek bir senaryo üzerinden ifade edecek olursak, telefon görüşme hizmeti sunan bir operatör işletmede telefon görüşme sürelerini hesaplayan ve buna göre konuşma ücretlerinin belirlendiği bir faturalama sistemi sunucusunun hizmet veremez duruma geldiğini varsayalım.

Böyle bir durumda felaket kurtarma noktası (RPO) planlaması yaparken bu sunucu için veri kaybınızın neredeyse yok denecek kadar az olması gerekmektedir. Aksi durumda 30 dakikalık bir geri kurtarma noktasına sistemi tekrar çalışır hale getirdiğinizde 30 dakika içinde yapılan tüm görüşmler faturalandırılmadığı için ciddi maddi kayıplar yaşanacaktır.

Çizelge 4.5 : Felaket Kurtarma Noktası (RPO)

Sunucu Sistemleri ve İlgili Departmanlar	**Kabul Edilebilir Minimum Geri Yükleme Noktası Süresi (Saat/Gün)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdehale önceliği)**
Tüm Kullanıcılar **(DC, EXC, FILE SRV)**	5 Saat	2.000	1.öncelikli
Muhasebe **(ETA)**	1 Saat	20	1.öncelikli
Öğrenci İşleri **(AYSIS)**	12 Saat	33.000	1.öncelikli
Personel Dairesi **(UBIS)**	12 Saat	7	2.öncelikli
İnsan kaynakları **(UBIS)**	20 Saat	5	2.öncelikli
Yazılım geliştirme **(SQL)**	1 Gün	5	2.öncelikli
Çağrı Merkezi **(CRM)**	2 Gün	22	2.öncelikli

Yukarıdaki tabloda da görüldüğü üzere işletmenizin veri merkezi ve IT servisleri için felaket kurtarma planlaması yapılırken felaket kurtarma noktası (RTO) çok önemli bir kriter ve doğru planlama gerektiren önemli bir süreçtir. İşletmenizin veri merkezindeki sunucu sistemleri ve tüm kritik IT servisler için;

- Felaket kurtarma noktası (RTO) belirlenmeli
- İş sürçleri üzerindeki etki analizleri yapılmalı
- Felaket kurtarma planına eklenmeli
- En etkin ve hızlı kurtarma çözümleri belirlenmeli
- Yetkin kurtarma ekibi oluşturuşmalı
- Sorumlu kurtarma ekibine gerekli eğitimler verilmeli

Yukarı da sıralan tüm adımlar eksiksiz olarak yapıldığı takdirde bir felaket durumunda bu sunucu sistemleri ve IT servisleri en az veri kaybı ve kesinti ile hizmet devamlılığı sağlanmış olacaktır.

4.1.6 Felaket kurtarma yönetim ekibi

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemkeri ve kritik iş servisleri için zarar görebileceği beklenmedik bir felaket durumunda yaşanacak yönetimsel krizi kontrol altına almak ve kurtarma sürelçerini etkin olarak yönetmek için "felaket kurtarma yönetim ekibi" nin belirlenmesidir.

Felaket kurtarma planı hazırlanırken veri merkezi ve IT servislerinde yaşanacak bir felaket anında yönetilmesi on zor süreçlerden biride kurtarma süreçlerinde sorumlulların doğru yönetilmesidir. Bu sebeple kriz anında süreci yönetecek ekip önceden belirlenmeli ve kriz yönetim ekibinin isimleri, iletişim bilgileri ile sorumluluk alanlarının belirtildiği bir tablo hazırlanmalıdır.

Çizelge 4.6 'da gösterildiği gibi bir felaket kurtarma yönetim ekibi tablosu hazırlanmalı ve felaket kurtarma planının içerisine eklenmelidir.

Çizelge 4.6 : Felaket Kurtarna Yönetim Ekibi

Felaket Kurtarma Yönetim Ekibi			
İsim	**Acil Telefonu**	**Cep Telefonu**	**Sorumlu olduğu Sistem ve Yazılımlar**
Yasin A.	0212 xxx	0541 xxx	Kriz Yönetim Ekip Lideri
Hasan A.	0212 xxx	0532 xxx	Kriz Yönetim Ekip Lider Yrd.
Ahmet B.	0212 xxx	0545 xxx	Sunucu Sistemleri, Ekip Sorumlusu
Ali D.	0212 xxx	0533 xxx	Network Sistemi, Ekip Sorumlusu
Fatih E.	0212 xxx	0505 xxx	Veri Yedekleme ve Depolama Sistemleri Sorumlusu
Gökhan H.	0212 xxx	0555 xxx	Sunucu Güvenlik Sistemi, Ekip Sorumlusu
Murat E.	0212 xxx	0542 xxx	Kullanıcı Destek ve Kontrol Sistemi, Ekip Sorumlusu

4.1.7 Felaket Kurtarma operasyon ekibi

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemkeri ve kritik iş servisleri için zarar görebileceği beklenmedik bir felaket durumunda yaşanacak operasyonel krizi kontrol altına almak ve kurtarma operasyonlarını sürelçerini etkin olarak yönetmek için "Felaket kurtarma operasyon ekibi" nin belirlenmesidir.

Felaket kurtarma planı hazırlanırken veri merkezi ve IT servislerinde yaşanacak bir felaket anında yönetilmesi on zor süreçlerden biride kurtarma süreçlerinde kurtarma operasyon sorumluluların doğru yönetilmesidir. Bu sebeple kriz anında süreci operasyon sürecinde görevlendirilecek ekip önceden belirlenmeli ve operasyon ekibinin isimleri, iletişim bilgileri ile sorumluluk alanlarının belirtildiği bir tablo hazırlanmalıdır.

Çizelge 4.7 'de gösterildiği gibi bir operasyon ekibi tablosu hazırlanmalı ve felaket kurtarma planının içerisine eklenmelidir.

Çizelge 4.7 : Operasyon Ekibi

Felaket Kurtarma Operasyon Ekibi				
Kurtarılacak Sistem	**Operasyon Personeli**	**İletişim Numarası**	**Kurtarma Seviyesi**	**Operasyon Sonucu**
Active Directory	Yasin A.	0212 xxx	1.Öncelikli	Tamamlandı
File Server	Hasan A.	0212 xxx	1.Öncelikli	Devam ediyor
Exchange Server	Ahmet B.	0212 xxx	1.Öncelikli	Başarısız
Terminal Server	Ali D.	0212 xxx	1.Öncelikli	.....
SQL Server	Fatih E.	0212 xxx	1.Öncelikli	.....
AYSIS	Gökhan H.	0212 xxx	2.Öncelikli	.....
ETA	Murat E.	0212 xxx	2.Öncelikli	.....
CRM	Yalçın A.	0212 xxx	3.Öncelikli	.....

4.1.8 Sistem kurtarma öncelik listesi

Veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli adımlarından biri de tüm sunucu sistemkeri ve kritik iş servisleri için zarar görebileceği beklenmedik bir felaket durumunda kurtarma operasyonu sırasında hangi sistemlerin hangi öncelik sırası ile kurtarılmaya başlanması gerektiğinin önceden bilinmesi gerekmektedir. Kriz anında böyle bir problemin oluşmaması ve kurtarma operasyonlarının daha etkin ve hızlı sonuçlandırılması için "Sistem kurtarma öncelik listesi" nin belirlenmesi gerekmektedir.

Sistem kurtarma öncelik listesi oluşturulurken, veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli kriterlerinden biri olan felaket iş-etki analizi sonuçlarına göre belirlenmiş felaket kurtarma süresi (RTO) ve felaket kurtarma noktası (RPO) değerlerimne göre hazırlanması gerekmektedir. Çizelge 4.8 'de gösterildiği gibi bir Sistem kurtarma öncelik listesi tablosu hazırlanmalı ve felaket kurtarma planının içerisine eklenmelidir.

Çizelge 4.8 : Sistem Kurtarma Öncelik Listesi

Sistem Kurtarma Öncelik Listesi					
Sunucu Sistemi & IT Servisi	**Sistemin Görevi ve Etki Alanı**	**Kurtarma Seviyesi**	**Felaket Kurtarma Noktası (RPO)**	**Felaket Kurtarma Süresi (RTO)**	**Sistem Operasyon Sorumlusu**
Active Directory	Bilgisayar Kullanıcı hesaplarının oluşturulduğu ve yönetildiği sunucudur.	1.Öncelikli	Felaket anından 6 Saat Öncesi	1 Saat	Yasin A.
File Server	Tüm Kullanıcılara dosya paylaşımı hizmeti veren sunucudur.	3.Öncelikli	Felaket anından 4 Saat Öncesi	2 Saat	Hasan A.
Exchange Server	Tüm Kullanıcılara e-mail hizmeti veren sunucudur.	2.Öncelikli	Felaket anından 3 Saat Öncesi	1 saat	Ahmet B.

4.1.9 Planın devreye alınması

Veri merkezi, sunucu sistemleri ve IT servisleri için beklenmedik bir felaket durumunda bundan önceki bölümlerde aktarmış olduğumuz süreçleri detaylı ve eksiksiz olarak planlayıp hazırlamış olduğunuz felaket kurtarma planı dökümanındaki süreçleri adım adım uygulayarak devreye alma durumunda başarılı olma ihtimaliniz yükselecektir.

İşletmenize özgü bir plan oluşturduğunuz takdirde çok daha az efor harcayıp çok daha az kesinti ve veri kaybı ile felaket sürecini atlatabilirsiniz.

Felaket anında izlenecek adımlar;

- Felaket duyursunun yapılması (Personel, Son Kullanıcı, Müşteri, Çözüm Ortağı, IT tedarik ve destek firmaları)
- Felaket kurtarma planının devreye alınması (Veri merkezi için daha hazırlanmış olan FKP dökümanına uygun süreçlerin başlatılması)
- Felaket durumunda haberleşmenin sağlanması (Felaket Kurtarma Yönetim ve Operasyon Ekipleri ile iletişime geçilmesi)
- Felaket durumunda sistemleri geri yüklenmesi (Felaket kurtarma merkezindeki yedek veri veya sistemlerin devreye alınması)
- Felaket sırasında çalışma ve operasyon süreçleri (Operasyon ekiplerinin RTO ve RPO değerlerine geri sistemleri geri yüklemesi)
- Normale dönüş ve kurtarma adımları (Felaket sonrası ana sistemlere geri dönülmesi Failback ve Rollback)
- Sistem ve operasyon kontrol listelerinin oluşturulması (aktivite checklist) (Felaket kurtarma süresince yapılan tüm işlemlerin sonuçlarının kontrol edilmesi)

Felaket anında kullanılması gereken formlar;

- Kriz yönetim ekibi iletişim formu
- Felaket kurtarma operasyon ekibi iletişim formu
- Zarar tespit ve değerlendirme formu
- Felaket kurtarma olay kayıtları formu
- Felaket kurtarma yönetimi sonuç raporu

Yukarıda sıralanan süreçlerin yanında aşağıda sıralanan eylemlerinde yapılması devreye alınan felaket kurtarma planının başarılı olmasında olumlu etki yaratacaktır.

Olabildiği kadar çabuk davranın; eğer uyarı alıyorsanız, dikkate alın. Monitör sistemleri, ortam izleme ve kritik sistemlerden gelen alarımları dikkate alın ve takiplerini yapın.

Bu size veri merkezi, sunucu sistemleri ve IT servislerini çalışamaz hale getirecek bir felaket çıkmadan önce erken harekete geçme imkânı sunacaktır. IT güvenliği ve sürekliliği; test edilmiş sağlam bir Felakek kurtarma planı ile mümkündür.

Aktif operasyon adımlarınızı belirleyin; felaket kurtarma planınızı için aktif adımları belirleyin ve tüm planlı işlemleri harekete geçirin; bu sizin aldığınız verilere bağlı bir firma kararı olabilir ya da sizin felaket kurtarma planınızı otomatik olarak tetikleyecek bir olay olabilir.

Felaket sonrası normale dönüş planınızı hazırlayın; yaşanan bir felaket ve sonrasında yapılan bir felakat kurtarma, tam bir felaket kurtarma planı oluşturmaz. Felaket kurtarma bittikten sonra sistemleri eski orjinal çalışma ortamlarına geri döndürülmesi (failback) sürçlerininde planlanması gerekmektedir.

Doğrula ve Test et; Felaket kurtarma planlarınızı sık sık test edin. Sisteme zar vermeyecek failover ve failback test yöntemlerini kullanım. Edinilen RTO değerlerini de içeren detaylı bir test sonuç raporu üzerinde çalışın. Bu bilgiler, felaket kurtarma planlarınızın işletme hedeflerine uyup uymadığını kontrol etmenizi sağlar. Bu sonuçlar aynı zamanda personellerinizin eğitilmesini ve olağan durumları size önceden de bildirmiş olur.

4.1.10 Önerilen belge ve tablolar

Bu bölümde IT felaket kurtarma planı dökümanın oluşturulması için hazırlanması gereken döküman konu başlıkları ve eklenmesi gereken tablolar hakkında bilgeler verilecektir.

- Felaket kurtarma planı ve süreçlerine dahil edilecek veri merkerzi, sunucu sistemleri ve IT servislerinin belirlenmesi.
  - ✓ Network altyapı bileşenleri (Envanter Tablosu)
  - ✓ Sunucu altyapı bileşenleri (Envanter Tablosu)
  - ✓ Telefon sistemleri altyapı bileşenleri (Envanter Tablosu)
  - ✓ Veri depolama sistemleri bileşenleri(Envanter Tablosu)
  - ✓ Yedekleme sistemleri bileşenleri (Envanter Tablosu)
  - ✓ Yazılım ve uygulama sistemleri (Envanter Tablosu)
  - ✓ Veri tabanı sistemleri (Envanter Tablosu)
  - ✓ Son kullanıcı bilgisayar sistemleri (Envanter Tablosu)

- Felaket kurtarma yönetim ile operasyon sorumlulularının belirlenmesi ve iletişim bilgileri tablolalarının hazırlanması

Felaket yönetim ekibi (Görev ve iletişim bilgileri Tablosu)

  - ✓ Veri merkezi ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ Sunucu sistemleri ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ Network sistemleri ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ Uygulama sistemleri ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ Operasyon ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ İletişim ekibi (Görev ve iletişim bilgileri Tablosu)
  - ✓ Finans ekibi (Görev ve iletişim bilgileri Tablosu)

- Felaket anında kullanılmak için önceden hazırlnıp felaket kurtarma planı döküman dosyasında olması gereken formlar;
    - ✓ Kriz yönetim ekibi (İletişim Formu)
    - ✓ Felaket kurtarma operasyon ekibi (İletişim Formu)
    - ✓ Zarar tespit ve değerlendirme (Kayıt Formu)
    - ✓ Felaket kurtarma olay kayıtları (Kayıt Formu)
    - ✓ Felaket kurtarma yönetimi sonuç raporu (Sonuç Raporu)

5. SONUÇ VE ÖNERİLER

Sonuç olarak; günümüz gelişen bilgi ve iletişim teknolojileri, işletmelerin artan veri merkezi ve IT servisleri hizmetleri bağımlılığı dikkate alındığında bu sistemler işletmelerin devamlılıklarını sağlamaları için en önemli yapıtaşlarından biri konumuna gelmiş durumdadır.

Sanallaştırma teknolojileri ise bu veri merkezi ve IT servislerini daha etkin yönetmek, veri güvenliğini artırmak ve sürekliliğini sağlamak için geliştirilmiş çok değerli bir teknolojidir.

Felaket kurtarma yönetimi ise günümüzde veri merkezi ve IT servisleri üzerinden müşteri veya personellerine hizmet sunan tüm işletmeler için artık bir seçenek değil zorunluluk haline gelmiştir.

Felaket kurtarma planı ise veri merkezi ve IT servisleri üzerinden sunulan hizmetlerin beklenmedik bir felaket anında kısmen veya tamamen kesilmesi durumunda hem sürecin doğru yönetilmesi hem de hizmetlerin enaz kayıpı ve kesinti süresi ile yeniden çalışabilir hale getirlmesi için olmazsa olmaz bir plandır.

Bu tez çalışmasının sonucunda; günümüzde bilgi teknolojilerini kullanan işletmelerin sahip oldukları veri merkezlerinde müşterilerine ya da personellerine ürün veya hizmet sunmak için kullandıkları sunucu sistemleri mimarisi hakkında bilgiler sunmak, bu sunucu sistemleri için sanallaştırma teknolojilerinin getirdiği yönetimsel kolaylıkları ve yine bu sunucu sistemlerinde iş sürekliliğini kesintiye uğratabilicek beklenmedik ve acil durumlarda ortaya çıkan sorunlara karşı nasıl daha etkin ve hızlı bir felaket kurtarma yönetimi yapılması gerektiği hakkında fikir ve bilgi sahibi olacaksınız.

Bu tez çalışması; “Felaket Kurtarma Planı” hazırlamak isteyen veya bu alanda araştırmalar yapmak isteyen veri merkezi yöneticileri, bilgi işlem sorumlulukları, IT uzmanları, üniversite öğrencileri ve akademisyenler için felaket kurtarma planlanlama sürecinde kaynak olarak kullanılması amaçlanmıştır.

Farklı bir işletmenin kendine özgü oluşturduğu felaket kurtarma planını kopyala-yapıştır yöntemi ile alıp bir felaket kurtarma planı hazırlamak yerine, kendi işletme yapınıza uygun analizleri yapıp en uygun felaket kurtarma süreçlerini tanımlayarak ve felaket kurtarma çözümlerini tercih ederek hazırlayacağınız size özgü bir felaket kurtarma planı, size daha etkin felaket kurtarma yönetimi sağlamanının yanı sıra işletmenize ise çok daha fazla fayda sağlayacaktır.

Kendi işletmenize özgü bir IT felaket kurtarma planı hazılamak, kapsamlı, ettkin ve doğru organize dilmiş bir IT Felaket Kurtarma Planına sahip olmak için için aşağıda sıralan tüm süreçlerin eksiksiz olarak tamamlamanız bu süreçte size oldukça katkı sağyalacaktır.

Veri merkezi ve IT servisleri için etkin kurtarma çözümleri seçilmiş ve doğru organize edilmiş bir felaket kurtarma planın işletmeye sağlayacağı temel avantajlar ise aşağıda sıralanmıştır.

- ✓ Veri Merkezi ve IT servisleri için olası risklerin engellenmesini ve engellenemeyecek felaketlerin de etkilerinin azaltılmasını sağlar.
- ✓ Olası ekonomik kayıpları önler veya azaltır.
- ✓ İşletmenin prestij kaybını önler.
- ✓ Felaketin olma ihtimalini azaltır.
- ✓ İş operasyonlarının ve fonksiyonlarının hzlı ve başarılı kurtarılmasını artırır.
- ✓ Kriz durumunda hayatı önem taşıyan fonksiyonların hasarını en aza indirir.
- ✓ Operasyon hata ve hasarlarını azaltır.
- ✓ İşletmenin devamlılığının stabilitesini arttırır.
- ✓ Kritik ve hassas sistemlerinizi belirlemenizi sağlar.
- ✓ Felaket durumunda karar verme sürelerini azaltarak önceden planlanmış kurtarma işlemleri sunar.
- ✓ Kriz anında karışıklığı engeller ve stres durumunda ortaya çıkabilecek insan kaynaklı hataları azaltır.
- ✓ İşletmenin sahip olduğu varlıkları ve çalışmalarını korur.
- ✓ İşe yeni başlayan çalışanlar için öğrenme ve uygulama materyali sunar.

KAYNAKLAR

Akıllı, Y. (2015). *Bulut Bilişime Giriş ve Microsoft Azure Nerdir ?* Yasin Akıllı kişisel Web Sayfası: http://www.yasinakilli.com/2015/10/09/bolum-1-bulut-bilisime-giris-ve-microsoft-azure-nedir/ adresinden alındı

Akpınar, H. (2015). *Prof. Dr. Haldun Akpınar*. Enformasyon Teknolojisi ve İşletmecilik Öğretimine Etkileri: http://haldunakpinar.com/yayinlar.htm adresinden alındı

Bilişim Derneği, T. (2016). *Kamu-Bib İş Sürekliliği Çalışma Grubu*. Türkiye Bilişim Derneği: http://www.tbd.org.tr/usr_img/cd/kamubib17/AnaMenu.htm adresinden alındı

Buyya, R., & Broberg, J. (2011). *Cloud Computing: Principles and Paradigms.* New Jersey: John Wiley & Sons Inc.

Cevat, Ş. (2010). Sanallaştırma. *Türkiye Bilişim Derneği, Kamu Bilişim Platformu XII Çalışma Grubu*, (s. 40-54). Ankara.

Çözümpark, B. T. (2015). *Storage üniteleri arasında data mirror*. Çözümpark: https://www.cozumpark.com/blogs/default.aspx adresinden alındı

Daş, F. (2012). Sanallaştırılmış Sunucularda Yedekleme Sistemi. *Yüksek Lisans Tezi*. Ankara: Gazi Üniversitesi, Bilişim Enstitüsü.

Dinç, E. (2014). *RTO ve RPO Nedir?* Erdal Dinç Kişisel Web Sayfası: http://www.erdaldinc.com/recovery-point-objectiverpo-ve-recovery-time-objectiverto-nedir/ adresinden alındı

Doğdu, E., & Nihat, Y. (2009). Felaketten Kurtarma ve Depolama. *Türkiye Bilişim Derneği, Kamu Bilişim Platformu XI Final Raporu* (s. 21-36). Ankara: Türkiye Bilişim Derneği.

Itadvisor. (2012). *Tier 3 Veri Merkezi Standartlarını Belirliyor*. itadvisor.com: http://itadvisor.com.tr/tier-3-veri-merkezinde-standartlari-belirliyor/ adresinden alındı

Kulaklı, A., & Aslan, S. (2010). işletmelerde Bilgi Teknolojilerindeki Gelişmelerin işletme ve Yönetim Fonksiyonları Üzerindeki Etkileri. *Beykent Üniversitesi Sosyal Bilimler Dergisi*, 14-20.

Marsh, S. (2016). *Kurumsal Risk Yönetimi*. Marsh: http://turkey.marsh.com/RiskDurumlar%C4%B1/KurumsalRiskY%C3%B6netimi.aspx adresinden alındı

Menken, I. (2010). *Virtualization The Complete Cornerstone Guide to Virtualization Best Practices.* Emereo Pty Ltd.

Microsoft. (2015). *Daikin, Microsoft Azure ile Altyapı Projesi.* Microsoft Customer Story:https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=26240 adresinden alındı

Microsoft Azure. (2015). *Simit Sarayı Microsoft Azure ile Felaket Kurtarma Yönetimi Projesi.* Microsoft Başarı Hikayeleri: https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=1252 adresinden alındı

Taşkın, E., & Sarıoğlu, S. (2012). İş Sürekliliği Yönetimi. *Kamu Bilişim Platformu Çalışma Grubu 3. Ara Rapor*, (s. 25-38). Ankara.

Ulakbim, D. (2016). *İşletmelerde Bilgi Teknolojilerindeki Gelişmelerin İşletme ve Yönetim Fonksiyonları Üzerine Etkileri.* Ulakbim Dergipark: http://dergipark.ulakbim.gov.tr/bujss/article/view/5000107265 adresinden alındı

Wikipedia Encyclopedia, W. (2016). *Wikipedia*. Wikipedia: https://en.wikipedia.org/wiki/X86_virtualization adresinden alındı

EKLER

EK A: Felaket Kurtarma Plan Çizelgeleri

EK A

Bu bölümde felaket kurtarma planı oluştururken hazırlamanız gereken tablolar sunulmaktadır.

Çizelge A.1 : Felaket Kurtarma Planı Kademeleri

FELAKET KURTARMA PLANI KADEMELERİ		
Kademe Seviyesi		**Veri Koruma Metod ve Çeşitliliği**
Kademe 0: (Tier 0)		FKP (Felaket Kurtarma Planı) Yok - Veri Yedekleme Yok
Kademe 1: (Tier 1)		FKP + Off Siste Veri Depolama ve Yedekleme Var
Kademe 2: (Tier 2)		FKP + Off Siste Veri Depo. ve Yedek. + Donanım ve altyapı yedekliliği
Kademe 3: (Tier 3)		FKP + Kademe 2 + Yedekli Veri Merkezi
Kademe 4: (Tier 4)		FKP + Kademe 3 + Aktif 2. Veri Merkezi

Çizelge A.2 : Felaket Türleri

FELAKET TÜRLERİ			
A	**B**	**C**	**D**
Donanım Arızaları	Bilgisayar Virüsleri	Elektrik Kesintileri	Yangınlar
Yazılım Hataları	Bilgisayar Korsanları	Klima Arızaları	Sel Baskınları
Ağ Bağlantı Hataları	İnternet Kesintileri	Güç Kaynağı Arızaları	Depremler
Veri Bozulma ve Silinmeleri	Test ve Güncelleme işlemleri hataları	kablolama Arızaları	Terör Saldırıları

Çizelge A.3 : İş-Etki Analizi

İŞ-ETKİ ANALİZ TABLOSU		
Sistem	**Etki Alanı**	**Kurtarma Seviyesi**
Active Directory	Tüm Kullanıcı hesaplarının oluşturulduğu, DNS ve DHCP hizmetlerinin sunulduğu ana sunucudur.	1.Öncelikli
File Server	Tüm Kullanıcılara dosya paylaşımı hizmeti veren sunucudur.	1.Öncelikli
Exchange Server	Tüm Kullanıcılara e-mail hizmeti veren sunucudur.	1.Öncelikli
Terminal Server	Muhasebe gibi önemli birimlerin sisteme erişimi için hizmet veren sunucudur.	1.Öncelikli
SQL Server	Kullanıcılara hizmet veren birçok uygulamanın Database lerinin çalıştığı sunucudur.	1.Öncelikli
AYSIS	Öğrenci, akademisyen ve personellerin kullandığı otomasyon hizmetini veren sunucudur.	1.Öncelikli
ETA	Muhasebe departmanının kullandığı otomasyonun hizmet vermesi için çalışan sunucudur.	1.Öncelikli
CRM	Çağrı Merkezi tarafından müşteri ilişkileri yönetiminde kullanılan yazılımın çalıştığı sunucudur.	1.Öncelikli
LYNC	Kullanıcıların kendi aralarında mesajlaşmalarını sağlayan otomasyonu çalıştıran sunucudur.	1.Öncelikli
MEYER	Personel Giriş-Çıkış sistemini çalıştıran sunucudur.	2. Öncelikli
ONLINE EĞİTİM	Online eğitim birimi tarafından kullanılan sistemlere ait sunucudur.	2. Öncelikli
UZAKTAN EĞİTİM	Uzaktan eğitim birimi tarafından kullanılan sistemlere ait sunucudur.	2. Öncelikli
CİTRİX	Masa üstü ve uygulama sanallaştırma teknolojisini barındıran sunucudur.	2. Öncelikli

Çizelge A.4 : RTO

FELAKET KURTARMA SÜRESİ (RTO)			
Sunucu Sistemleri ve İlgili Departmanlar	**Kabul Edilebilir Minimum Kurtarma Süresi (Saat)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdehale önceliği)**
Tüm Kullanıcılar **(DC, EXC, FILE SRV)**	45 Dakika	2000	1.öncelikli
Muhasebe **(ETA)**	1 Saat	20	1.öncelikli
Öğrenci İşleri **(AYSIS)**	1 Saat	33.000	1.öncelikli
Personel Dairesi **(UBIS)**	5 Saat	7	2.öncelikli
İnsan kaynakları **(UBIS)**	6 Saat	5	2.öncelikli
Yazılım geliştirme **(SQL)**	6 Saat	5	2.öncelikli
Çağrı Merkezi **(CRM)**	12 Saat	22	2.öncelikli

Çizelge A.5 : RPO

FELAKET KURTARMA NOKTASI (RPO)			
Sunucu Sistemleri ve İlgili Departmanlar	**Kabul Edilebilir Minimum Geri Yükleme Noktası Süresi (Saat/Gün)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdehale önceliği)**
Tüm Kullanıcılar **(DC, EXC, FILE SRV)**	5 Saat	2.000	1.öncelikli
Muhasebe **(ETA)**	1 Saat	20	1.öncelikli
Öğrenci İşleri **(AYSIS)**	12 Saat	33.000	1.öncelikli
Personel Dairesi **(UBIS)**	12 Saat	7	2.öncelikli
İnsan kaynakları **(UBIS)**	20 Saat	5	2.öncelikli
Yazılım geliştirme **(SQL)**	1 Gün	5	2.öncelikli
Çağrı Merkezi **(CRM)**	2 Gün	22	2.öncelikli

Çizelge A.6 : FK Yönetim Ekibi

FELAKET KURTARMA YÖNETİM EKİBİ			
İsim	**Acil Telefonu**	**Cep Telefonu**	**Sorumlu olduğu Sistem ve Yazılımlar**
Yasin A.	0212 xxx	0541 xxx	Kriz Yönetim Ekip Lideri
Hasan A.	0212 xxx	0532 xxx	Kriz Yönetim Ekip Lider Yrd.
Ahmet B.	0212 xxx	0545 xxx	Sunucu Sistemleri, Ekip Sorumlusu
Ali D.	0212 xxx	0533 xxx	Network Sistemi, Ekip Sorumlusu
Fatih E.	0212 xxx	0505 xxx	Veri Yedekleme ve Depolama Sistemleri Sorumlusu
Gökhan H.	0212 xxx	0555 xxx	Sunucu Güvenlik Sistemi, Ekip Sorumlusu
Murat E.	0212 xxx	0542 xxx	Kullanıcı Destek ve Kontrol Sistemi, Ekip Sorumlusu
Yalçın A.	0212 xxx	0541 xxx	Santral Sistemleri, Ekip Sorumlusu

Çizelge A.7 : FK Operasyon Ekibi

FELAKET KURTARMA OPERASYON EKİBİ				
Kurtarılacak Sistem	**Operasyon Personeli**	**İletişim Numarası**	**Kurtarma Seviyesi**	**Operasyon Sonucu**
Active Directory	Yasin A.	0212 xxx	1.Öncelikli	Tamamlandı
File Server	Hasan A.	0212 xxx	1.Öncelikli	Devam ediyor
Exchange Server	Ahmet B.	0212 xxx	1.Öncelikli	Başarısız
Terminal Server	Ali D.	0212 xxx	1.Öncelikli	.....
SQL Server	Fatih E.	0212 xxx	1.Öncelikli	.....
AYSIS	Gökhan H.	0212 xxx	2.Öncelikli	.....
ETA	Murat E.	0212 xxx	2.Öncelikli	.....
CRM	Yalçın A.	0212 xxx	3.Öncelikli	.....

Çizelge A.8 : Sistem Kurtarma Öncelik Listesi

SİSTEM KURTARMA ÖNCELİK LİSTESİ					
Sunucu Sistemi & IT Servisi	**Sistemin Görevi ve Etki Alanı**	**Kurtarma Seviyesi**	**Felaket Kurtarma Noktası (RPO)**	**Felaket Kurtarma Süresi (RTO)**	**Sistem Operasyon Sorumlusu**
Active Directory	Bilgisayar Kullanıcı hesaplarınun oluşturulduğu ve yönetildiği sunucudur.	1.Öncelikli	Felaket anından 6 Saat Öncesi	1 Saat	Yasin A.
File Server	Tüm Kullanıcılara dosya paylaşımı hizmeti veren sunucudur.	3.Öncelikli	Felaket anından 4 Saat Öncesi	2 Saat	Hasan A.
Exchange Server	Tüm Kullanıcılara e-mail hizmeti veren sunucudur.	2.Öncelikli	Felaket anından 3 Saat Öncesi	1 saat	Ahmet B.
SQL Server	Kullanıcılara hizmet veren birçok uygulamanın Database lerinin çalıştığı sunucudur.	1.Öncelikli	Felaket anından 1 Saat Öncesi	30 Dakika	Fatih E.

Çizelge A.9 : FK Sunucu Bilgi Çizelgesi

Felaket Kurtarna Sunucu Bilgi Çizelgesi	
Konum:	Merkez Kampus - D blok - Sistem Odası – A5 Kabini
Sunucu Modeli:	Dell R720
İşletim Sistemi:	Windows Server 2012 R2
İşlemci:	Intel – 20 Çekirdekli
Hafıza:	Kingston – 512 GB
Disk Alanı:	2 TB
Seri No :	ABC123456789
Sunucu ismi :	Exchange Server
DNS IP:	10.1.1.20
IP Adresi:	10.1.1.145
Uygulama:	Microsoft Excahange Server 2013
Veri tabanı:	MS SQL Server 2008 R2
Cluster:	Exchange Server2 – 10.1.1.146
Sistem Sorumlusu, Teknik Destek, ve Çözüm Ortağı İletişim Bilgileri	
Donanım:	DELL Türkiye – Ahmet A. – 0212 000 00 00
Yazılım:	Microsoft Türkiye – Mehmet M. - 0212 000 00 00
Sistem Sorumlusu:	Yasin A. – Sistem Uzmanı – 0541 000 00 00
Veri Tabanı Sorumlusu:	Aykut A. – Veritabanı Uzmanı – 0532 000 00 00
Uygulama Sorumlusu:	Ensar A. – Sistem Uzmanı – 0541 000 00 00
IT Destek Sorumlusu:	Murat A. – IT Destek Uzmanı – 0505 000 00 00
Sistem Veri Yedekleme Bilgileri	
Günlük	Saat 22:00 da disk ortamına / FKM
Haftalık	Pazar 23:00 Disk ortamına / Teyp Ortamına
Aylık	Arşiv Ünitesine
Felaket Kurtarma Prosedürü	
Senaryo 1 – Uygulama ve Veri Kaybı	1- Ana Veri Merkezinde Cluster sistemvarsa devreye al 2- Replikasyon veya Yedek dosyası varsa kullan 3- Her iki seçenek başarısız olursa hızlıca yazılım çözüm ortağından yeni kurulum desteği al.
Senaryo 2 – Donanımsal Sistem Kaybı	1- Ana Veri Merkezinde Cluster sistemvarsa devreye al 2- Uzak veri merkezindeki sisteme al 3- Her iki seçenek başarısız olursa hızlıca donanım çözüm ortağından yeni kurulum desteği al.

Çizelge A.10 : FK Olay Kayıt Çizelgesi

Felaket Kurtarma Olay Kayıt Çizelgesi			
Felaketin Tanımı:			
Felaket Başlangıç Zamanı:			
Felaket Kurtarma Ekibi Müdehale Zamanı:			
Olay Kayıtları			
Yapılan Operasyon ve işlemler	**Tarih / Saat**	**Sonuç**	**Ek Bilgi ve Öneriler**
Operasyon Sonucu:			
Felaket Kurtarma Sonucu:			

Çizelge A.11 : FK İşlem Süreç Takip Çizelgesi

Felaket Kurtarma İşlem Süreç Takip Çizelgesi					
Kurtarma İşlemleri (***Öncelik sırasına göre)***	**Sorumlu Personel**	**Tamamlanma Zamanı (Tarih / Saat)**		**Bulgular**	**Diğer Detaylar**
		Beklenen	**Gerçekleşen**		
1.					
2.					
3.					
4.					
5.					
6.					

ÖZGEÇMİŞ

Ad-Soyad	**:**	Yasin AKILLI
Doğum Yeri Ve Tarihi	**:**	Şanlıurfa, 1985
E-posta	**:**	info@yasinakilli.com

ÖĞRENİM DURUMU

- **Lisans** **:** 2011, Anadolu Üniversitesi, İF, İşletme
- **Yüksek Lisans** **:** 2016, İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği

İŞ DENEYİMİ

- **24 TV & Star Gazetesi** **:** Sistem Uzmanı – (2011 - 2013)
- **İstanbul Aydın Üniversitesi** **:** Veri Depolama ve Yedekleme Sistemleri Uzmanı – (2013 - 2015)
- **Türk Telekom** **:** Sunucu Sanallaştırma Uzmanı – (2016)

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

Akıllı Y., Güneş A., *Disaster Recovery Planning for Data Centers and IT Services*, International Advanced Research Journal In Sciense Enginering and Technology, June 2016, Vol.3, Issue 6