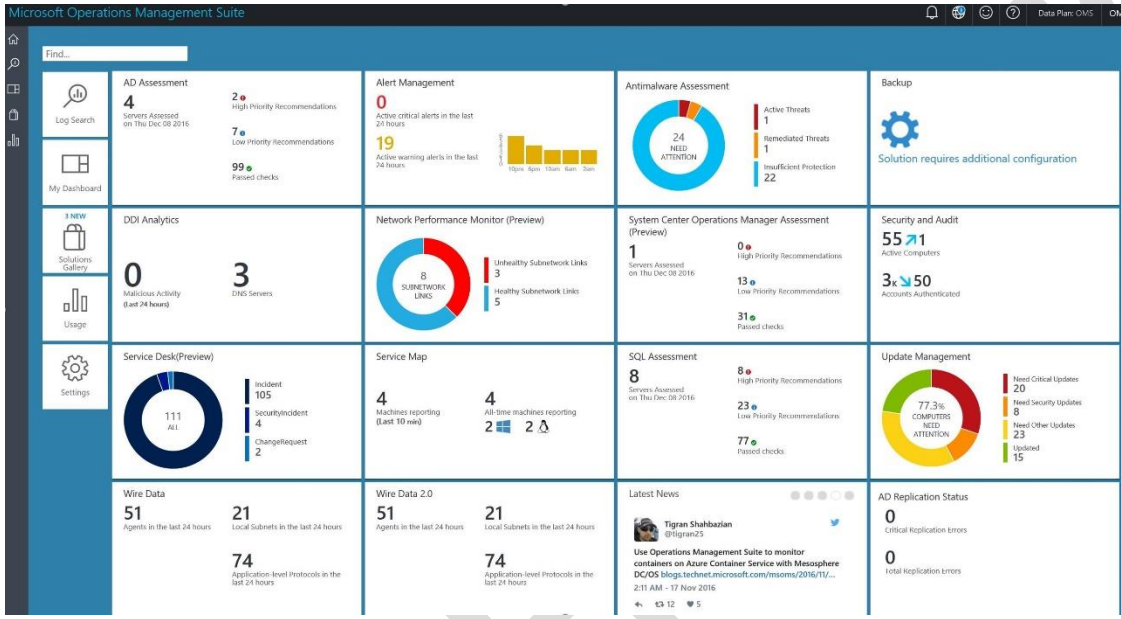


# Tüm Detayları ile Microsoft OMS

2017



Emre ERBULMUŞ (PeakUp)

MSHOWTO Bilişim Topluluğu

16.01.2017

# İÇİNDEKİLER

EMRE ERBULMUŞ Hakkında.....	1
Microsoft Operation Management Suite (OMS) Genel Bakış.....	4
Operation Management Suite'in Mimarisi.....	5
1. Insight and Analytics.....	5
2. Otomasyon ve Denetim.....	6
3. Koruma ve Olağanüstü Durum Kurtarma (Azure Backup & Azure Site Recovery).....	7
4. Güvenlik ve Uyumluluk.....	8
Operation Management Suite'in Log Bileşenleri.....	9
Operation Management Suite'in Ana yapısı.....	10
Operation Management Suite'te Workspace nasıl oluşturulur.....	13
Operation Management Suite Agent kurulumu.....	15
• Azure Platform'da bulunan sunucularınız için.....	15
• On-Prem ortamlarda bulunan sunucularınız için.....	17
Operation Management Suite Solutions Gallery.....	22
1. AD Assessment.....	22
2. Malware Assessment.....	24
3. Alert Management.....	25
4. Security And Audit.....	27
5. Change Tracking.....	28
6. Update Management.....	29
7. SQL Assessment.....	31
8. Agent Health.....	32
Operation Management Suite Kullanıcı Yönetimi.....	35
Operations Management Suite ile Office 365 Kullanımı.....	36
Operations Management Suite ile PowerBI Kullanımı.....	39
SCOM ile OMS Nasıl Entegre Edilir.....	43
Operations Management Suite lisanslama ve Fiyatlandırma.....	49
• Operations Management Suite aboneliği.....	50
• Çözüme göre Operations Management Suite fiyatlandırması.....	51
• Microsoft Operations Management Suite hesaplama.....	52

## **Emre ERBULMUS Hakkında...**

İstanbul'da doğdu. Lisede Sistem Ağ uzmanlığı mezunu ve Yalova üniversitesinde ise Bilgisayar Programcılığı bölümünden mezun oldu. AÖF İşletme Fakültesinde devam etmektedir. İSS, Glabol-BT, BilgeAdam firmalarında Teknik Destek Uzmanlığı, IT Danışmanı, Sistem yöneticiliği pozisyonlarında görev aldı. Bu sektöre gönül vermiş biri olarak en iyi yerlerde olmayı hedefliyor. Şuan ise Microsoft'un Bulut Partner'i PeakUp Information Technologies firmasından 'Cloud Technologies Consultant' olarak çalışmaktadır.

### **İlgilendiklerim ve üzerinde çalıştıklarım**

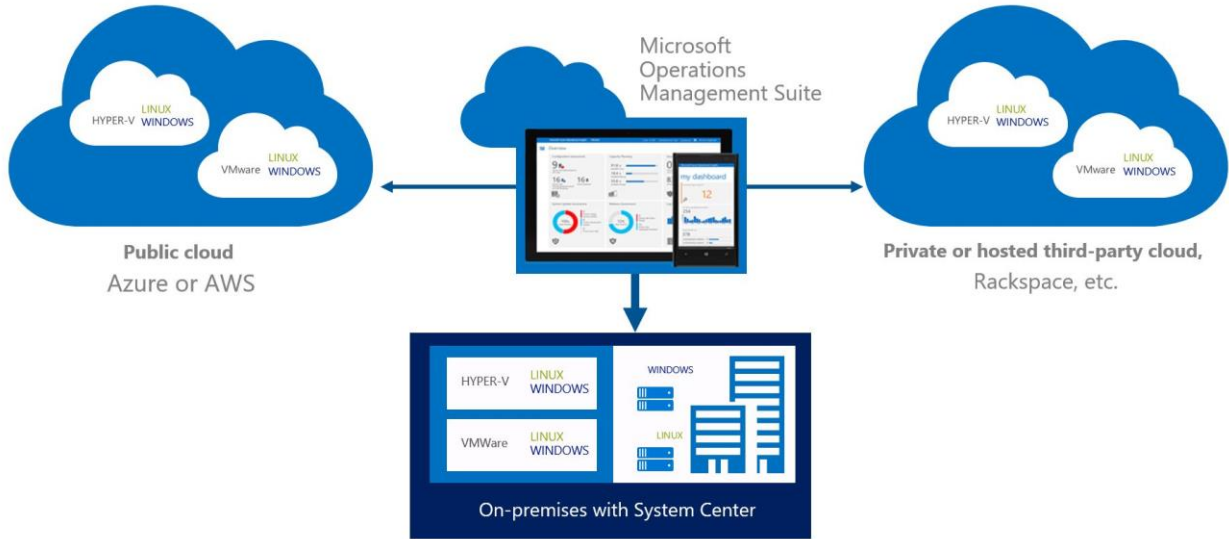
- MS Windows Server Ailesi (2008r2, 2012-2012r2)
- Microsoft Client Windows (7, 8, 10)
- **HyperV Sanallaştırma Platformlarının yönetimi**
- **Active Directory ve Domain kurulumu, konfigürasyonu ve yönetimi**
- **DHCP, DNS, NPS, Remote Access kurulum ve konfigürasyonu**
- **Firewall kurulum ve konfigürasyonu (Coslat, Sophos, Watchguard)**
- **Disk, Dosya ve Erişim Yönetimi (DFS, FSRM)**
- **Group Policy Dizaynı**
- **Backup Alma Metodları (Cobian Backup, Windows Backup)**
- **Veeam Backup Kurulum ve Yönetimi**
- **WSUS ve WDS yapılandırması**
- **MS Office uygulamaları**
- **PC donanım, bakım hizmetleri**
- **Bulut Bilişim Mimarisi OMS, OFFİCE 365 ve Azure**
- 

### **Sahip olduğum Sertifikalar**

- MS: Designing and Providing Microsoft Volume Licensing Solutions to Large Organizations
- MCPS: Microsoft Certified Professional
- MCTS: Designing, Assessing, and Optimizing Software Asset Management (SAM)
- MCSE: Private Cloud
- MCSA: Windows Server 2012
- MCSE: Cloud Platform and Infrastructure
- VMTSP: Veeam Technical Sales Professional
- WMSP: Veeam Sales Professional
- **Sistem Ağ ve Güvenlik Uzmanlığı Eğitimi (MSCE) - Bilge Adam Katılım Sertifikası**

## Microsoft Operation Management Suite (OMS) Genel Bakış

Operation Management Suite, Microsoft'un hibrit bulut için sunduğu BT yönetim çözümdür. Tek başına kullanılabilceği gibi, mevcut System Center altyapınıza da entegre olabilen OMS, altyapınızın bulut tabanlı yönetimi için size maksimum esneklik ve kolaylık sağlar. Bulut dünyası için tasarlanan OMS, rekabetçi ve hızlı firmaların ihtiyaçlarını karşılayabilmek için, hibrit bulut altyapınızı bir bütün olarak yönetilebilir. Farklı yönetim çözümleri ve ara yüzleri ile entegre etmek için hiç vakit harcamadan, yönetim süreçlerinin en kısa sürede çalışır duruma gelmesini sağlayabilirsiniz.



Operation Management Suite ile Azure, AWS, Linux, Hyper-V, VMware ve OpenStack dâhil her türlü fiziksel veya bulut ortamınızı istediğiniz bir şekilde yönetebilirsiniz. OMS, Aynı zamanda Planlama ve yönetimde verimliliği en üst düzeye çıkarmak ve sorunları kolayca tespit edebilmenize olanak sağlar. OMS kısaca On-prem veya bulut sistemli yapılarınızdan veri toplayan ve bunların analizini uçtan uca yapan bir servistir. Ayrıca alınan hata veya uyarılara karşı alınması gereken önlemleri sizlere sunar.

## Operation Management Suite'in Mimarisi

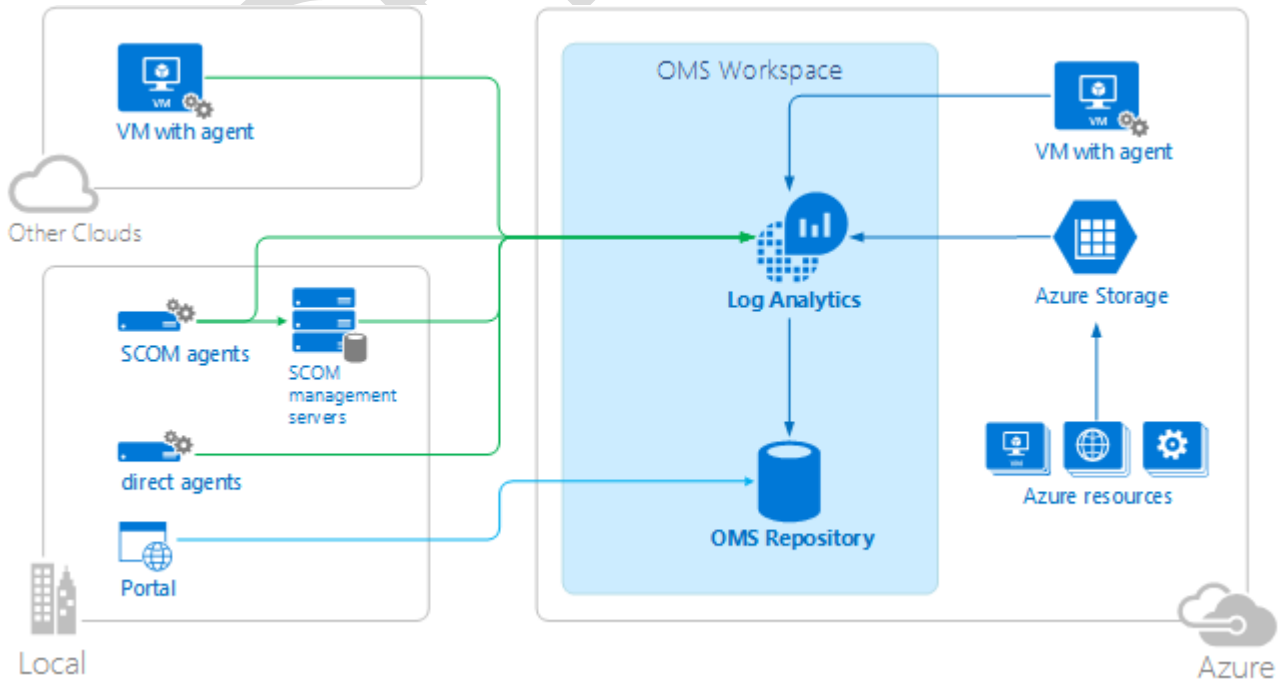
Oms'in mimarisini aslında 4 ana bileşende toplayabiliriz, Bunlar;

- Insight and Analytics
- Automation & Control (Otomasyon ve Denetim)
- Protection and Disaster Recovery ( **Koruma ve Olağanüstü Durum Kurtarma** )
- Security and Compliance (**Güvenlik ve Uyumluluk** )



### 1. Insight and Analytics

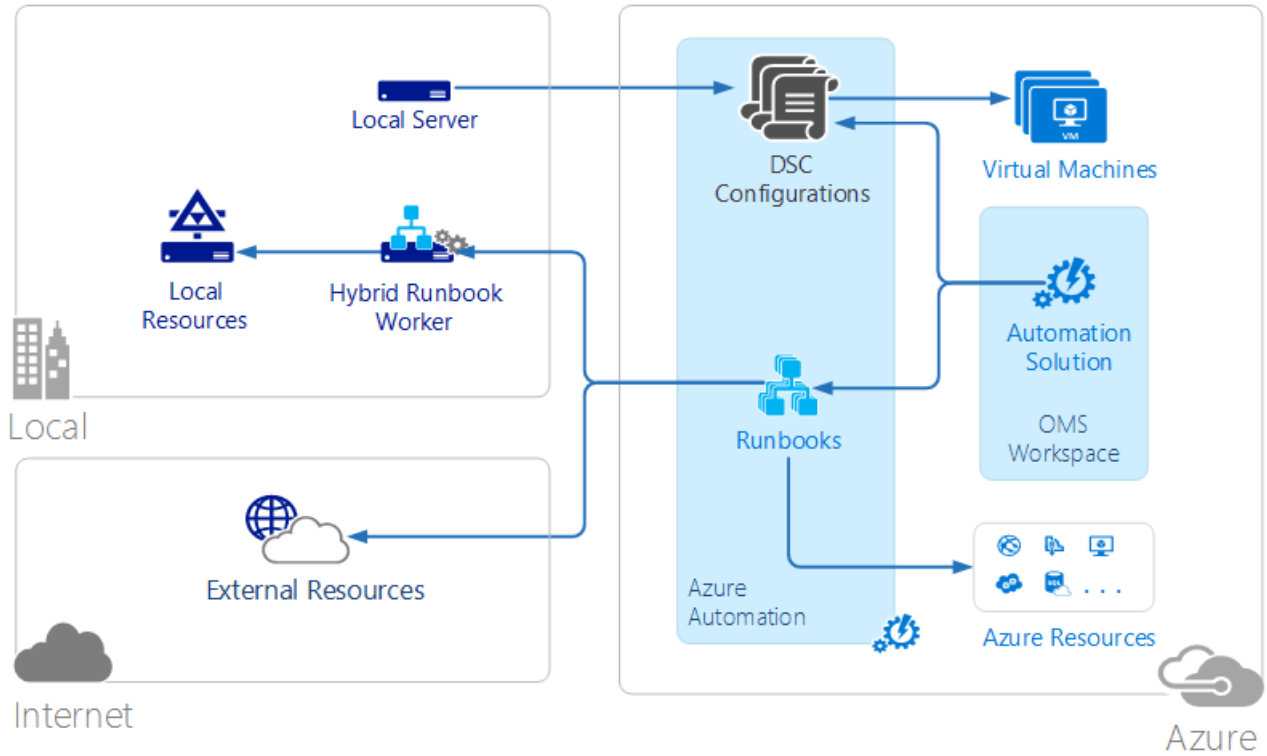
Log Analytics, tarafından toplanan tüm veriler, Azure'da barındırılan (repository) OMS deposunda depolanır. İşletim sistemleri ve uygulamalar tarafından oluşturulan günlük ve performans verilerini toplamanıza, bunlar arasında bağlantı kurmanıza ve bu veriler üzerinde arama işlemi yapmanıza yardımcı olur. Toplanacak verileri OMS'in çözümleriyle birleştirebilir ve bu veriler üzerinden mantıksal raporlar alabilirsiniz . Ayrıca çözümler en az yapılandırmayla veya hiç yapılandırma istemeden otomatik olarak sunulan hizmetlerle işlemler sağlanır.





## 2. Otomasyon ve Denetim

Azure Otomasyonu, **Kullanıcıların bulut veya local ortamda sıklıkla gerçekleştirdikleri iş yüklerini, hatasız ve sık tekrarlanan görevlerini otomatik hale getirmek için kullanılan bir yöntemdir.** Bu yöntem zamandan tasarruf sağlar ve normal yönetim görevlerinin güvenilirliğini de artırır, hatta bu kuralları düzenli aralıklarla otomatik olarak gerçekleştirilecek şekilde ayarlanabilir. Runbook'ları kullanarak işlemleri otomatik hale getirebilir ya da istenen yapılandırmayı kullanarak varolan yapılandırmayı otomatik hale getirebilirsiniz. Runbook, **Azure Automation'da otomatik işlemleri gerçekleştiren görevler grubu olarak adlandırılabilir.** Bu bir sanal makineyi başlatma ve günlük girişi oluşturma gibi basit bir işlemler de diyebiliriz.

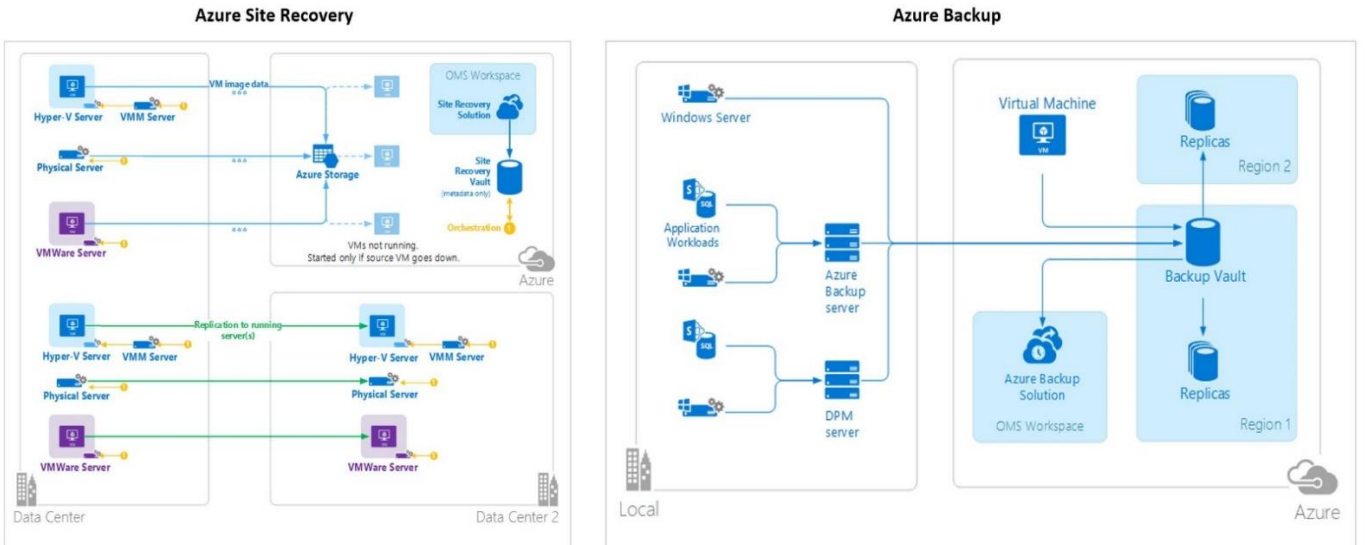




### 3. **Koruma ve Olağanüstü Durum Kurtarma** (Azure Backup & Azure Site Recovery)

Azure Backup, varolan uygulama verilerinizi korur ve herhangi bir yatırım sağlamadan önemli verilerinizi uzun süre boyunca saklar. SQL Server ve SharePoint gibi uygulama iş yüklerinizin yanı sıra fiziksel ve sanal Windows sunucularındaki verilerinizi de yedekler. Uzun vadeli depolama açısından verilerinizi farklı bölgelerde saklama seçenekleri sunmaktadır.

Azure Site Recovery; şirket içi Hyper-V sanal makineleri, VMware sanal makineleri, fiziksel Windows/Linux sunucularını felaketten kurtarma işlemlerini düzenleyerek iş sürekliliği ve olağanüstü durumlarda kurtarma stratejinize katkı sağlar. Bu makineleri cloud ortamına yada ikinci bir veri merkezine taşıyarak veri merkezini genişletebilirsiniz. Site Recovery, aynı zamanda iş yükleri için basit bir yük dengeleme ve kurtarma işlemi sunar.



## Azure Site Recovery için üç temel senaryo bulunmaktadır;

- Hyper-V sanal makinelerini

Hyper-V sanal makineleri VMM tarafından yönetiliyorsa, ikincil veri merkezine veya Azure depolama hizmetine yönelik taşıma gerçekleştirebilirsiniz. Azure'a yönelik taşıma, güvenli bir İnternet bağlantısı üzerinden yapılır. Hyper-V sanal makineleri VMM tarafından yönetilmiyorsa yalnızca Azure depolama hizmetine yönelik olarak çoğaltma işlemini gerçekleştirebilirsiniz.

- VMWare sanal makinelerini

VMware sanal makinelerini VMware veya Azure depolama hizmetini çalıştıran ikincil bir veri merkezine yönelik olarak taşınabilir. Azure'a yönelik taşıma, siteler arası bir VPN veya Azure ExpressRoute üzerinden ya da güvenli bir İnternet bağlantısı yoluyla gerçekleştirilebilir. İkincil bir veri merkezine yönelik taşıma, InMage Scout veri kanalı üzerinden gerçekleştirilir.

- **Fiziksel Windows ve Linux sunucularını**

Fiziksel sunucuları ikincil bir veri merkezine veya Azure depolama hizmetine yönelik olarak taşıyabilirsiniz. Azure'a yönelik taşıma, siteler arası bir VPN veya Azure ExpressRoute üzerinden ya da güvenli bir İnternet bağlantısı yoluyla gerçekleştirilebilirsiniz. Azure Site Recovery, bazı veri istatistiklerini görüntüleyen bir OMS çözümüne sahiptir, ancak işlemler için Azure portalını kullanmanız gerekecektir.



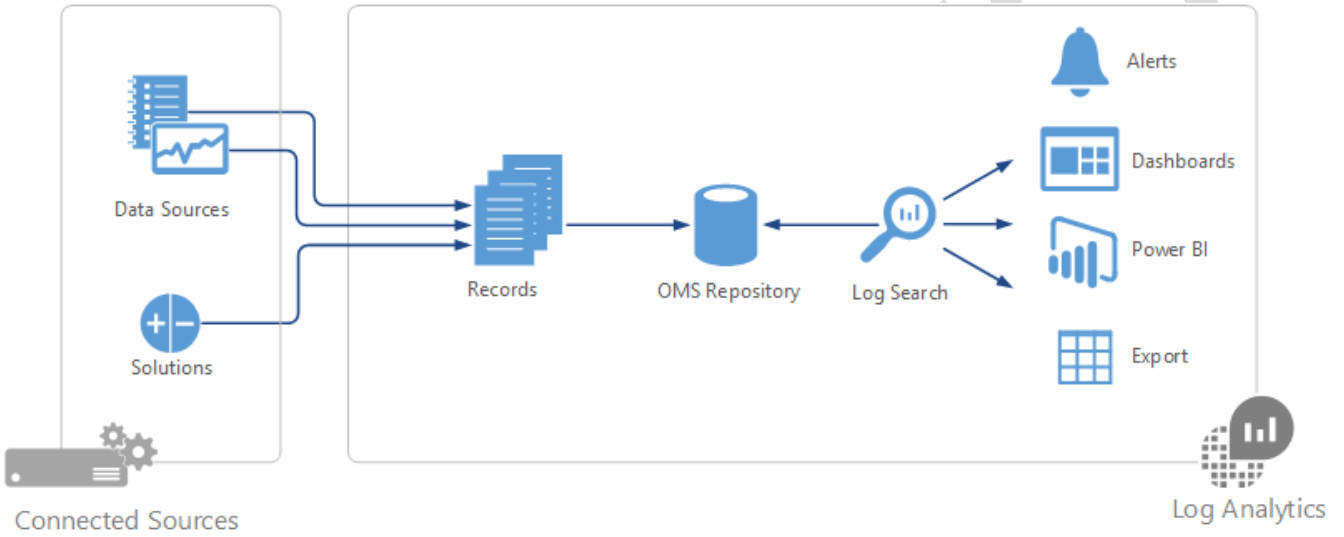
#### 4. **Güvenlik ve Uyumluluk**

Güvenlik ve Uyumluluk, altyapınıza ilişkin güvenlik risklerini belirlemenize, değerlendirmenize ve azaltmanıza yardımcı olur. Yönetilen sistemlerdeki güvenlik olaylarını toplayarak çözümler sağlamaktadır. Aynı zamanda kötü amaçlı yazılımların durumunu ve sunucu güncelleştirmelerin en stabil halini raporlayabilir ve gözlemleyebilirsiniz.



## Operation Management Suite'in Log Bileşenleri

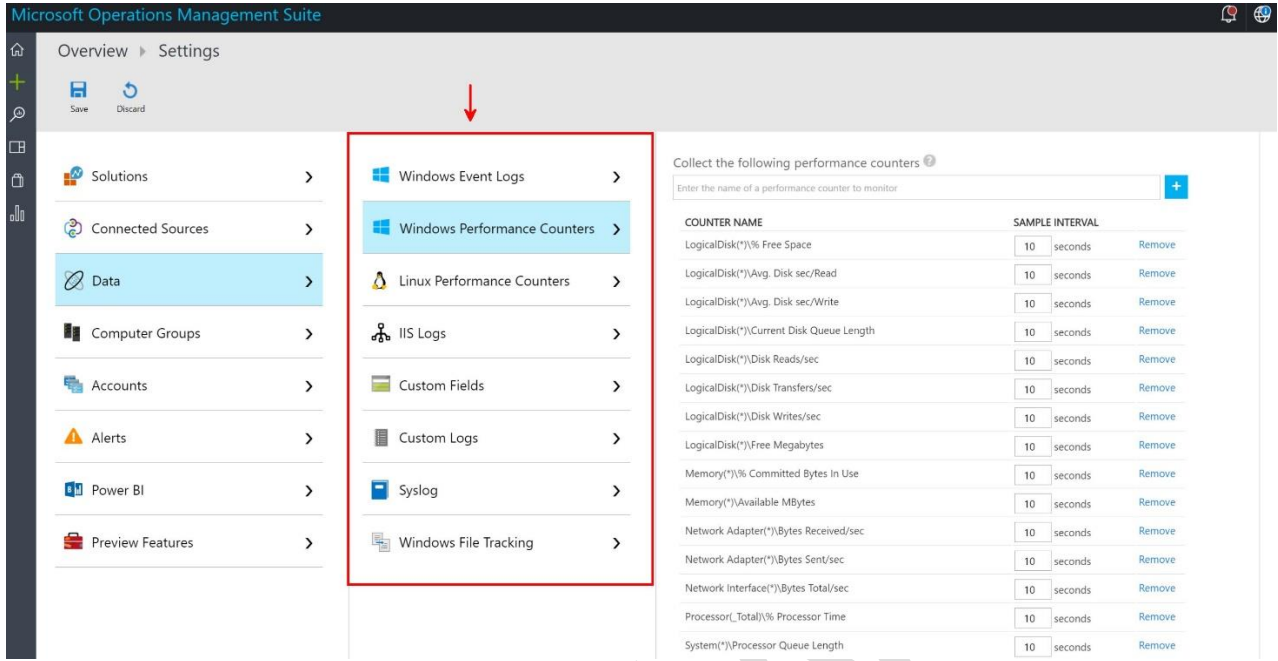
OMS'in arka tarafta nasıl log topladığını inceliyor olursak, resimde görüldüğü üzere Azure içerisinde barındırılan bir OMS repository bulunur. Bu Repository merkezi olarak belirlenir, Veri kaynakları ile yapılandırılarak ve hesabınıza yeni çözümler eklenerek varolan çözüm kaynaklarından repository bölümüne aktarılır. Aktarma işlemi de OMS'in Agent'i ile yapılır.



Log Search tarafında ise OMS repository üzerine toplamış olan Log'ları OMS dashboard'unda görülür. Aynı zamanda bu Log'ları bir PowerBI ortamına yada bir Excel'e export edilebilir. Bunları dışında belirlediğimiz Log'ları bir uyarı (Alerts) ile görebiliriz.

### OMS Repository Database'in içinde nasıl Log'lar bulunur.

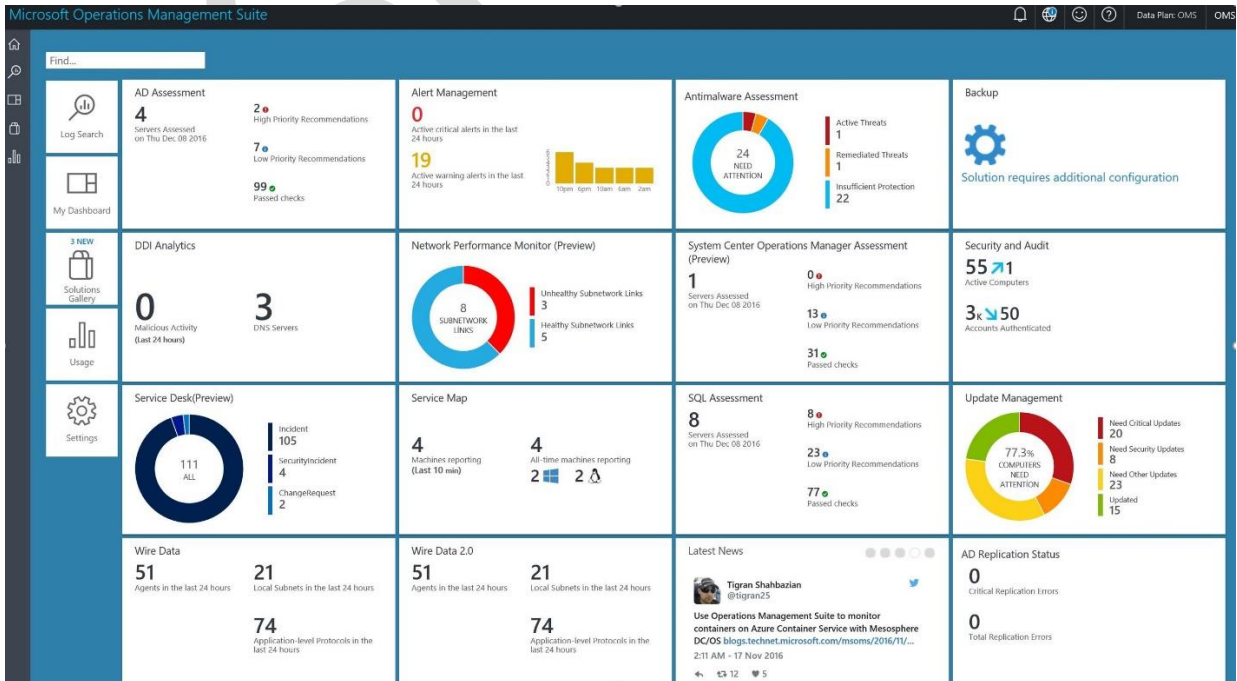
- Custom Logs
- Windows Event logs
- Windows Performance counters
- Linux Performance counter
- IIS logs
- Syslog



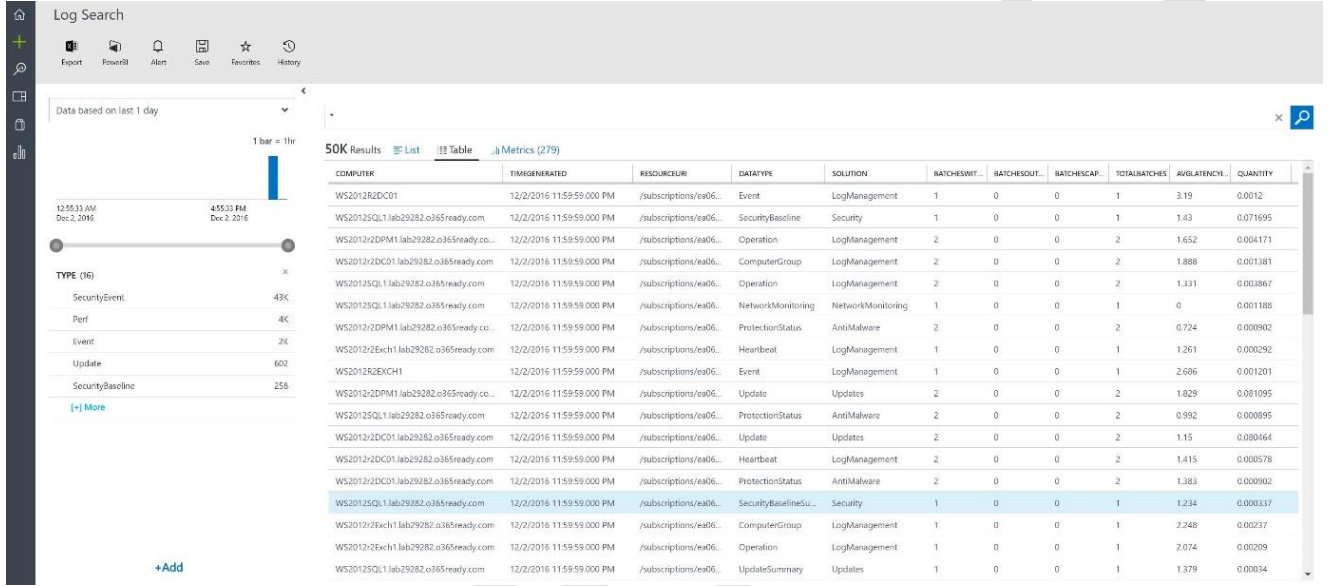
OMS Portalı üzerinden Settings – Data yollarını takip ederek ilgili log'ları inceleyebilirsiniz.

## Operation Management Suite'in Ana yapısı

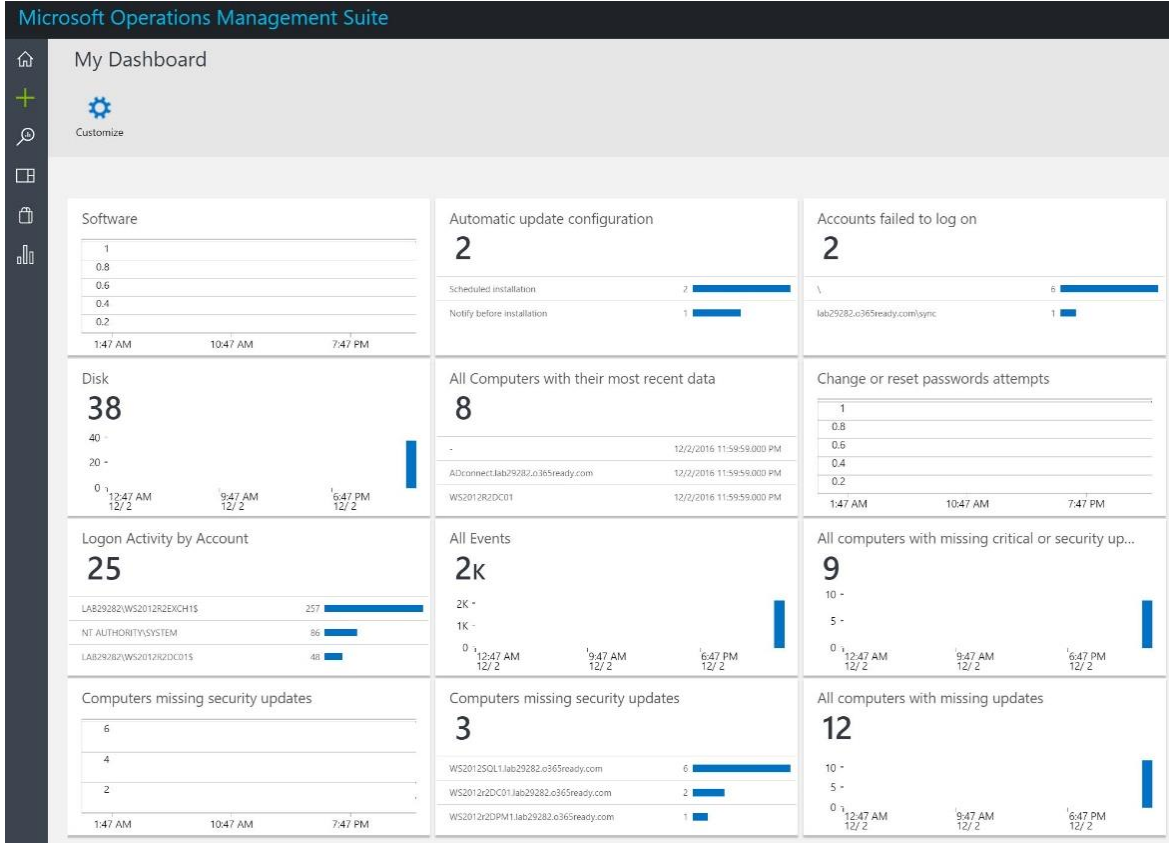
OMS'in Ana yapısını genel olarak Log Search, My Dashboard, Solutions Gallery, Usage ve Settings bölümünden oluşmaktadır. Ana bölümde ise eklenen Solutions'ları görebilirsiniz. Her birinin farklı bir görevi olduğundan ana başlıklarına göre çeşitli bilgiler bulunmaktadır. Tek tek üzerine tıklandığından sizlere o konuyla ilgili çözüm ve öneriler sunarak ortamınıza katkı sağlar.



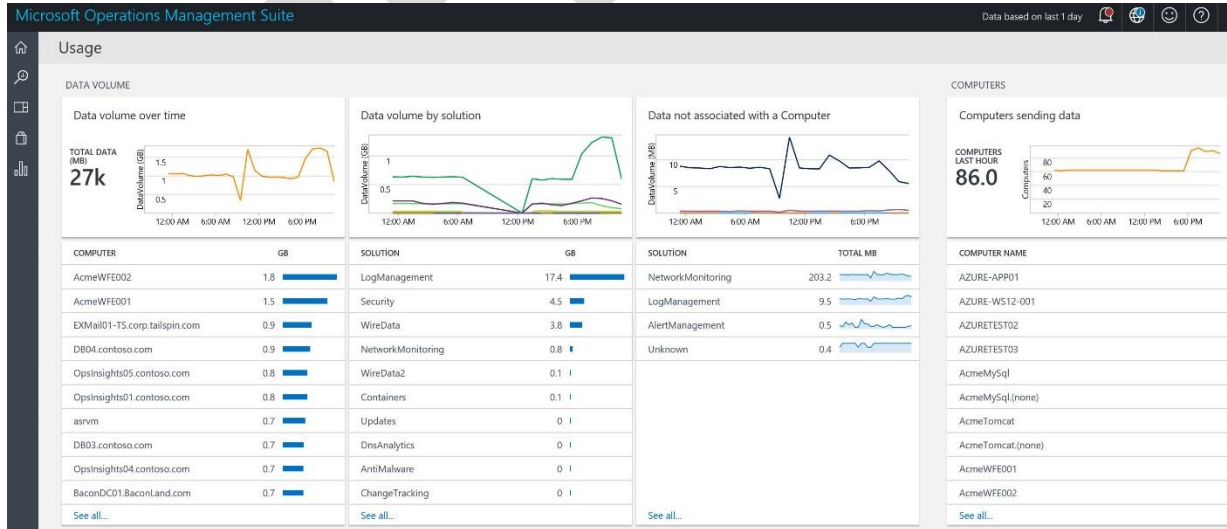
Veri kaynakları, bağlı olduğu her sunuculardan toplanan farklı veri türleridir. Bunlar, Windows ve Linux sunucularından alınan logları (performans verileri, IIS logları ve özel loglar) içerir. Toplamak istediğiniz her veri kaynağını yapılandırabilirsiniz. Yapılandırma, otomatik olarak isteğe bağlı her kaynağa dağıtılır.



Log Analytics dışındaki verileri analiz etmek için OMS deposundaki verileri Power BI veya Excel gibi araçlara aktarabilirsiniz. Log Analytics verilerini kullanan özel çözümler oluşturmak veya başka sistemlerle tümleştirmek için Günlük Arama API'sini de kullanabilirsiniz. Depoladığınız verileri hızlı bir şekilde toplayıp veya birleştirmek için sorgu dizinleri kullanılır. Verileri doğrudan OMS portalında çözümlenmek veya sorgunun sonuçları önemli bir koşulu gösterdiğinde günlük aramalarının otomatik olarak çalışmasını sağlamak için Günlük Aramaları oluşturabilir ve kaydedebilirsiniz.



My Dashboard, genel ortamınızın durumunu kısa bir grafikte göstermek için panonuza kayıtlı günlük aramaları görselleştirmelerle ekleyebilirsiniz. Bu kayıtları istediğiniz gibi şekillendirebilir ve düzenlenebilirsiniz.

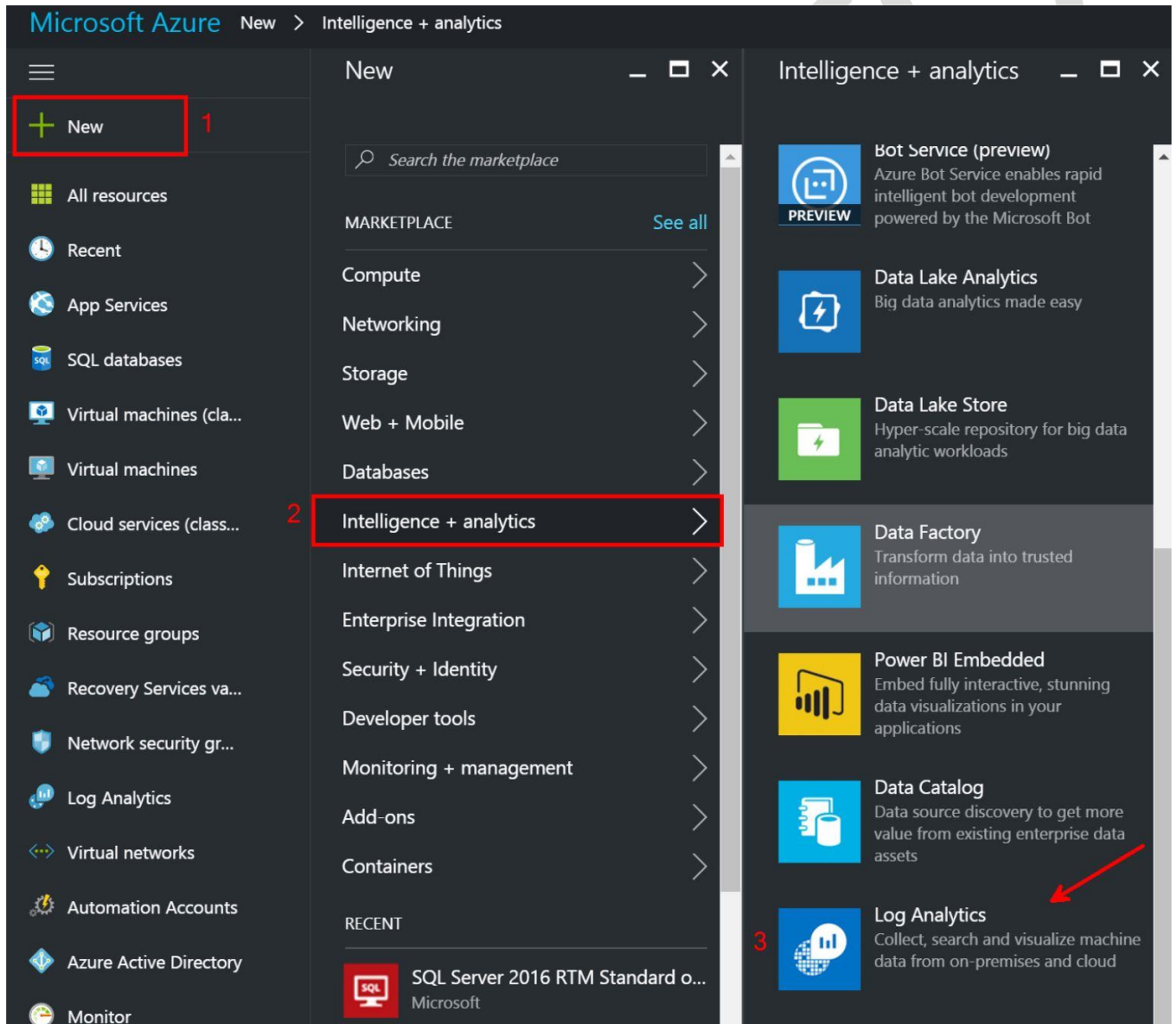


OMS ortamınızda ne kadar veri kullanımı yapıldığını Usage kısmına girerek inceleyebilirsiniz. Bu bölümde ise hangi sunucu ne kadar log toplamış ve solution'ların hangisi daha fazla log üretiyor gibi kullanım miktarlarını görebilirsiniz.

## Operation Management Suite'te Workspace nasıl oluşturulur

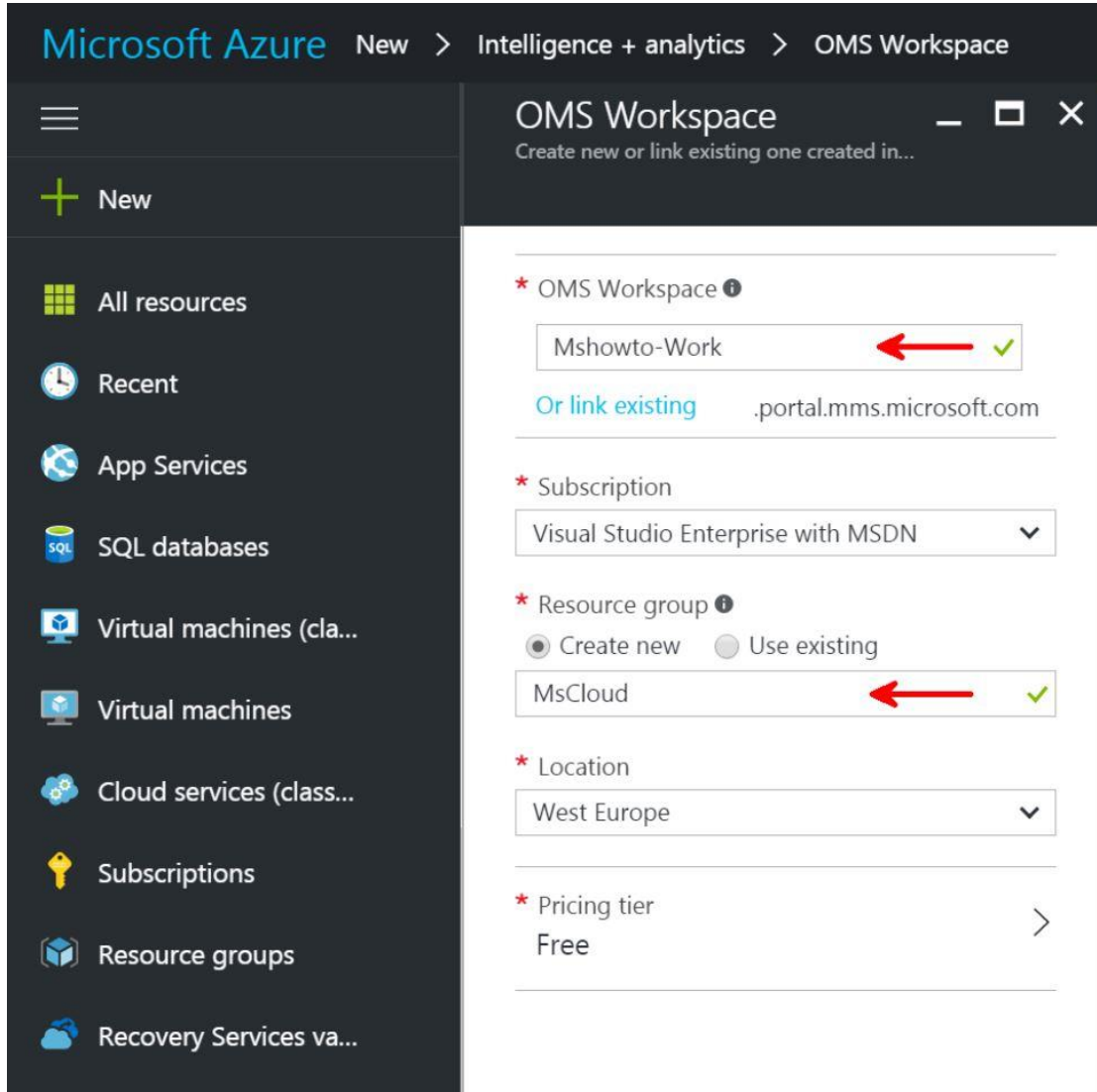
OMS, temel olarak Workspace yani çalışma alanı olarak kabul edilen bir kavram üzerinde hizmet sunar. Her Workspace altında farklı çözümler ve farklı sunucular üzerinde toplanan log'lar yer alır. Toplanan her log'ları OMS dashboard'ına yansıtılıp istenilen şekilde gözlemlenebilir.

### Workspace nasıl oluşturulur :

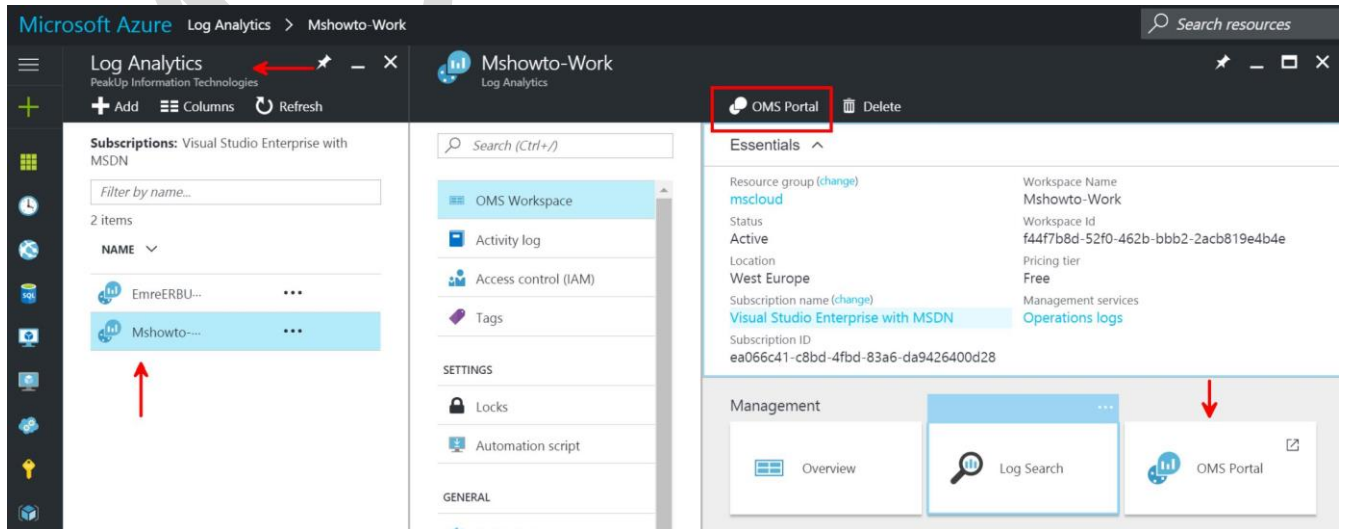


The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with a 'New' button highlighted in red and labeled '1'. The main area shows the 'New' marketplace with a search bar and a list of categories. The 'Intelligence + analytics' category is highlighted in red and labeled '2'. The right sidebar shows a list of services under 'Intelligence + analytics', with 'Log Analytics' highlighted in red and labeled '3', and a red arrow pointing to it.

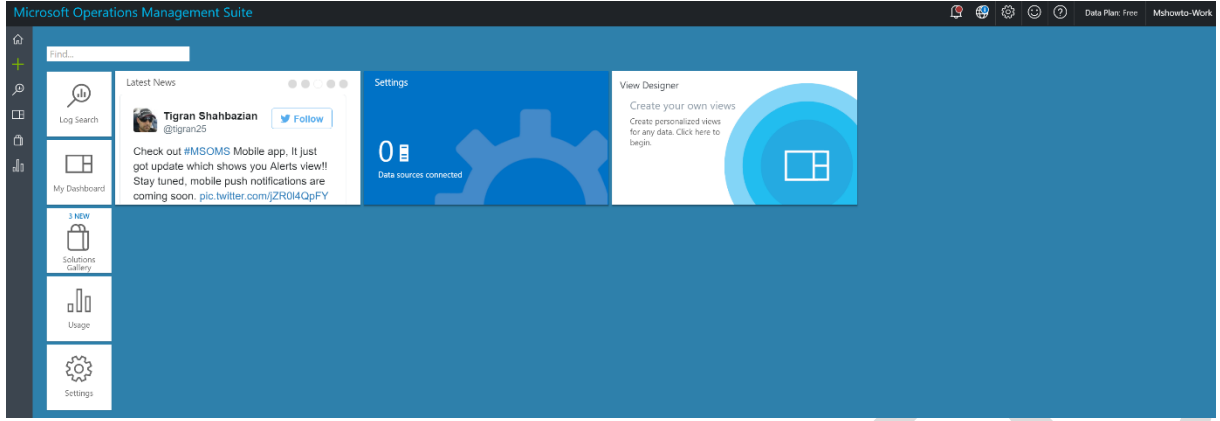
Azure portalına başarılı girişin ardından New – Intelligence + Analytics – Log Analytics tıklanır.



Sonrasında ise OMS Workspace'in ismi, Resource Group'u ve location'ı belirterek çalışma alanı oluşturulur.



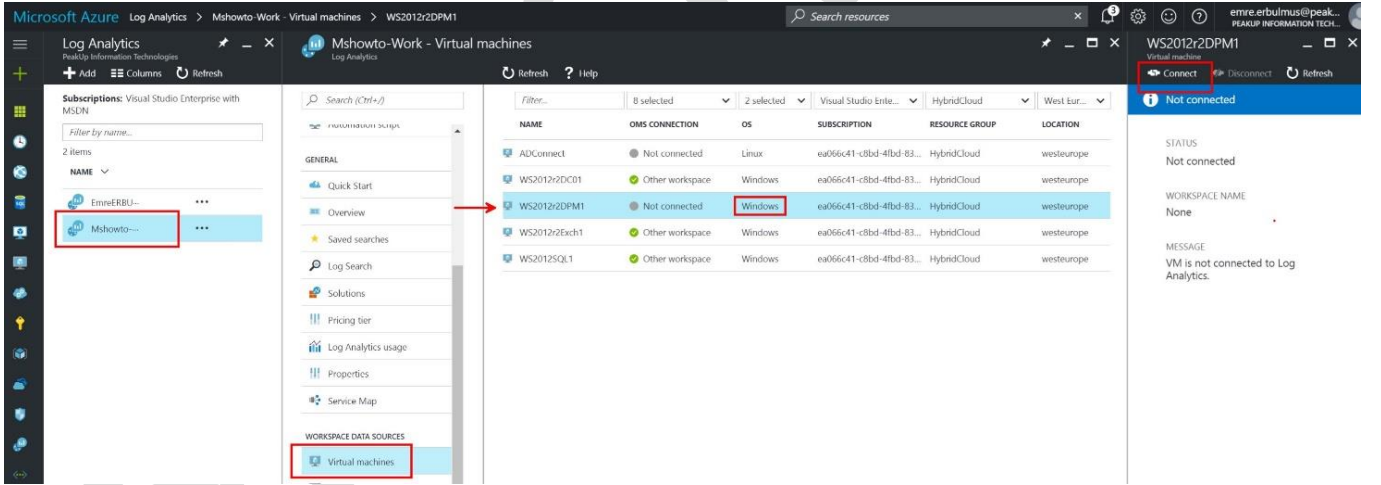
Ekran görüntüsünde gösterildiği şekilde OMS Portal'ına giriş yapılır.



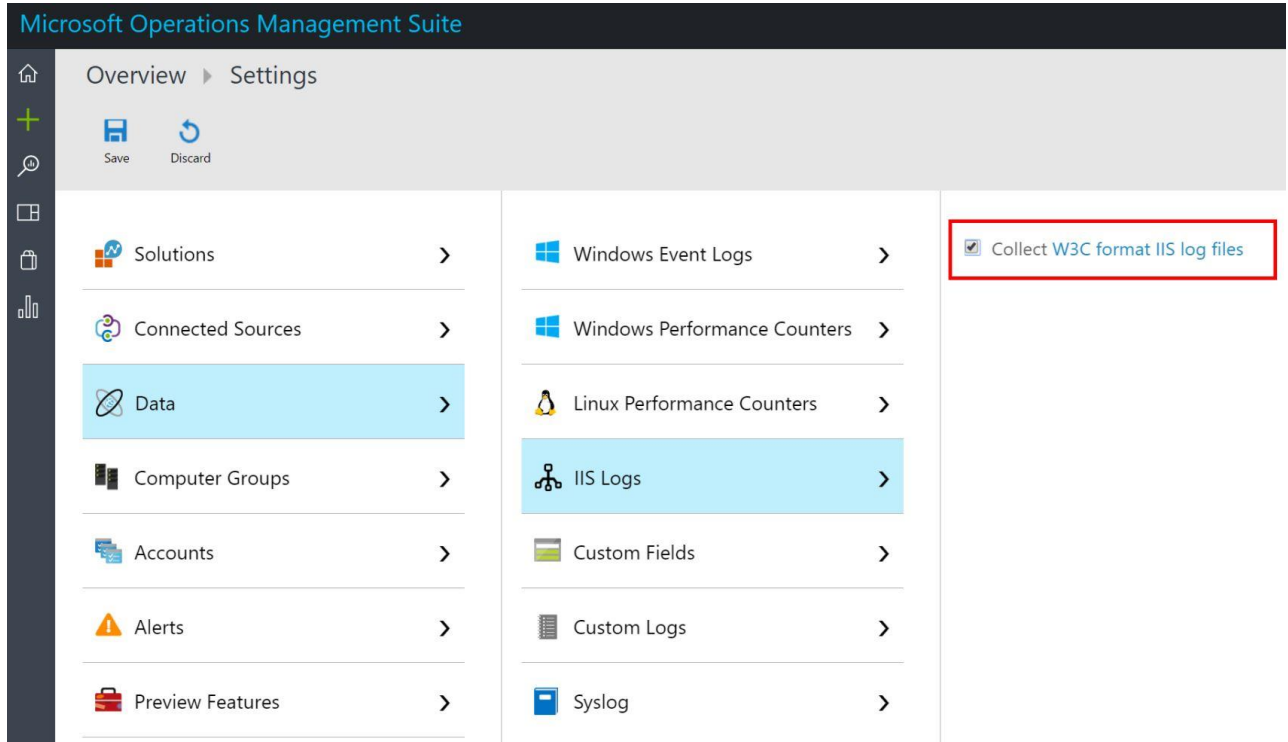
OMS portalına ilk giriş yapıldığında boş bir dashboard ve standart olarak eklenen ayarlar ve OMS ile paylaşılan Twitter butonu gelmektedir.

Operation Management Suite Agent kurulumu

- **Azure Platform'da bulunan sunucularınız için,** Azure portalında Oluşturulan Workspace (çalışma alanı) alanına girilir.

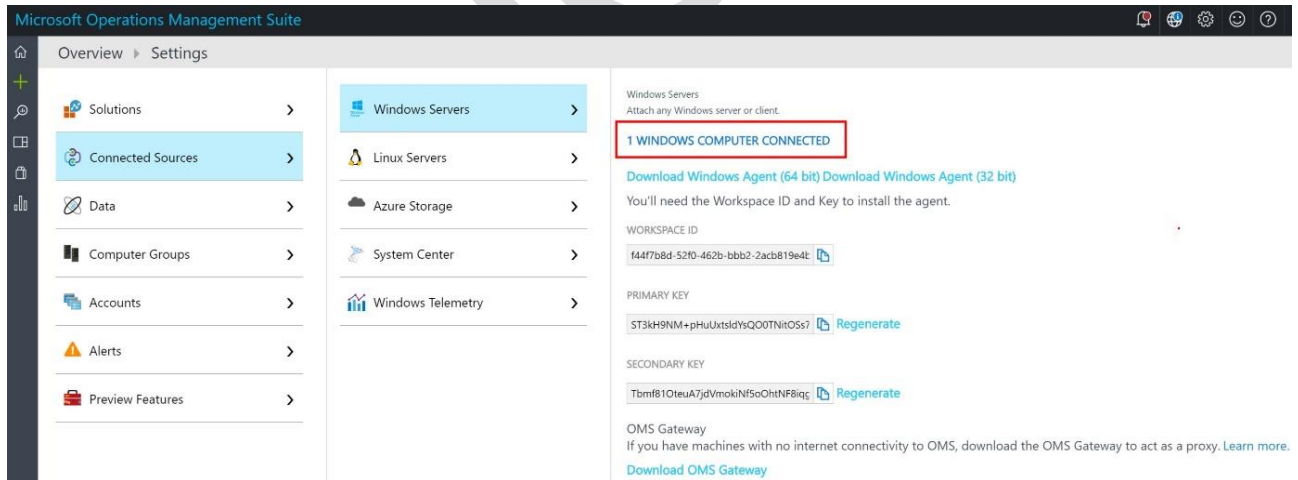


Workspace Data Sources grubundan Virtual Machines tıklanır. Burada bağlantı sağlayacağımız sunucular görülür ve Agent kurulumu yapılacak sunucu seçilip Connect butonuna tıklayarak kurulum gerçekleşir.



The screenshot shows the Microsoft Operations Management Suite (OMS) interface. The left sidebar contains navigation options: Overview, Settings, Solutions, Connected Sources, Data (highlighted), Computer Groups, Accounts, Alerts, and Preview Features. The main content area is titled 'Settings' and is divided into two columns. The right column is titled 'IIS Logs' and contains several options: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs (highlighted), Custom Fields, Custom Logs, and Syslog. A red box highlights the 'Collect W3C format IIS log files' checkbox, which is checked.

Agent kurulumu tamamlandıktan sonra portal üzerinden aktivasyonu tamamlamam için Settings – Data – IIS logs yollarını takip ederek Collect W3C format IIS log file linki işaretlenip, kaydedilir.



The screenshot shows the Microsoft Operations Management Suite (OMS) interface. The left sidebar contains navigation options: Overview, Settings, Solutions, Connected Sources (highlighted), Computer Groups, Accounts, Alerts, and Preview Features. The main content area is titled 'Settings' and is divided into two columns. The right column is titled 'Windows Servers' and contains several options: Windows Servers, Linux Servers, Azure Storage, System Center, and Windows Telemetry. A red box highlights the '1 WINDOWS COMPUTER CONNECTED' status. Below this, there are links for 'Download Windows Agent (64 bit)' and 'Download Windows Agent (32 bit)'. The 'WORKSPACE ID' is displayed as 'f44f7b8d-52f0-462b-bbb2-2acb819e4t'. The 'PRIMARY KEY' is displayed as 'ST3kh9NM+pHuUxtsldysQ00TnItOss7' with a 'Regenerate' link. The 'SECONDARY KEY' is displayed as 'Tbm810teuA7jdVmkniN5oOhtNF8iqg' with a 'Regenerate' link. At the bottom, there is a section for 'OMS Gateway' with a 'Download OMS Gateway' link.

Birkaç dakika sonra Connected Sources – Windows Servers bölümünde 1 Adet sunucu üzerine agent kurulumunun yapıldığı görünmektedir.



- On-Prem ortamlarda bulunan sunucularınız için, Operation Management Suite portalı üzerinde Settings - Connected Source – Windows Servers – Download Windows Agent link'ine tıklayarak Agent'imizi sunucumuza indirip ve yönetici olarak çalıştırıyoruz.

The screenshot shows the Microsoft Operations Management Suite (OMS) portal. The left sidebar contains navigation options: Overview, Settings, Solutions, Connected Sources, Data, Computer Groups, Accounts, Alerts, and Preview Features. The main content area is titled 'Settings' and has 'Windows Servers' selected. Below this, there are links for 'Linux Servers', 'Azure Storage', 'System Center', and 'Windows Telemetry'. On the right, the 'Windows Servers' configuration page is shown. It indicates '1 WINDOWS COMPUTER CONNECTED' and provides two download links for the Windows Agent: 'Download Windows Agent (64 bit)' and 'Download Windows Agent (32 bit)'. Below these links, there are fields for 'WORKSPACE ID' (containing 'f44f7b8d-52f0-462b-bbb2-2acb819e4e'), 'PRIMARY KEY' (containing 'ST3kH9NM+pHuUxtsldYsQO0TNitOSs7'), and 'SECONDARY KEY' (containing 'Tbmf81OteuA7jdVmokiNF5oOhtNF8iqg'). Red arrows point to the 'Download Windows Agent' links and the 'Regenerate' buttons for the keys.

The screenshot shows the 'Microsoft Monitoring Agent Kurulumu' (Installation) window. The title bar is blue and contains the Microsoft logo and the text 'Microsoft Monitoring Agent Kurulumu'. The main content area has a white background with a blue border. It features the heading 'Microsoft Monitoring Agent Kurulum Sihirbazı'na hoş geldiniz' (Welcome to the Microsoft Monitoring Agent Setup Wizard). Below the heading, there is a paragraph of text: 'Kurulum sihirbazı, Microsoft Monitoring Agent'i bilgisayarınıza yükler. Devam etmek için diğer tüm programları kapatın ve İleri'ye tıklayın.' (The setup wizard will install Microsoft Monitoring Agent on your computer. To continue, close all other programs and click Next.) At the bottom of the window, there are three buttons: '< Geri' (Back), 'İleri >' (Next), and 'İptal' (Cancel). The 'İleri >' button is highlighted in blue.

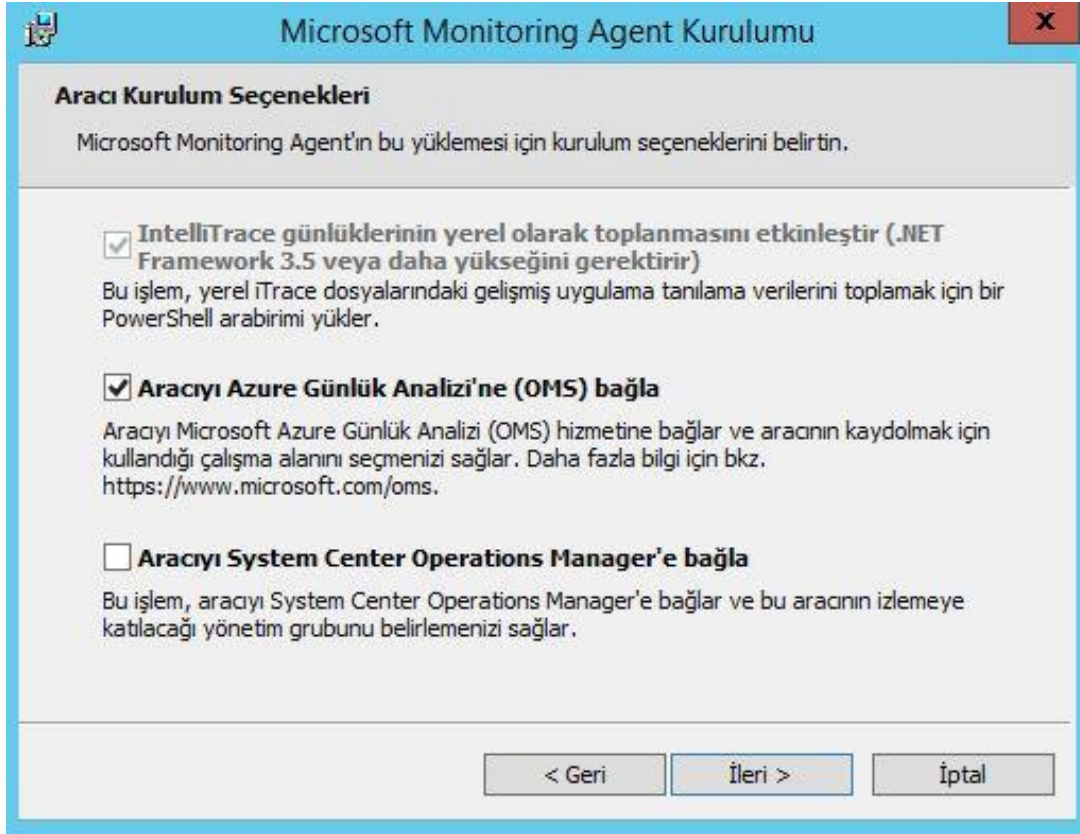
Agent kurulumu için 'ileri' diyoruz.



Yazılım lisansini kabul ediyoruz. 'I Agree' diyoruz.



Agent'in kurulacağı yeri belirtiyor kurulumdan sonra zaten bu yere bakıyor olacağız.C:\Program Files\Microsoft monitoring Agent\ klasoru altına kurulumu yapıyor olacaktır.



Agent kurulum için karşımıza 2 seçenek geliyor.

Connect the agent to Microsoft Azure operational Insights : Azure ile bağlantı sağlıyorsanız bu checkbox'ı işaretlemeniz gerekir,

Connect the agent to System Center Operations Manager : Bu checkbox'da ise System Center Operations manager ürünü kullanıyorsanız ve işlemleri bu yönde uygulacaksanız bu seçenektan ilerlemeniz gerekir.

**Microsoft Monitoring Agent Kurulumu**

**Azure Günlük Analizi**

Aracıyı Azure Günlük Analizi çalışma alanına bağlayın.

Çalışma Alanı Kimliği: f44f7b8d-52f0-462b-bbb2-2acb819e4b4e

Çalışma Alanı Anaht... [Redacted]

Azure Cloud: Azure Commercial

Çalışma alanı kimliği ve anahtarı <https://www.microsoft.com/oms/> adresindeki Azure Günlük Analizi portalında bulunabilir.

HTTP proxy yapılandırması sağlamak için Gelişmiş'i tıklayın.

İleri'ye tıkladığınızda bu özellikler Azure Günlük Analizi hizmeti tarafından doğrulanacaktır.

< Geri İleri > İptal

Portal üzerindeki oluşturulan ID ve Key'i Agent kurulum penceresinde istenilen yere kopyalıyoruz. Daha sonra 'ileri' diyoruz.

**Microsoft Monitoring Agent Kurulumu**

**Microsoft Update**

Bilgisayarınızın güvenli ve güncel durumda kalmasına yardımcı olmak için Microsoft Update'i kullanın

Microsoft Update, Windows ve bu ürün dahil diğer Microsoft Ürünleri için güvenlik ve önemli güncelleştirmeleri sağlar. Güncelleştirmeler Otomatik Güncelleştirme ayarınız kullanılarak teslim edilir veya Microsoft Update web sitesini ziyaret edebilirsiniz.

Güncelleştirmeleri denetlediğimde Microsoft Update'i kullan (önerilir)

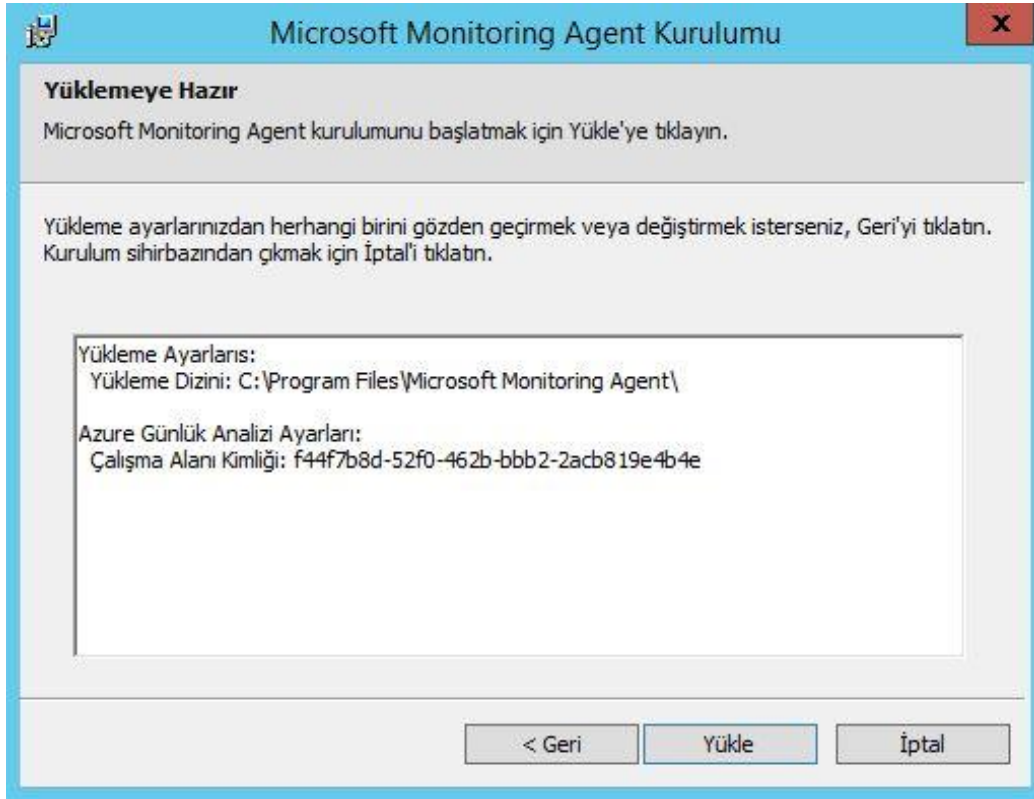
Microsoft Update'i kullanmak istemiyorum

<http://update.microsoft.com/microsoftupdate/v6/about.aspx?ln=en> adresindeki Microsoft Update SSS' sayfasına bakın

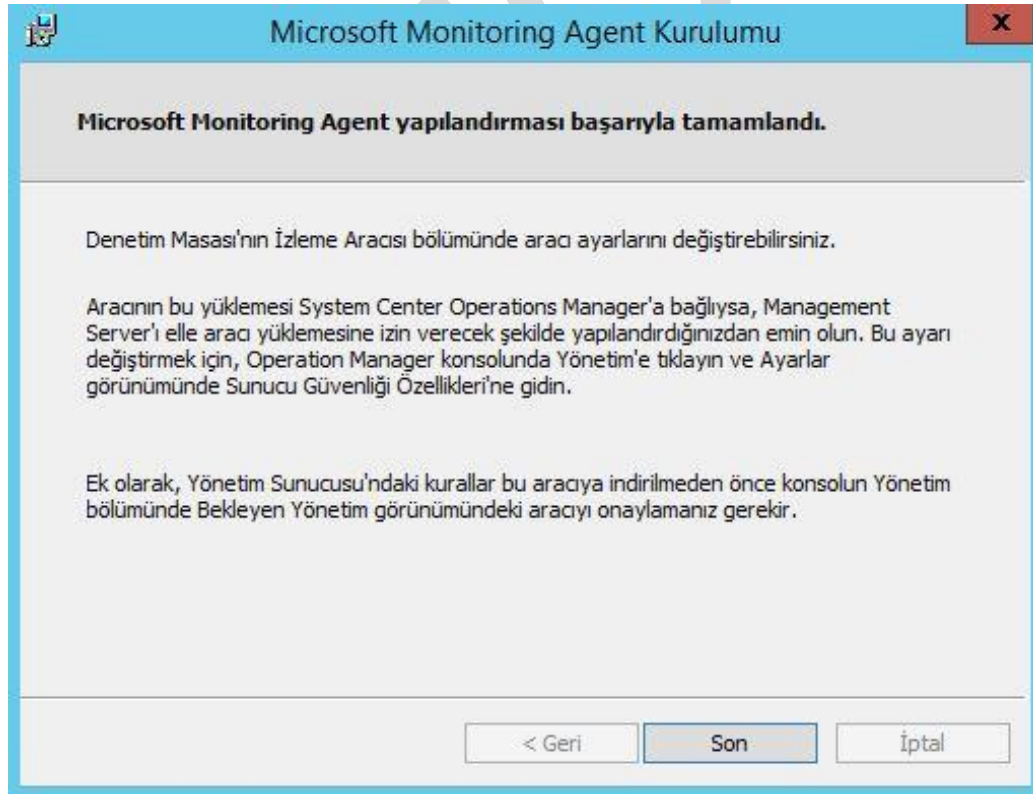
<http://update.microsoft.com/microsoftupdate/v6/privacy.aspx?ln=en> adresindeki çevrimiçi Gizlilik bildirimimizi okuyun

< Geri İleri > İptal

Microsoft Update'lerini henüz istemediğimi belirtiyorum ve 'ileri' butonu ile ilerliyorum.



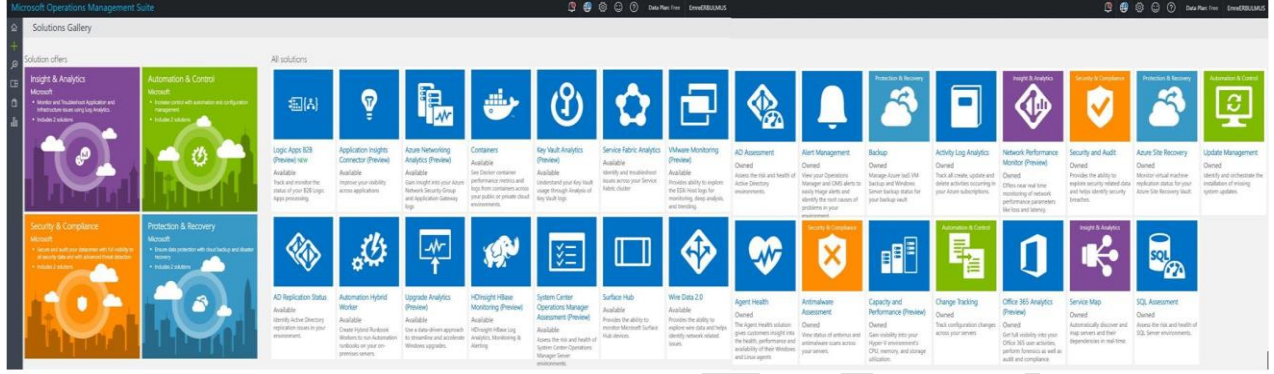
Kurulumu geçmeden önce kısa bir rapor sunuyor bize, Raporu inceleyerek 'Install' butonuna tıklıyoruz.



Agent kurulumu başarılı bir şekilde tamamlanıyor. 'SON' butonu ile sonlandırıyoruz.

## Operation Management Suite Solutions Gallery

Yazımızın başında anlatmak istediğimiz gibi uçtan uca bir çözüm sağlayan Oms, genel anlamıyla her ürüne hizmet vermektedir. İlk günden bugüne kadar yeni yeni çözümler eklenerek Cloud ürünlerinden kendini bir adım daha öne çıkartmıştır. Her çözümün farklı bir görevi ve bir iş akışı bulunmaktadır. Bu çözümleri tam anlamı ile aşağıdaki ekran görüntüsünde inceleyebilirsiniz.



Makalenin ilk serisinde anlatıldığı üzere Microsoft, OMS mimarisini 4 ana başlıkta birleştirdiğini Solutions Gallery bölümünden de görebiliyoruz. Çözümlerin bir kısmını sizlere anlatmaya çalışacağım;

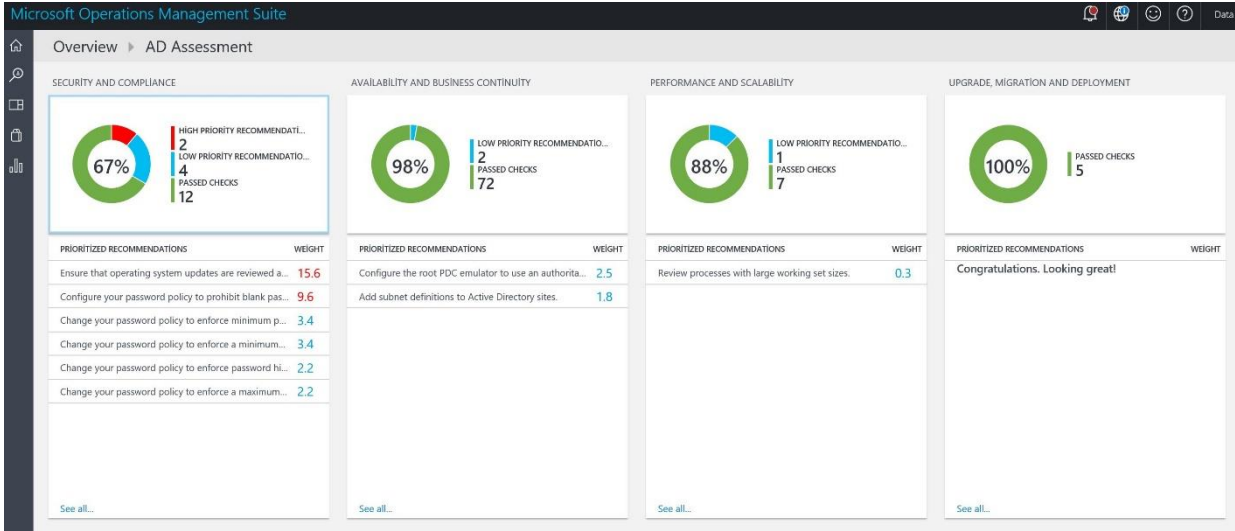
### 1. AD Assessment

Active Directory ortamının sağlık ve risk durumunu değerlendiren bir servistir. Aynı zamanda düzenli aralıklarla alt yapı ile ilgili öneriler sunmaktadır. Bu öneriler doğrultusunda alt yapılarda oluşabilecek felaketler önlenabilir. AD Assesment ile Active Directory'e ait güvenlik logları, performans, upgrade ya da deployment gibi Active Directory ile ilgili Assesment anlamında tüm süreçlerin takibinin yapılacağı monitörler yer almaktadır.

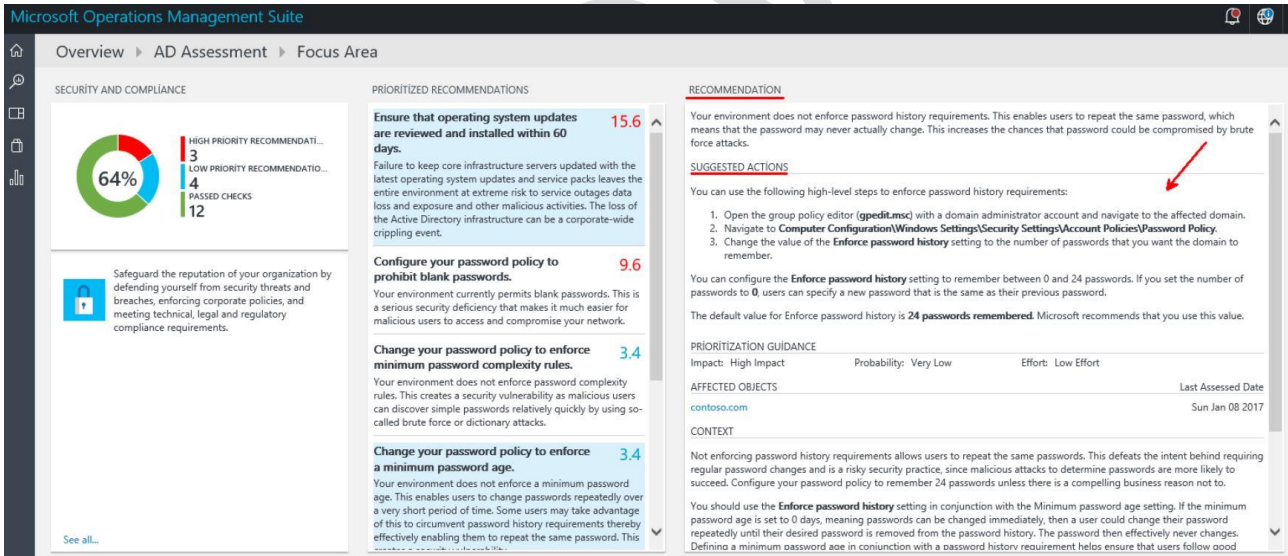


AD Assesment logları temelde 5 alt başlıkta toplanmış olup, her alt başlık kendi içerisinde loglar toplamaktadır.

- Security and Compliance
- Availability and Business Continuity
- Performance and Scalability
- Upgrade, Migration and Deployment



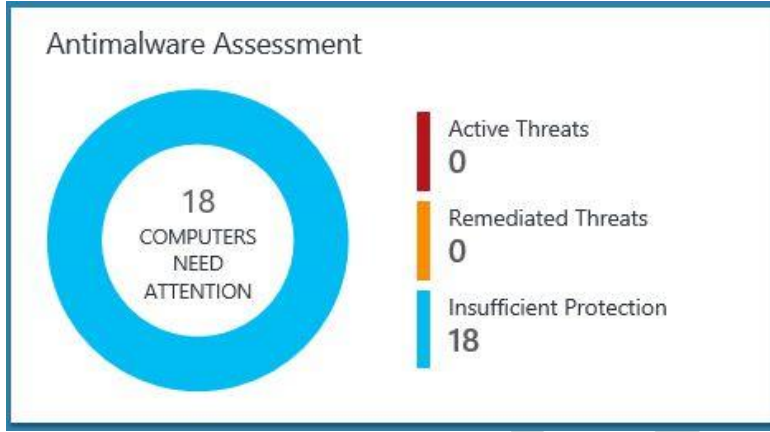
AD Assessment, logları Microsoft'un Best Practices Analyzer (BPA)'ına göre kontrol edip akabinde de kullanıcılara topladıkları logları analiz ederek öneriler sunmaktadır. AD Assessment'in sunmuş olduğu logları monitorleme işlemleri ile beraber sunulan öneriler ile de alt yapılarınızı daha düzgün bir hale getirebilirsiniz. AD Assessment ile örnek dashboard aşağıdaki gibidir



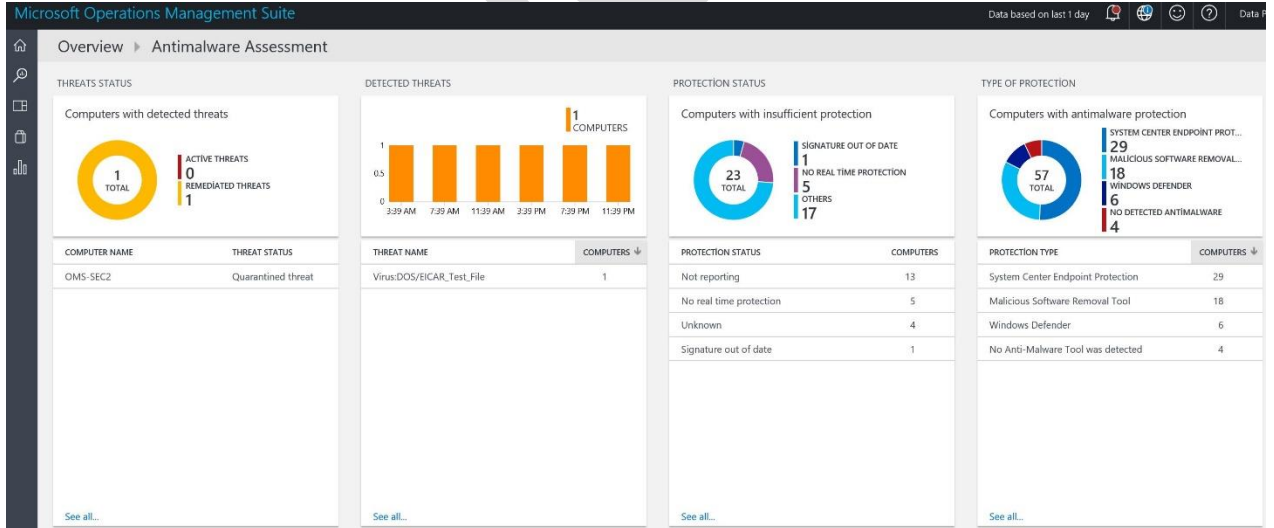
AD Assessment - Security and Compliance tabından herhangi bir aksiyona tıkladığınızda, öncelikli önerilerine göre sıralandığını göreceksiniz. Önem derecesi yüksek olan işlemleri ilk sıraya koyarak sizlere konuyla ilgili tavsiyeler sunar. Ekran görüntüsünü incelersek, ortamın kullanıcı şifreleri ile ilgili güvenli bir çalışma yapılmadığı önerisinin sunduğunu tavsiyeler kısmında incelenebilir. **Suggested Actions (Önerilen Eylem)** tabına baktığımızda ise tavsiyeler kısmında önerilen uyarı ile ilgili nasıl bir çözüm yolu sağlayacağınızı detaylı bir şekilde anlatmaktadır. Ayrıca Context tabında ise çözümle ilgili Microsoft'un technet makaleleri sunarak sizlere en doğru yolu gösterir.

## 2. Malware Assessment

Microsoft OMS çözümlerinden Malware Assessment hem Windows hem de Linux sunucularınızın zararlı yazılım durumlarını ve potansiyel tehditlerini takibini sağlayan çözümdür. Malware Assessment ile hem Azure hemde local ortamındaki makinaların üzerindeki Windows Defender'ın aktif durumunu ve sunucu ya da bilgisayarları tehdit eden durumlar gözlemlenir. Aynı zamanda Antimalware Assessment izlenen sunucularda algılanan tehditleri okur ve belirli aralıklarda ise işlenen verileri buluta gönderilir.

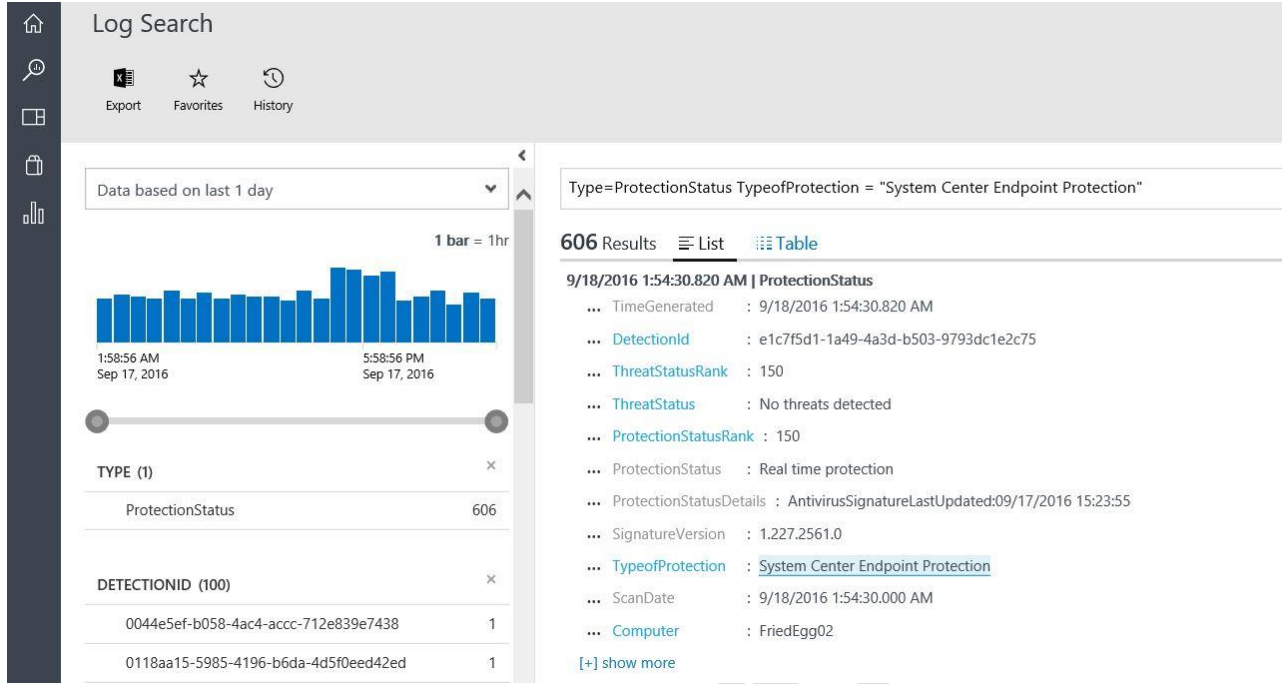


Solutions Gallery bölümünden Antimalware Assessment aktif edilir. Kısa süre içinde ilgili Logların ekrana yansıdığını göreceksiniz.



Buluta gönderilen verileri Antimalware Assessment paneli üzerinden görebilirsiniz. Bunlar; Threats Status, Detected Threats, Protection Status, Type The Protection tablaları olmak üzere 4'e ayrılmaktadır.

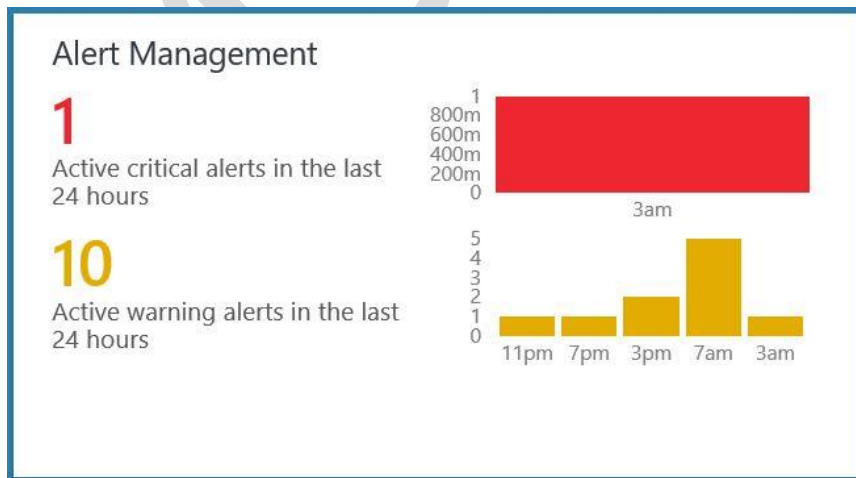




İstediği bağı olarak seçilen log'un üzerine tıklandığında karşınıza detaylı bir şekilde inceleyebileceğiniz bir panel gelecektir. Burada sunucu ve client cihazlarınızın tehdit altında olup olmadığı ayrıntılı bir şekilde görebilirsiniz.

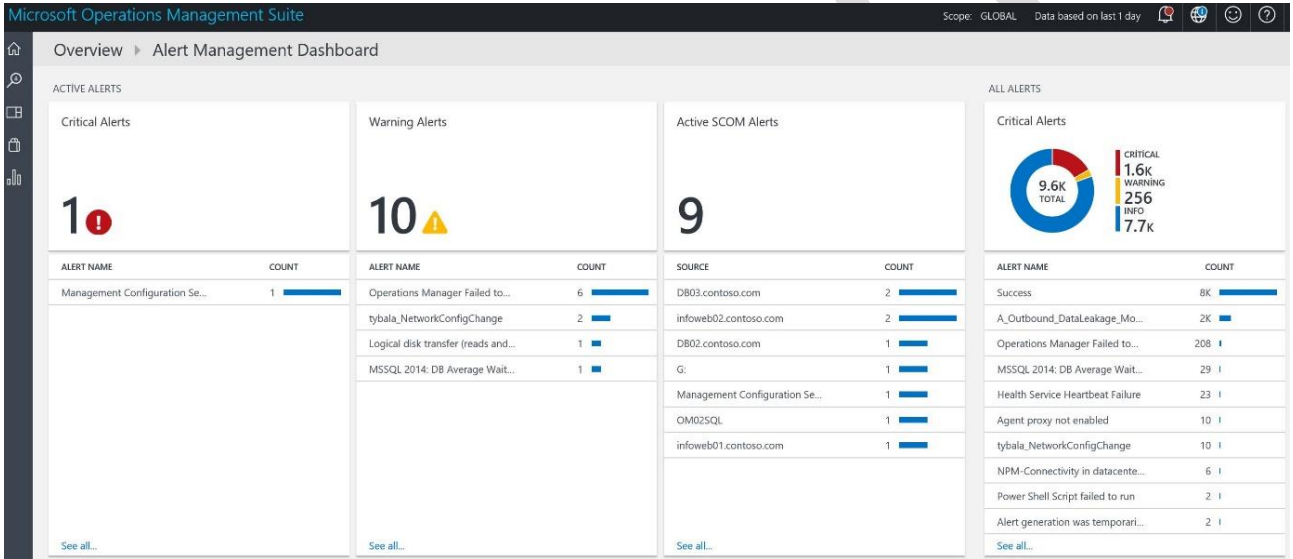
### 3. Alert Management

Operations Management üzerindeki uyarılarınızı ve bunlara bağlı tüm sunucularınızı görüntülemenize yardımcı olur. Bu çözüm aracı sayesinde, uyarıları kolayca analiz etmenize ve sunucunun temel nedenlerini belirlemenize yardımcı olabilir. Ayrıca OMS içinde üretilen uyarıların kontrol edilmesine ek olarak, bu uyarıları belirlediğimiz zaman diliminde ve istediğimiz aralıklarla mail yolu ile raporlayabiliyoruz.



## Varolan ortamımızda nasıl Alert'ler oluşturabiliriz ;

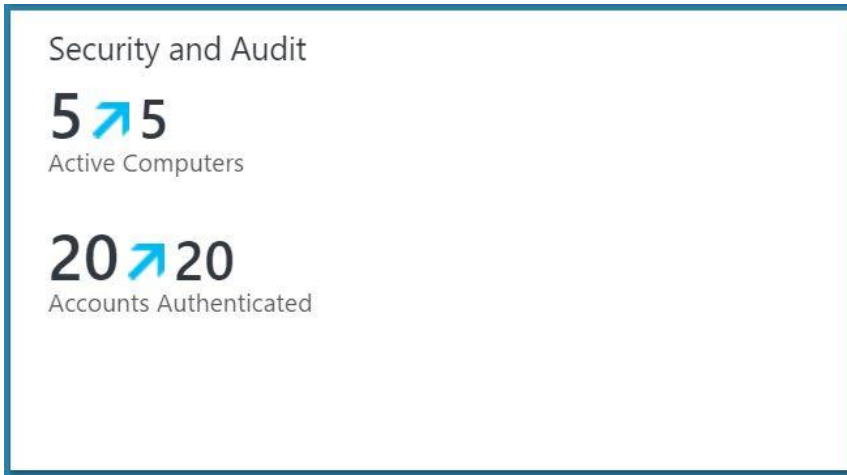
- OMS ile entegre olan sunuculara, her uzakmasaüstü yapıldığından System Admin'ine mail atılabilir.
- Bir kullanıcı hesabının sunucu üzerine kaç kere LOGON olduğunun uyarı maili atılabilir.
- Critical update'lerini durumunu gösteren bir uyarı maili gönderilebilir.
- Sunucuların Disk,Cpu ve Ram durumunu gösteren bir uyarı maili gönderilebilir.



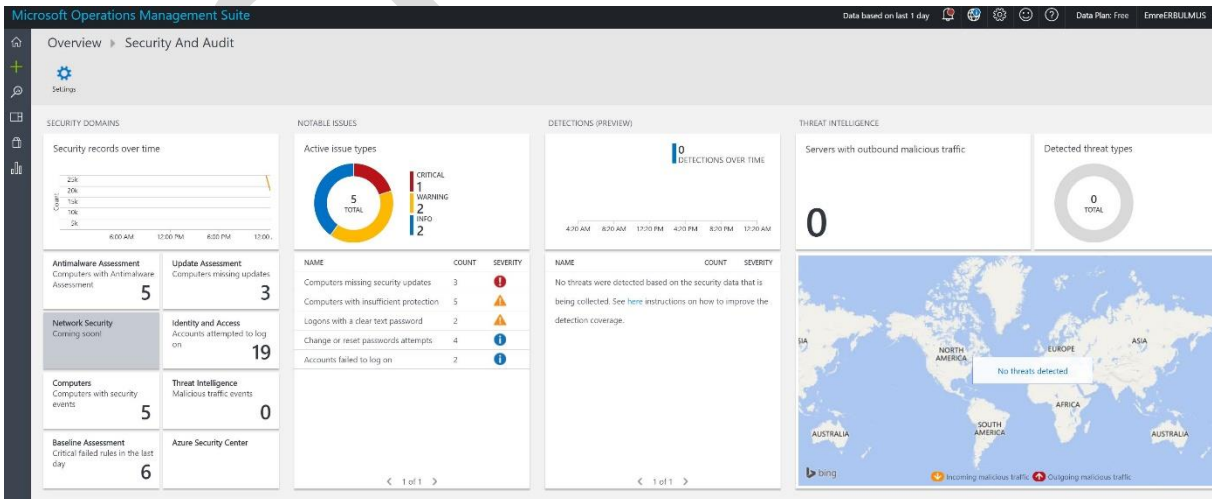
Aler Management bölümüne tıkladığımızda yukarıdaki ekran görüntüsü bizi karşılayacaktır. Bu Dashboard üzerinde oluşturduğumuz Alerts'in ne zaman çalıştığını ve çalışırken alınan uyarıları sizler sunmaktadır. Scom üzerindeki uyarıları da Active Scom Alerts bölümünde takip edebilirsiniz.

#### 4. Security And Audit

Azure Monitoring'nin "Security And Audit" çözümü, sunucu ve bilgisayarlardan toplanan güvenlik ve denetim verileri üzerinde analizler yapılmasını sağlayan ve monitör edilecek makinalar ile bağlantı sağlandığında cihazlar üzerinde alınan aksiyonların takibini de gerçekleştirebildiği çözümdür. Ayrıca ortamda gerçekleşen problemleri görüntüleyerek, BT süreçlerine yarar sağlar.



Security Domains - Notable Issues - Detections (Preview) - Threat Intelligence isimli bölümlerden oluşmaktadır. Bunlarda kendi içinde dallanarak yapınızın en uc noktasındaki aksiyonu inceleyebilirsiniz.

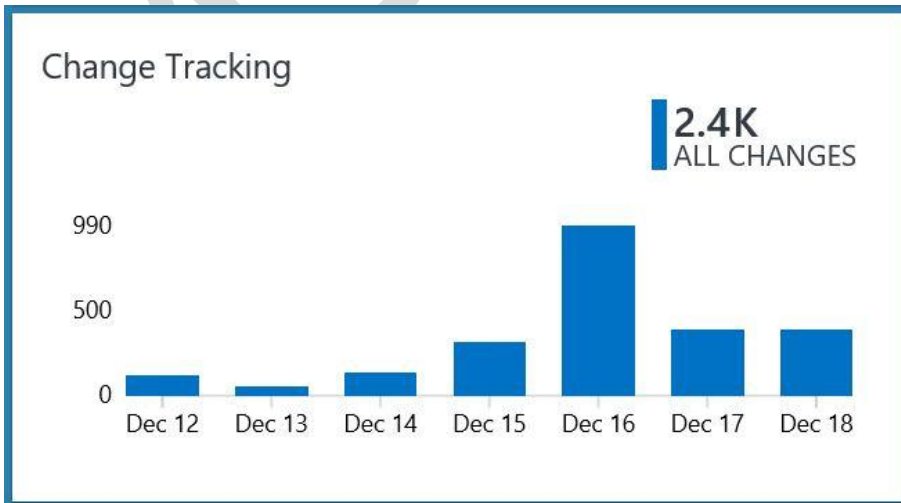


OMS Güvenlik ve Denetim panosu dört ana kategoride düzenlenmiştir:

- **Güvenlik Etki Alanları:** Bu bölümde güvenlik kayıtlarını içeren bilgiler görür. Bu kayıtlar kötü amaçlı yazılım değerlendirmesine, ağ güvenliği, kimlik ve erişim bilgileri, sunucu ve client güvenliği ve Azure Güvenlik Merkezi 'dir.
- **Önemli Sorunlar:** Bu seçenek etkin sorunların sayısını ve sorunların önem derecesini hızlıca tanımlamanıza yardımcı olur.
- **Algılama (Önizleme):** Kaynaklarınıza karşı gerçekleşen güvenlik uyarılarını görselleştirerek saldırı düzenlerini tanımlayabilmenizi sağlar.
- **Tehdit Bilgileri:** Giden kötü amaçlı IP trafiğine sahip sunucuların toplam sayısını, kötü amaçlı tehdit türünü ve bu IP'lerin nereden geldiğini gösteren bir haritayı görselleştirerek saldırı düzenlerini tanımlayabilmenizi sağlar.
- **Sık kullanılan güvenlik sorguları:** Bu seçenek ortamınızı izlemek için en sık kullanabileceğiniz güvenlik sorgulama bölümüdür. Bu sorgulardan birine tıkladığınızda, bu sorguya ilişkin sonuçlar elde edilir.

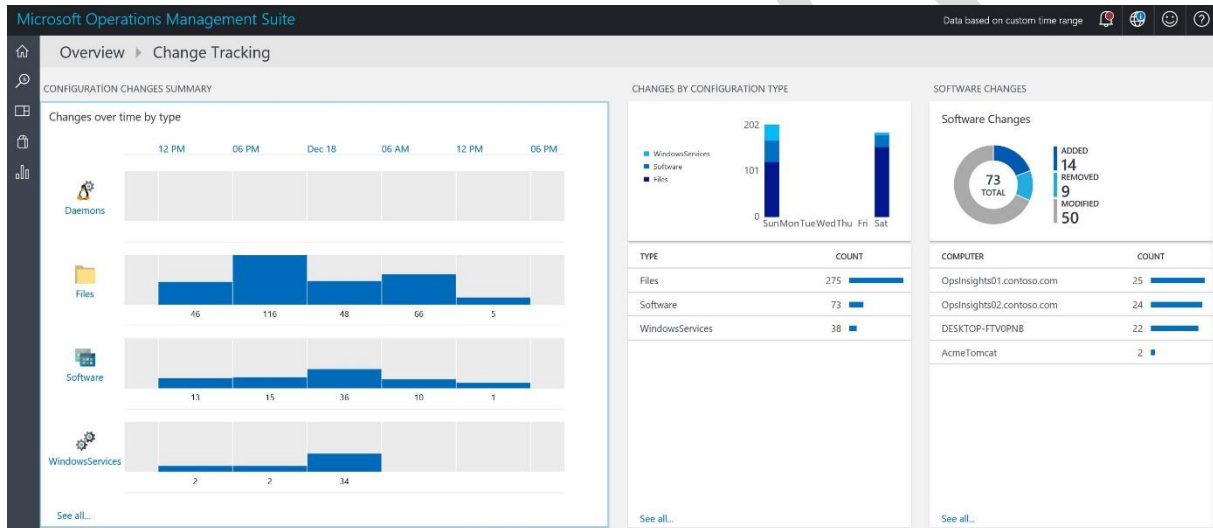
## 5. Change Tracking

Sunucular üzerinde herhangi bir yüklü olan yazılımlarda, uygulamalarda ya da serviste değişiklik olduğunda "Change Tracking" bölümünden gözlemlenebilir. Temelde aşağıdaki değişiklikleri monitör edilmekte olup, loglara ilgili alt başlıklardan erişim sağlanır.



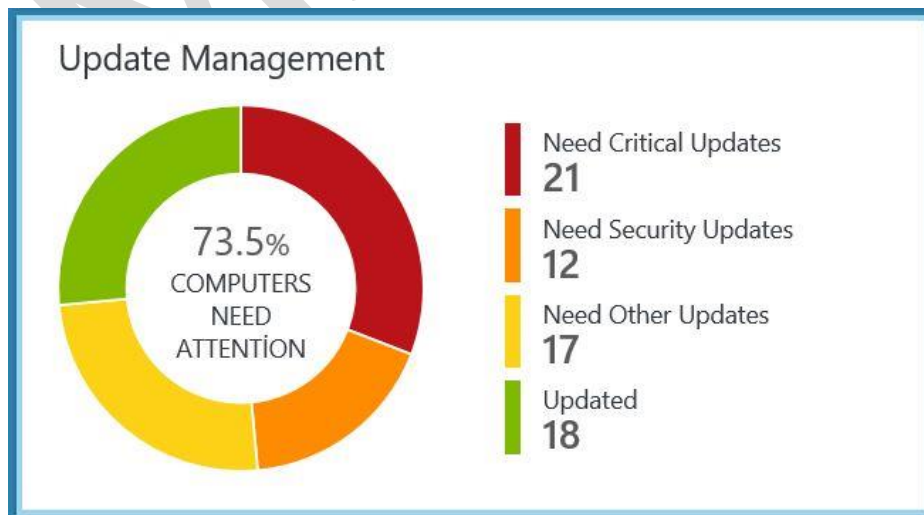
Kullanıma hazır görünümle, önemli senaryolara ilişkin bilgiler edinebilirsiniz, Bu bilgiler aşağıda verilmektedir;

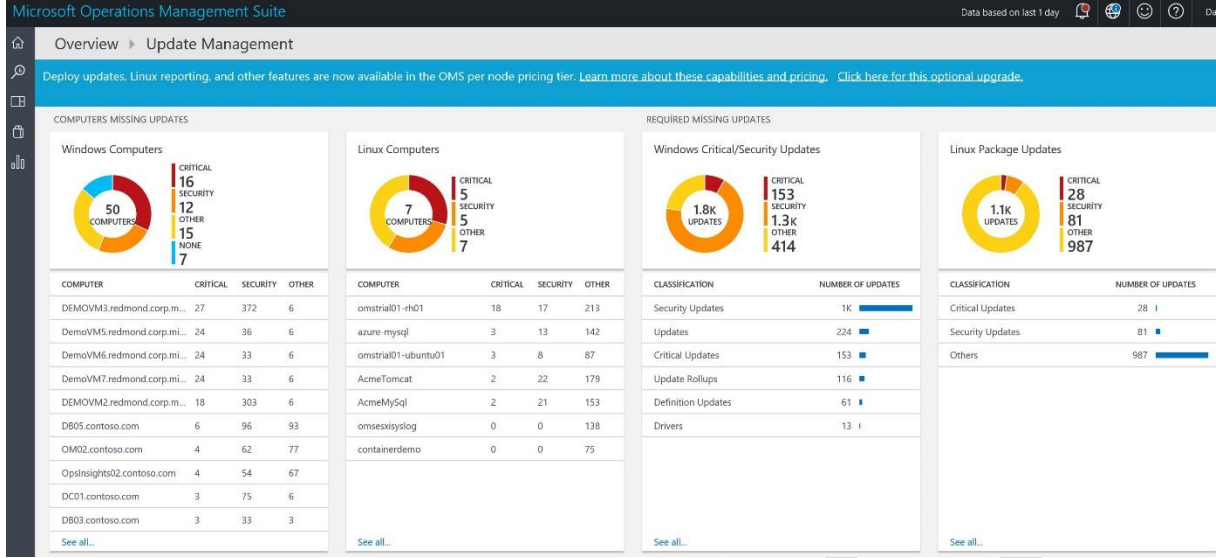
- Yazılım ve Windows hizmetleri için yapılandırma türüne göre değişiklikler
- Bireysel sunucular için uygulamalar ve güncellemeler için yazılım değişiklikleri
- Her bir uygulama için yazılım değişiklikleri sayısı
- Bireysel sunucular için Windows hizmet değişiklikleri
- Exchange, SQL, SharePoint gibi belirli bir iş yüküne uygulanan değişiklikler



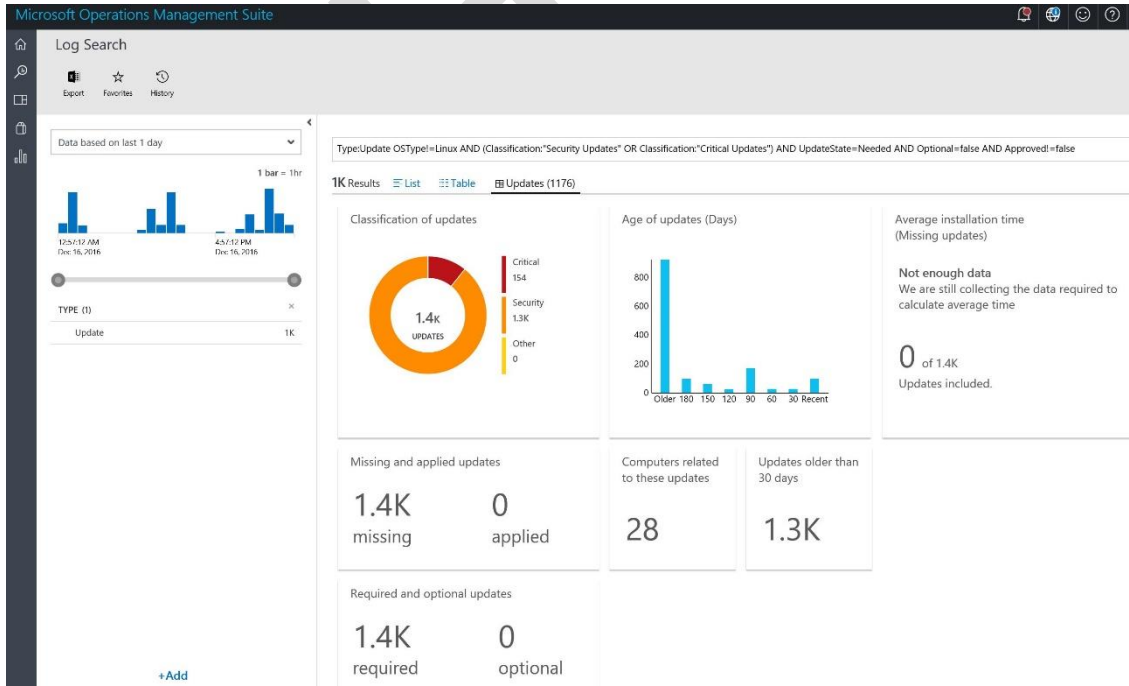
## 6. Update Management

OMS dashboard'una update management çözümünü eklediğinizde, Windows ve linux sunucularına ait update'lerin durumu görebilirsiniz.





Update Management çözümüne tıkladığınızda Computers Missing Updates (Windows Computers - Linux Computers) - Required Missing Updates (Windows Critical/Security Update - Linux package Update) isimli iki ana başlık göreceksiniz. Computers Missing Updates , hangi sunucuların update alıp, almadığını ve bu update'lerin sayısını gösteren bölümdür. Required Missing Updates, ise windows ve linux sunucularına ait eksik update'leri gösteren bölümdür.

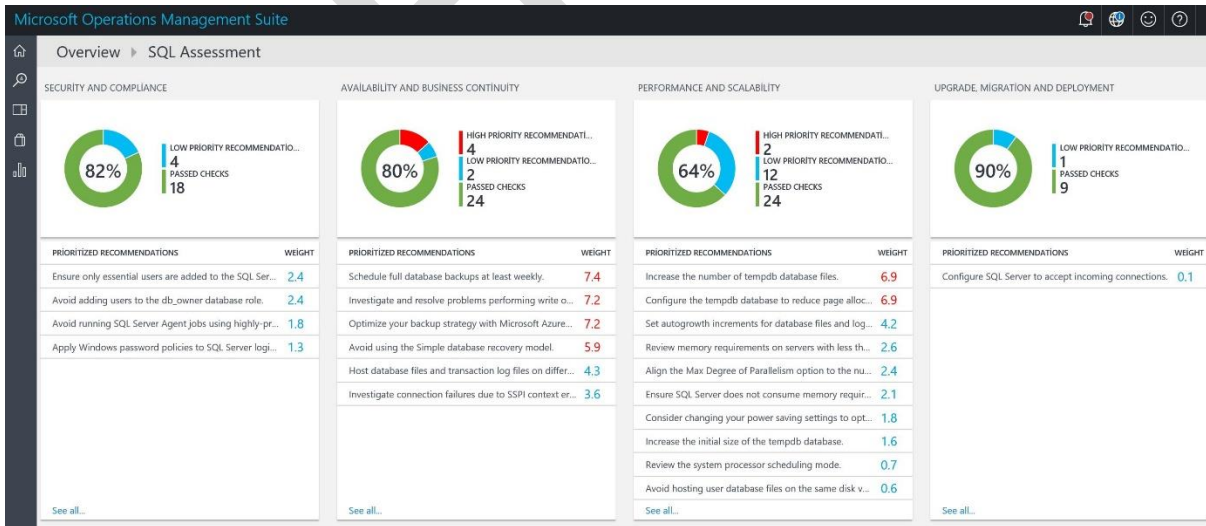


Örnek olarak Windows Critical/Security Update tıkladığımızda Windows sunucuların güvenlik ve kritik güncellemelerin analiz tablosunu görebilirsiniz.

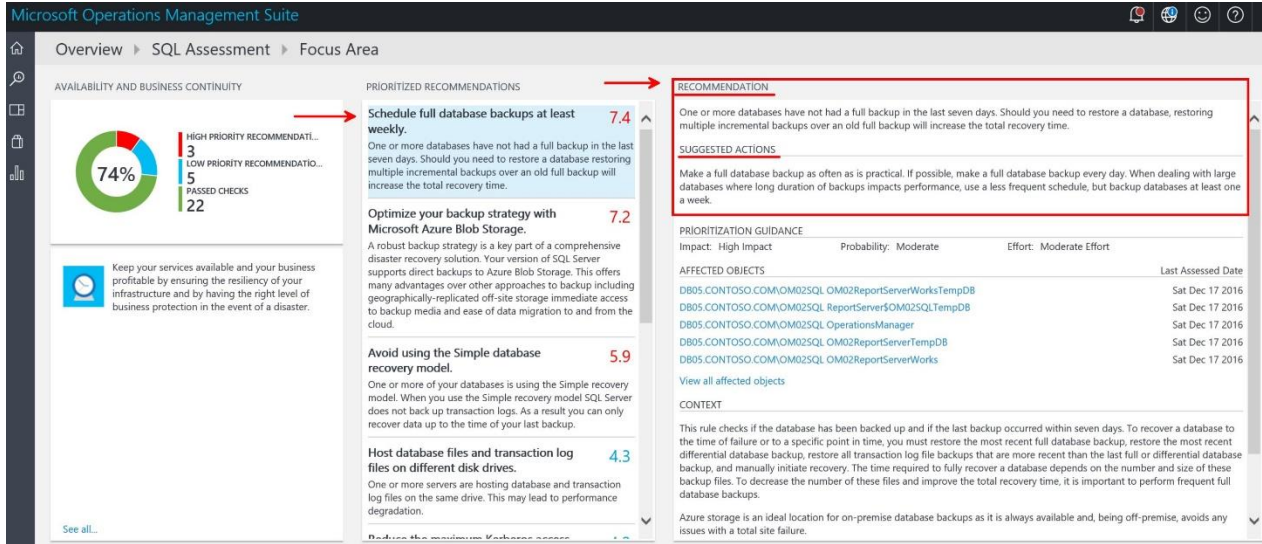
## 7. SQL Assessment

SQL Assessment bölümünde SQL sunucusu ile ilgili alınması gereken önlemleri ve önerileri bulabilirsiniz. Bu öneriler değerlendirilerek SQL alt yapısında iyileştirmeler yapıлып, stabil çalışması sağlanabilir. SQL Assessment logları temelde 5 alt başlıkta toplanmış olup, her alt başlık kendi içerisinde loglar toplamaktadır.

- Security and Compliance
- Availability and Business Continuity
- Performance and Scalability
- Upgrade, Migration and Deployment



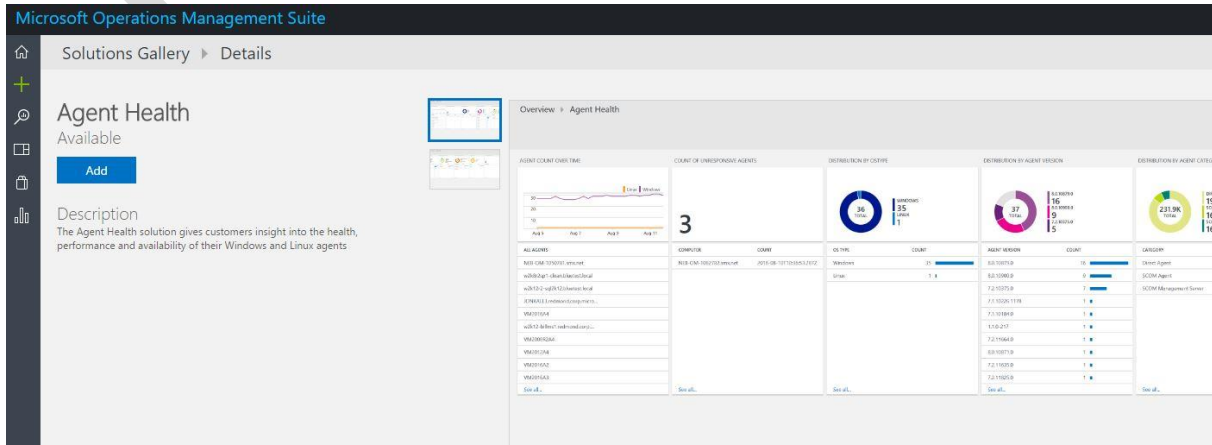
Sql Assessment solutions'ına tıkladığında çeşitli analizler görünmektedir. Bu öneriler doğrultusunda SQL veri tabanının sağlık durumunu inceleyebilirsiniz. Her öneriler öncelik sırasına göre bir puanlama ile yansıtılır.



Resimde gösterildiği üzere öncelik sırası en yüksek olan 7.4 puanlı öneriyi inceleyelim. “**Schedule full database backups at least weekly**” bu uyarı SQL veri tabanının haftada en az bir kez yedekleme yapılması gerektiğinin uyarısını vermektedir. Recommendation kısmında belirtilen suçlar üzerinde son 7 gün içinde bir yedekleme yapılmadığı gözlemlenmiştir. Buna istinaden bir attaki bölümde ise (Suggsted actions) yedekleme yapılmayan sunucuların biran önce yedekleme yapılması gerektiğini vurgumaktadır. Böylece düzenli bir yedekleme sonrasında veri tabanının performansını etkilediğini görebilirsiniz.

## 8. Agent Health

Agent Health, Windows ve linux sunucularınız üzerinde kurulu olan OMS agent'ların durumu ve dağıtım istatistiklerini görsel halde gösteren bir çözümdür. Birden fazla sunucularınızın olduğunu düşürsek, bu çözümle birlikte sunucular üzerinde Agent sağlık durumu yakından takip edebilirsiniz. Ayrıca Agent'inizin OMS ile iletişim halinde olup olmadığını da gözlemleyebilirsiniz.





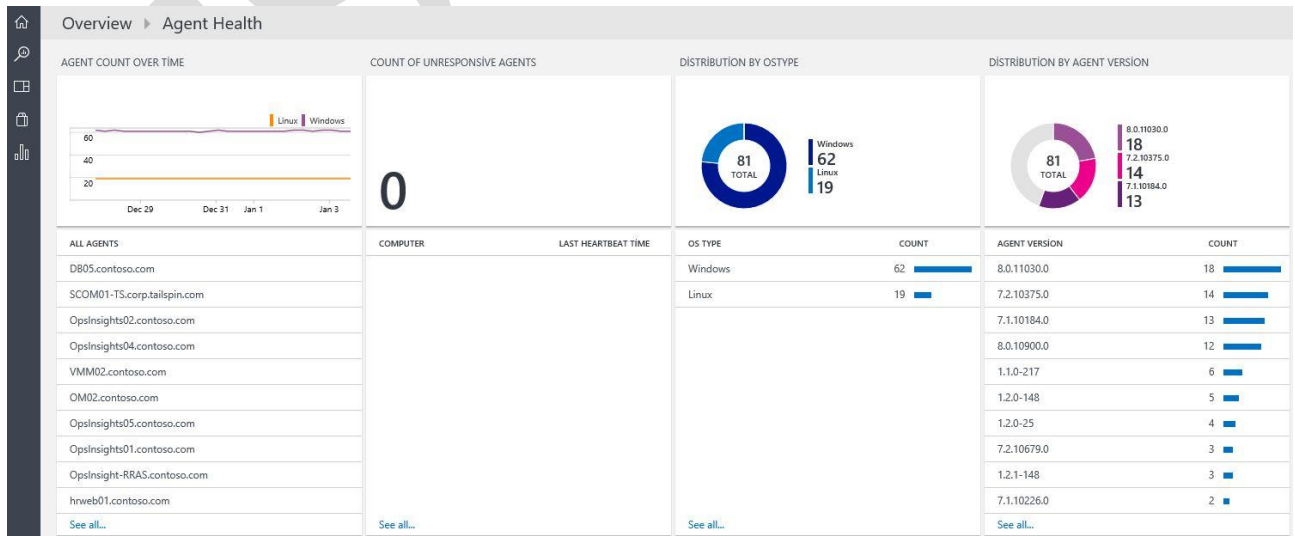
Solutions Gallery bölümünden Agent Health çözümünü aktif hale getirilir.



Çözümü etkinleştirildikten sonra, Agent Health çözümü OMS Dashboard sayfanıza eklenir ve son 24 saat içinde toplam agent sayısını ve yanıt vermeyen temsilci sayısını gösterir.

Agent Health aşağıdaki başlıklardan oluşmaktadır. Bunlar ;

- Agent count over time
- Count of unresponsive agents
- Distribution by OS Type
- Distribution by Agent Version
- Distribution by Agent Category
- Distribution by Management Group
- Geo-location of Agents
- Count of Gateways Installed

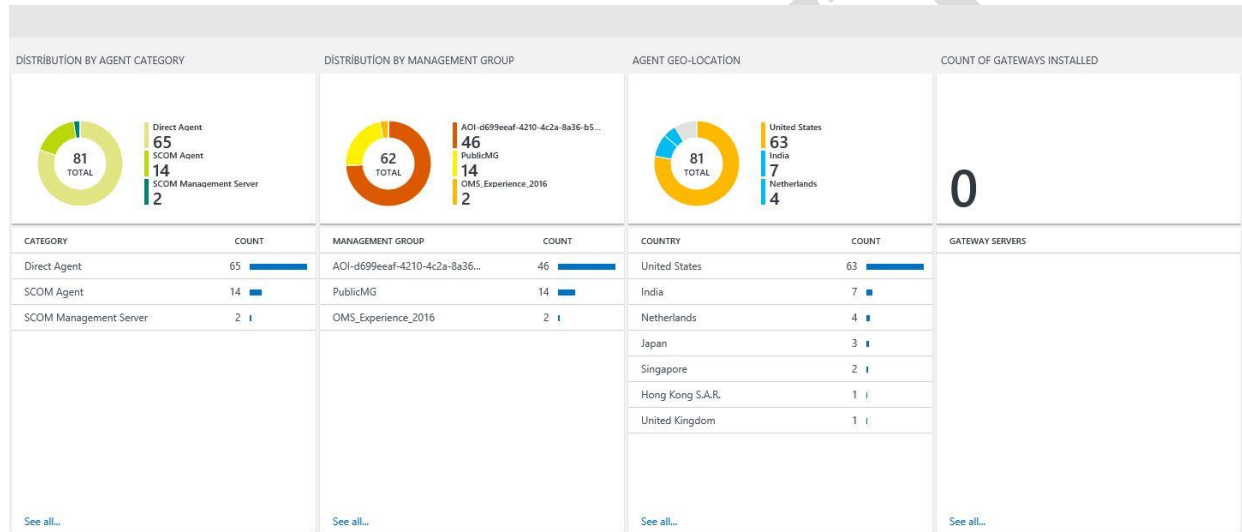


Agent count over time : Hem Linux hem de Windows agent'ların kaç günlük geçerli olduklarını gösteren kısımdır

Count of unresponsive agents : Son 24 saat içinde bir sinyal gönderen agent'ları listeler.

Distribution by OS Type : Ortamınızda kaç tane Windows ve Linux agent'ının bulunduğunu gösteren bölümdür.

Distribution by Agent Version : Ortamınıza kurulan farklı ajan sürümlerinin ve sayısını gösterir.

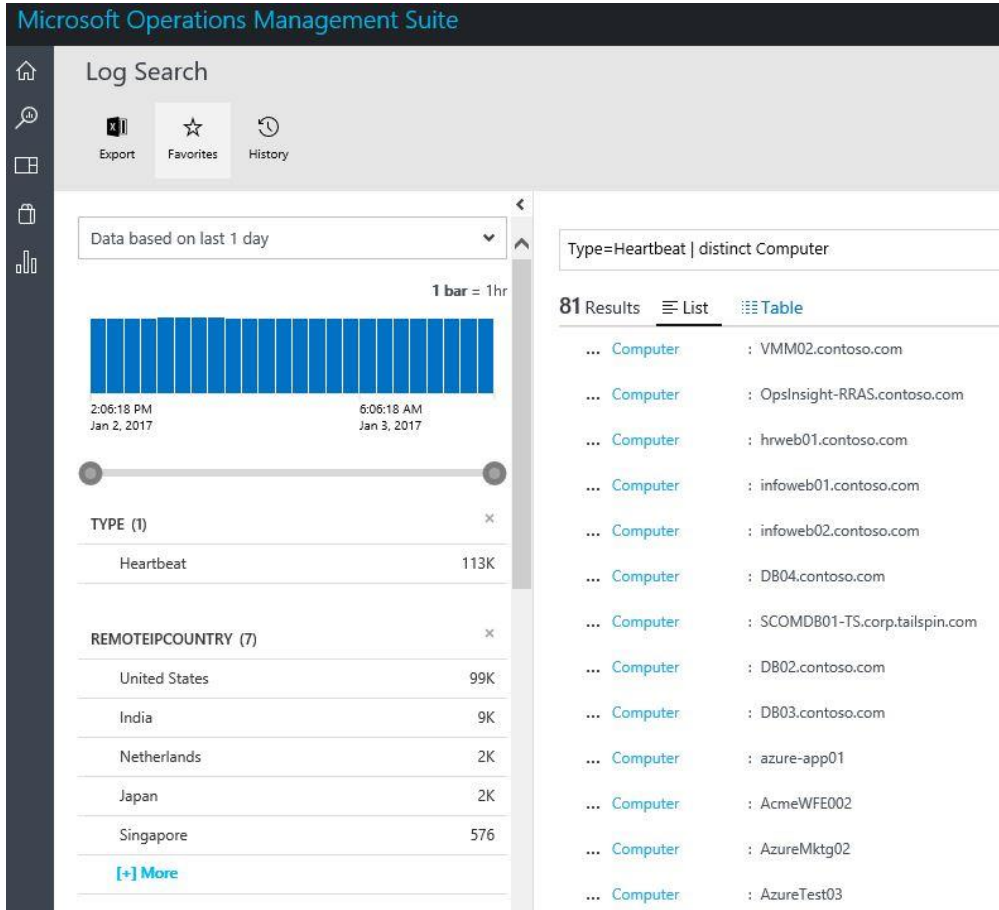


Distribution by Agent Category : Agent heartbeat olaylarını gönderen farklı agent kategorilerinin bir bölümüdür. (SCOM ve SCSM yönetim kontrolleri)

Distribution by Management Group : Ortamınızdaki farklı SCOM Yönetim gruplarını gözlemlediğiniz bölümdür.

Geo-location of Agents : Agent'ların bulunduğu farklı ülkelerin ve her ülkede kurulu olan agent'ların toplam sayısı gösteren bölümdür.

Count of Gateways Installed : OMS Gateway kurulu olduğu sunucuların sayısının listelendiği bölümdür.



Type=Heartbeat | Distinct Computer sorgu cümlesi sayesinde OMS Agent'i kurulu olan tüm bilgisayarları listeleyebilirsiniz.

## Operation Management Suite **Kullanıcı Yönetimi**

Operation Management Suite üzerinde kullanıcı yetkilendirme işlemi Settings - Account - Manage Users yollarını takip ederek yapabilirsiniz. Bu pencerenin üst bölümünde Tenant'inizi, Domain name'mi ve size atanan tenant id'nizi görebilirsiniz.

Microsoft Operations Management Suite

Overview > Settings

Solutions >

Connected Sources >

Data >

Computer Groups >

Accounts >

Alerts >

Power BI >

Preview Features >

Workspace Information >

Manage Users >

Azure Subscription & Data Plan >

Automation Account >

MANAGE USERS

Link Organization

Organizational accounts will be added from the following Azure Active Directory Tenant:

Tenant Display Name:  
PeakUp Information Technologies

Tenant Domain Name:  
peakup.org

Tenant ID:  
c8be3380-d32e-4fb4-99f9-e815f6ede362

Change Organization

Add Users

Choose account type:  Organizational Account  Microsoft Account  Microsoft Support

Choose user type:  Administrator  Contributor  ReadOnly User

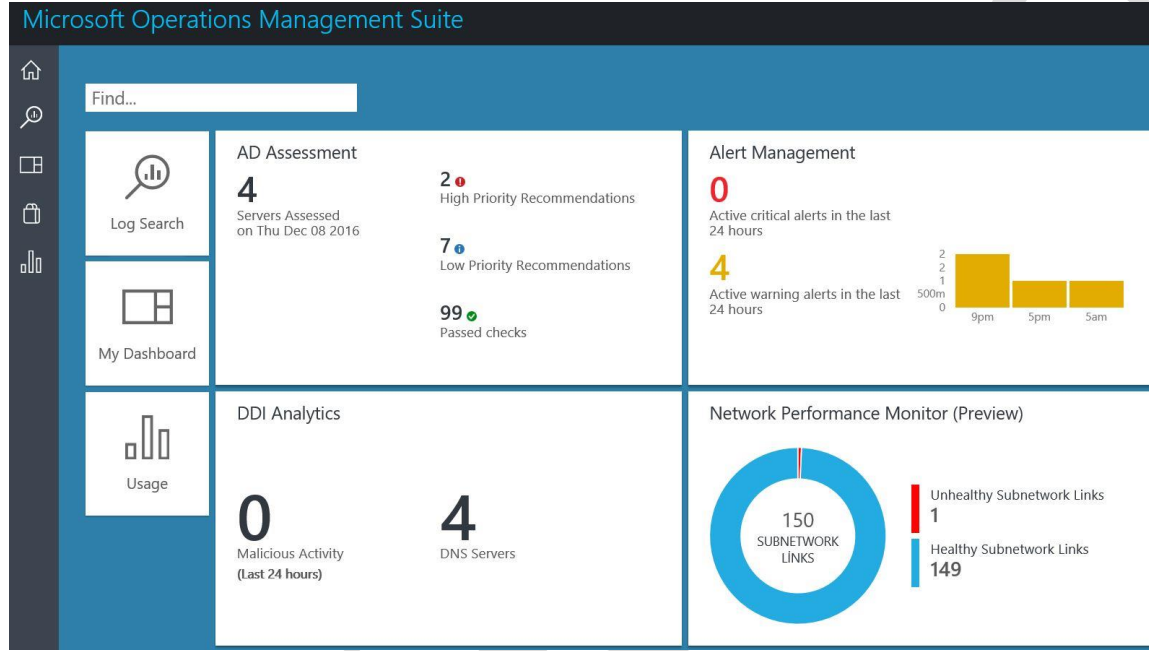
\* Administrators can invite new users to join this workspace

Choose User/Group:  User  Group

Type user name here... Add

USER NAME	ADMINISTRATOR	CONTRIBUTOR	READONLY USER	STATUS	REMOVE
emre.erbulmus@peakup.org	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Active	X
emre.erbulmus@peakup.org	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Active	X

Alt bölümde ise kullanıcı yetkilendirme işlemlerini göreceksiniz. Resimde görüldüğü üzere ilgili Search kısmına User ve Group isimleri aratarak OMS portalına istenilen kişilere yetki verebiliriz. Bu yetkiler hesap türüne ve kullanıcı türüne göre ikiye ayrılır. Hesap türüne göre, Organizational Account - Microsoft Account – Microsoft Support diye 3'e ayrılır. Bu hesap türlerine ise Administrator – Contributor – ReadOnly User yetkileri verilebilir.



Örneğin herhangi bir hesap türü altındaki bir kullanıcıya ReadOnly User yetkisi verdiğinizde yukarıdaki resimde görüldüğü gibi Settings ve Usage butonları kaybolacaktır. Bu sayede hiçbir kullanıcı varolan ayarlar üzerinde değişiklik yapamayacaktır.

## Operations Management Suite ile Office 365 Kullanımı

OMS sayesinde birçok veri merkezinizden ya da bulut platformu üzerinden topladığımız log'ları artık, Office 365 tarafında yapılan aksiyonların takibini sağlayarak ilgili log'ları topluyor olacağız. Office 365 solutions Gallery 'nin desteklediği iş yükleri ise Azure AD, Exchange ve SharePoint 'tir. İlgili Office 365 hesabınızı ekledikten sonra hiç şey yapmanıza gerek kalmayacaktır, zaman içerisinde belirli aralıklarla Office 365 log'ların toplandığını göreceksiniz. Operations management suite portalına girerek, Office 365 Solutions Gallery'ni dashboard'a ekliyoruz.

**Dashboard'umuza eklenen Office 365 solutions'na bağlantı sağlamak için Connectec Sources butonu üzerinden Office 365 butona geliyoruz. Akabinde Connect Office 365 linkine tıklayarak hesabımızın girişini yapıyoruz.**

Giriş yaptığımız office 365 hesabı ile ilgili gerekli bilgileri ve izinleri kabul ederek bağlantımızı gerçekleştiriyoruz.

Office 365 (Preview)

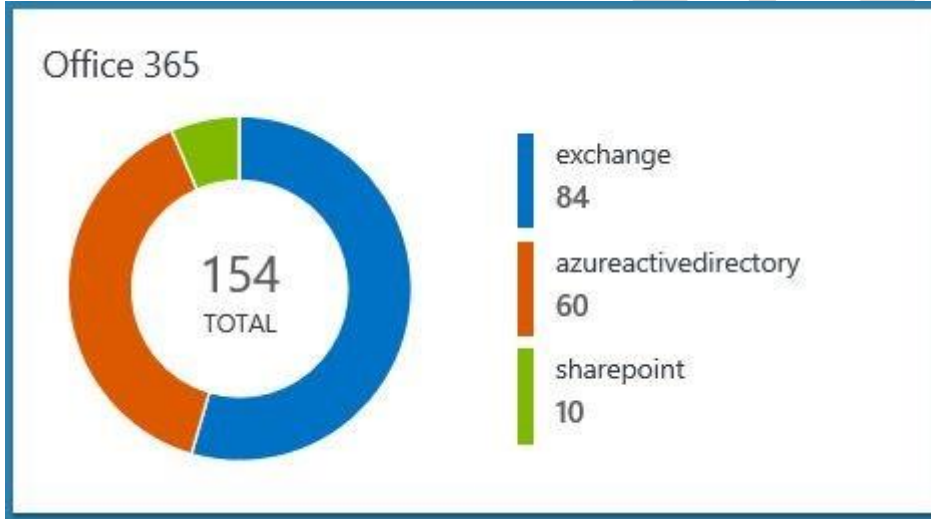
Connect your Office 365 environments.

1 OFFICE 365 SUBSCRIPTION CONNECTED

Connect Office 365

Account	Subscription	Workloads	Status	Remove
support@peakup365.onmic...	d0cef054-10af-4869-aabb-5960b37e...	Azure Active Directory Exchange SharePoint	Active	<a href="#">x</a>

İlgili Account'umuzu eklendiğini görebiliyoruz. Farklı Office 365 Account da ekleyebiliyoruz.



Kısa bir süre içinde ilgili Office 365 Account 'u üzerinde alınan aksiyonları OMS portalında görebilirsiniz.

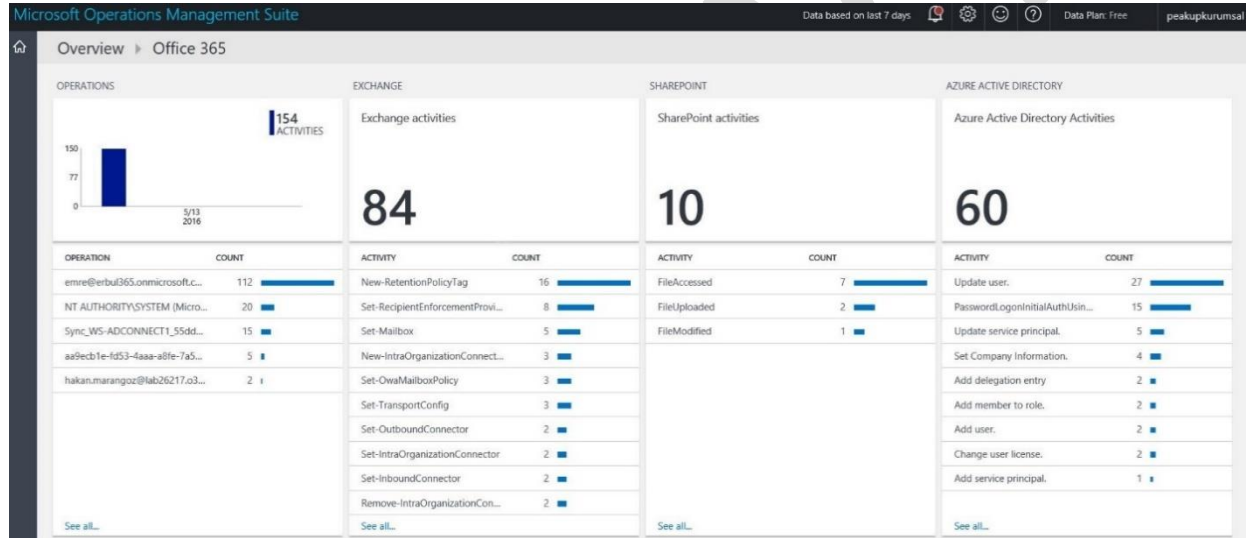
## Office 365 Solutions Gallery altında;

Operations: Tüm izlenen Office 365 hesapları hakkında bilgiler toplar ve analizleri gösterir.

Azure AD: Azure Active Directory ile birlikte kullanıcı oturum açma denemesi veya şifre değişikliği gibi işlemleri görebilirsiniz.

Exchange: Add-Mailbox Permission, Set-Mailbox vs. aksiyonları ve Exchange Server faaliyetlerinin dökümünü gösterir.

SharePoint: Bu bölümde ise Sharepoint belgeleri üzerindeki tüm faaliyetleri gösterir. Herhangi bir dosyaya kim tarafından erişildiği ve hangi ip tarafından bu dosya üzerinde işlem sağlandığını görebilirsiniz. Örneğin, organizasyon veya popüler SharePoint siteleri dışında paylaşılan dosyaları takibini sağlayabilirsiniz.



## Operations Management Suite ile PowerBI Kullanımı

Power BI aslında sizlere her gün kullandığınız Excel ve Office 365 gibi ürünlerinizde veriler ile çalışmanız için yeni ve güçlü bir yol sunuyor. Artık Excel ile daha önce benzerini görmediğiniz şekilde verileri keşfedebilecek, analiz edebilecek, görselleştirebilecek ve bu sayede işiniz için değerli istatistik veriler oluşturabileceksiniz. Office 365 için Power BI ile bulut tabanlı bir BI ortamının dağıtımını kolayca yapabilir ve kullanıcıların her yerden paylaşmasını, ortak çalışabilmelerini ve raporlara erişebilmelerini sağlayabilirsiniz.



Şimdi Operations Management Suite ile PowerBI'nın özelliklerini birleştirerek bulut çözümlerine ne kadar fayda sağladığına şahit olacağız. İlk olarak Azure panelinden Operations Insight servislerinden OMS Portal'ına giriş yapıyoruz.

Microsoft Operations Management Suite

Overview ▶ Settings

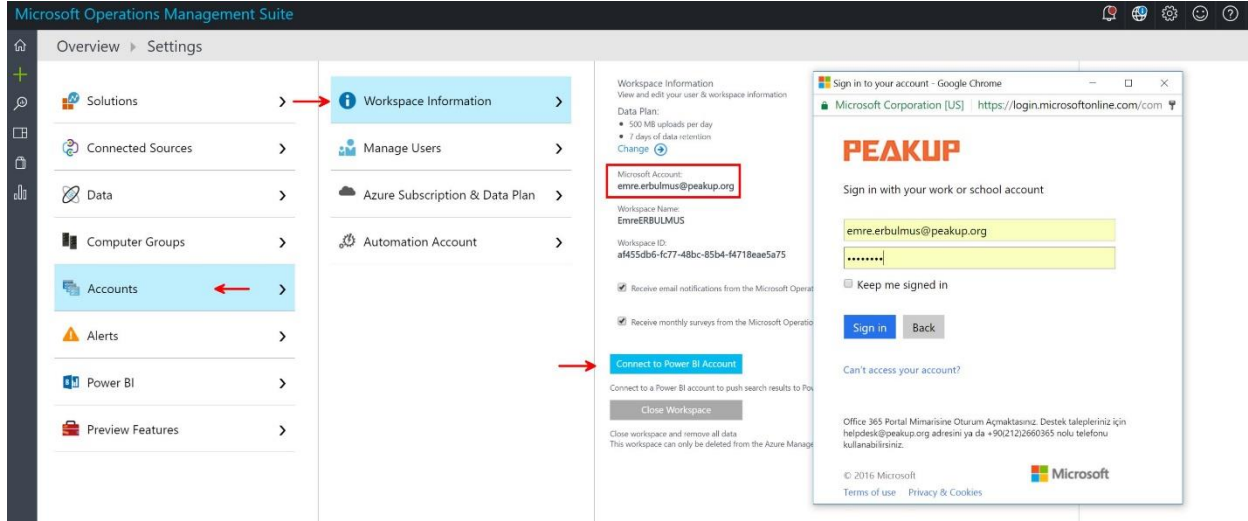
Try out these exciting new features before they are made generally available. Preview features are still works in progress, and we are looking for your feedback to make them even better!

FEATURE NAME	DESCRIPTION	
PowerBI Integration	Configure OMS to periodically push data to PowerBI based on a search query.	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>
Custom Logs	Configure OMS to collect custom text log files from your local environment and create searchable events from them.	<input checked="" type="button" value="Enabled"/> <input type="button" value="Disabled"/>

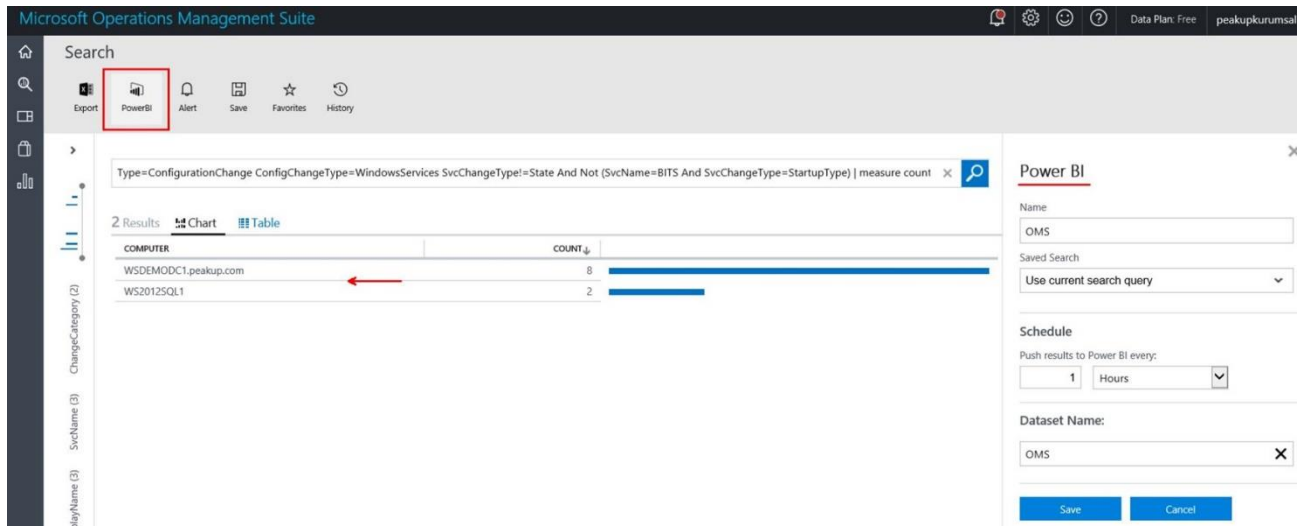
Preview Features

Microsoft OMS Portalına giriş yapıldıktan sonra Settings bölümünden PREVIEW FEATURES link'i altında PowerBI Integration özelliğini Enable diyerek aktif ediyoruz.

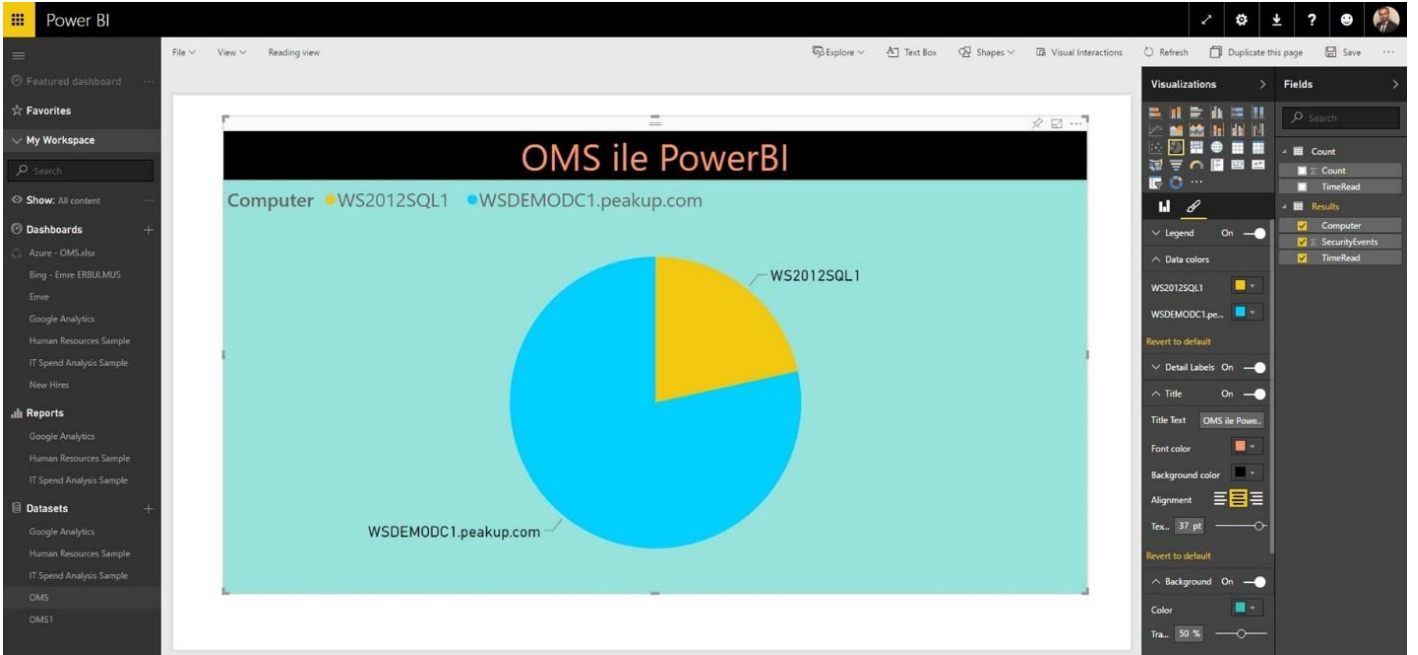




PowerBI özelliğini aktif ettikten sonra ise Settings bölümüne gelerek ACCOUNTS kısmından PowerBI hesap bilgilerimizi doğruluyoruz.



PowerBI hesabımızı doğruladıktan hemen sonra Log Search tabı altında PowerBI simgesini görebiliriz. PowerBI simgesine tıklayarak sol tarafta ilgili PowerBI ekranı açılır. Name ve DataName isimleri girdikten sonra save butonuna basarak ilgili dokümanı PowerBI dashboard'umuza gönderiyoruz. Resimde görüldüğü üzere iki sunucu üzerindeki çalışan Windows Services'lerin âdetini PowerBI ' portalına kaydettik.



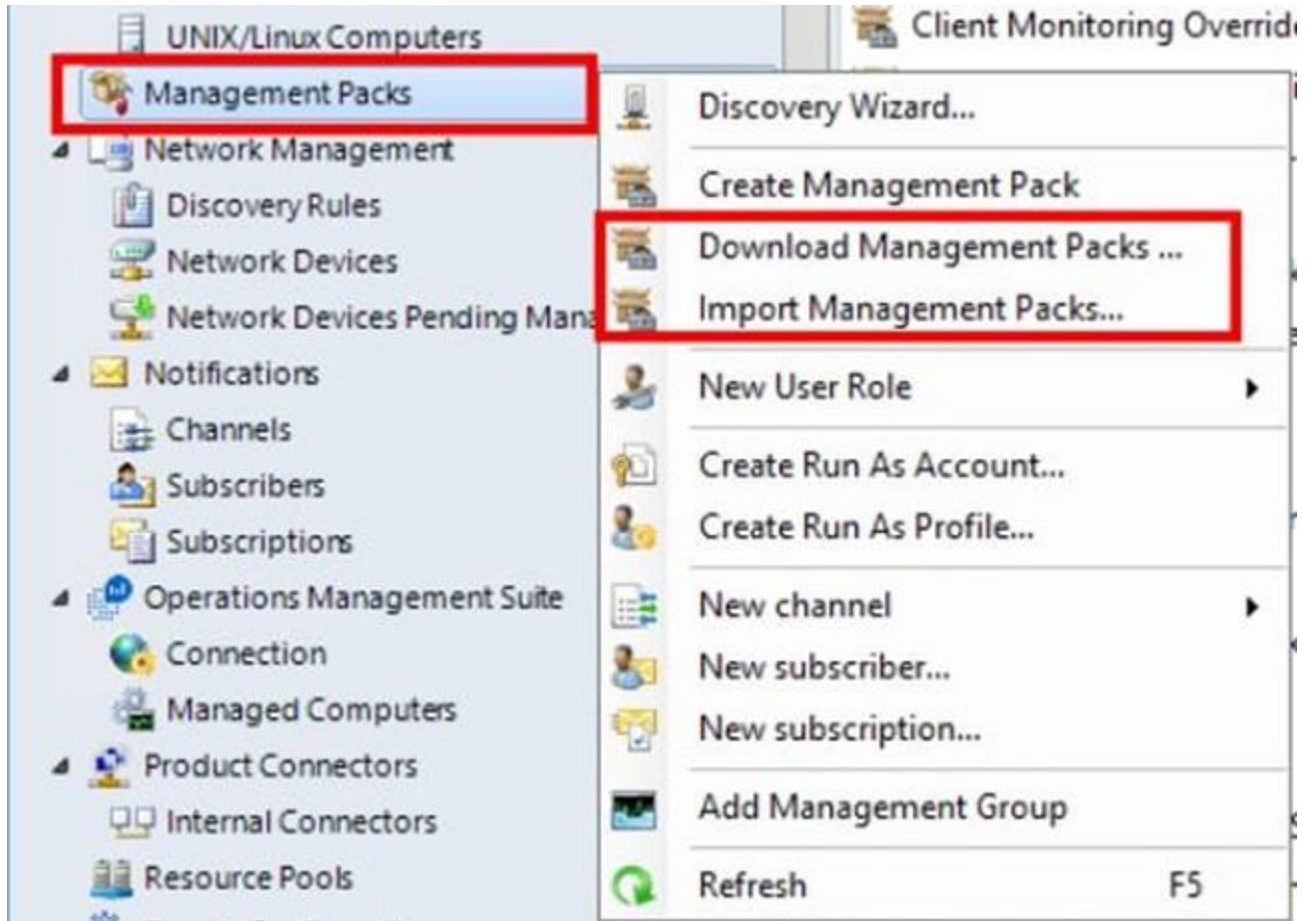
Ardından PowerBI Portalına giriş yaptıktan sonra ise Datasets bölümünden, Operations Management Suite üzerinde kaydettiğimiz oms dokümanı görebiliriz. OMS dokümanına tıklayarak sol taraftaki Fields bölümü açılmaktadır. Biraz aşağı indiğimizde Results tabını göreceksiniz bu tabı genişleterek Computer – SecurityEvents – TimeRead link'lerini işaretliyoruz. Ayrıca Visualizations bölümü üzerinden isteye bağlı grafik şekillerini ve renklerini kullanarak kendi PowerBI raporlamamızı oluşturabiliriz.

Alınan tüm aksiyonlarınızı OMS ve PowerBI sayesinde analiz edip, istatistik veriler oluşturabilirsiniz.

## SCOM ile OMS Nasıl Entegre Edilir

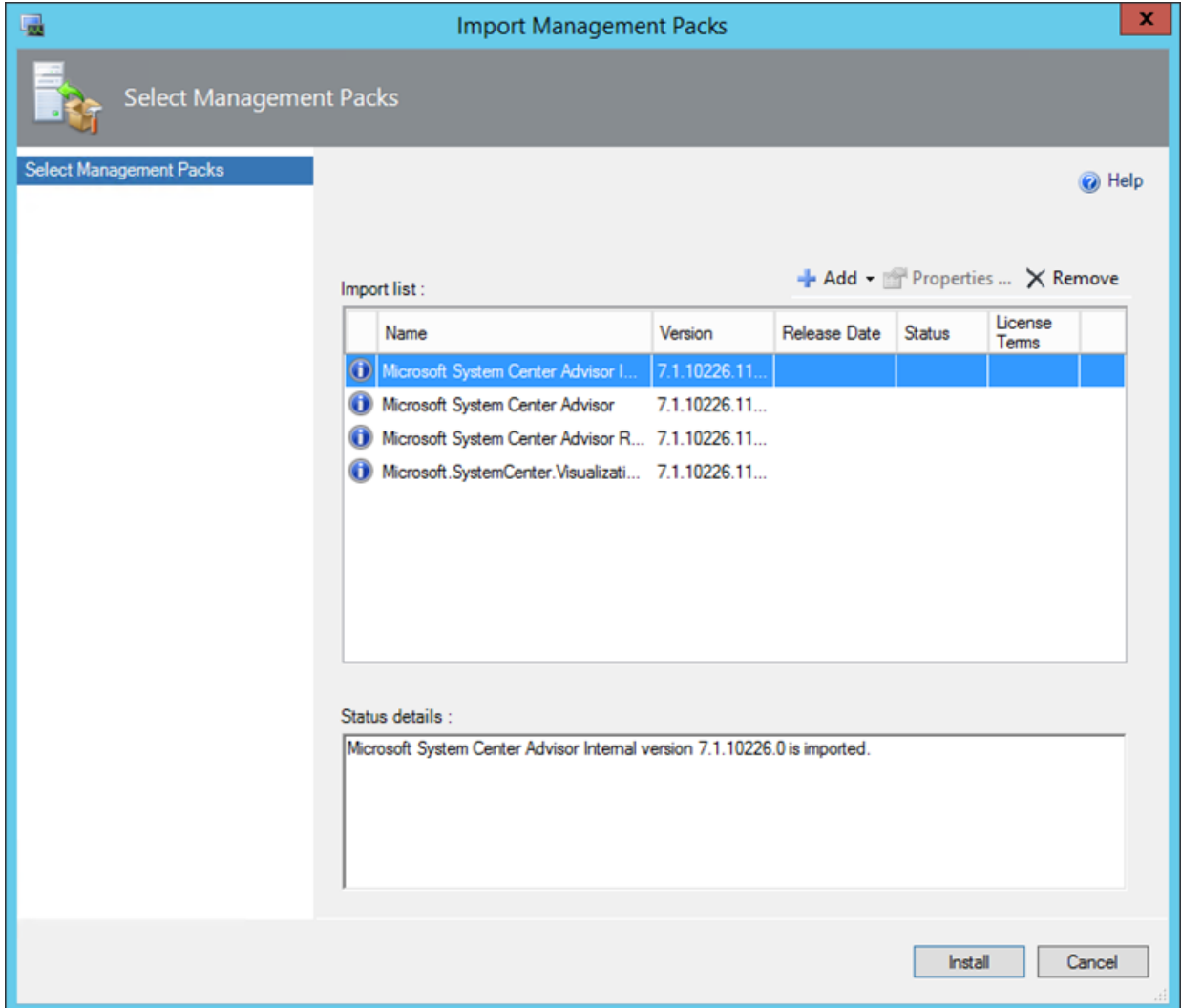
Operations Management Suite makalelerimizde Windows, Linux, Azure, Hyper-V, VMware ve Amazon gibi veri merkezlerinde OMS entegrasyonu **sağlarken** bir agent **yardımı** ile veri **toplayıp** analiz edebiliyorduk, System Center Operations Manager (SCOM) **üzerindeki** verilerinizi ise **doğrudan**, Operations Management Suite ile **ilişkilendirerek** verilerinizi analiz edebilirsiniz.

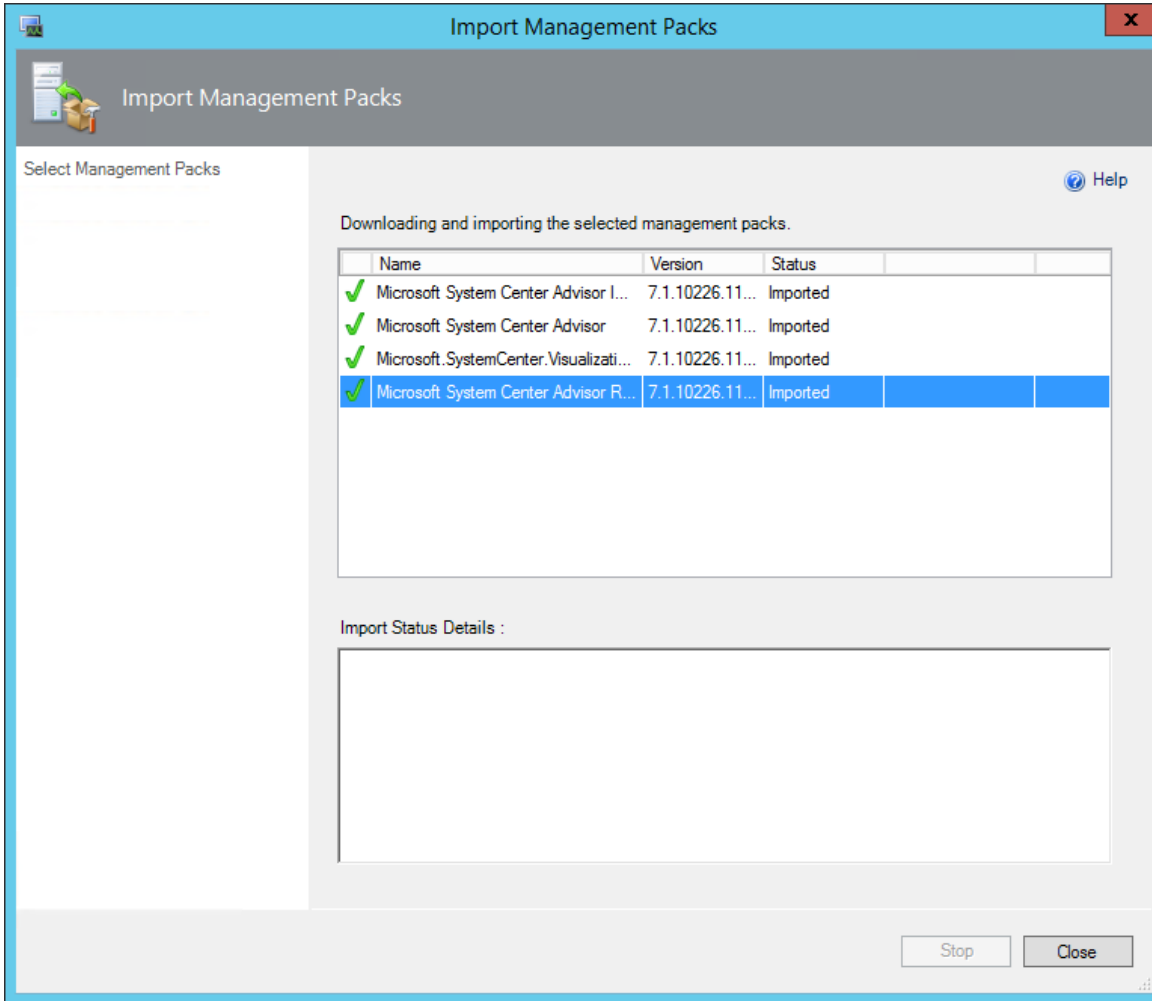
Bu **yazımızda** ise Scom ile Operations Management Suite entegrasyonunu **gerçekleştiriyor olacağız**. İlk olarak local **ortamınızda** bulunan scom **makinamızın** **güncelleştirmeleri** ve rollup **update'lerin** **yapılması** gerekir.



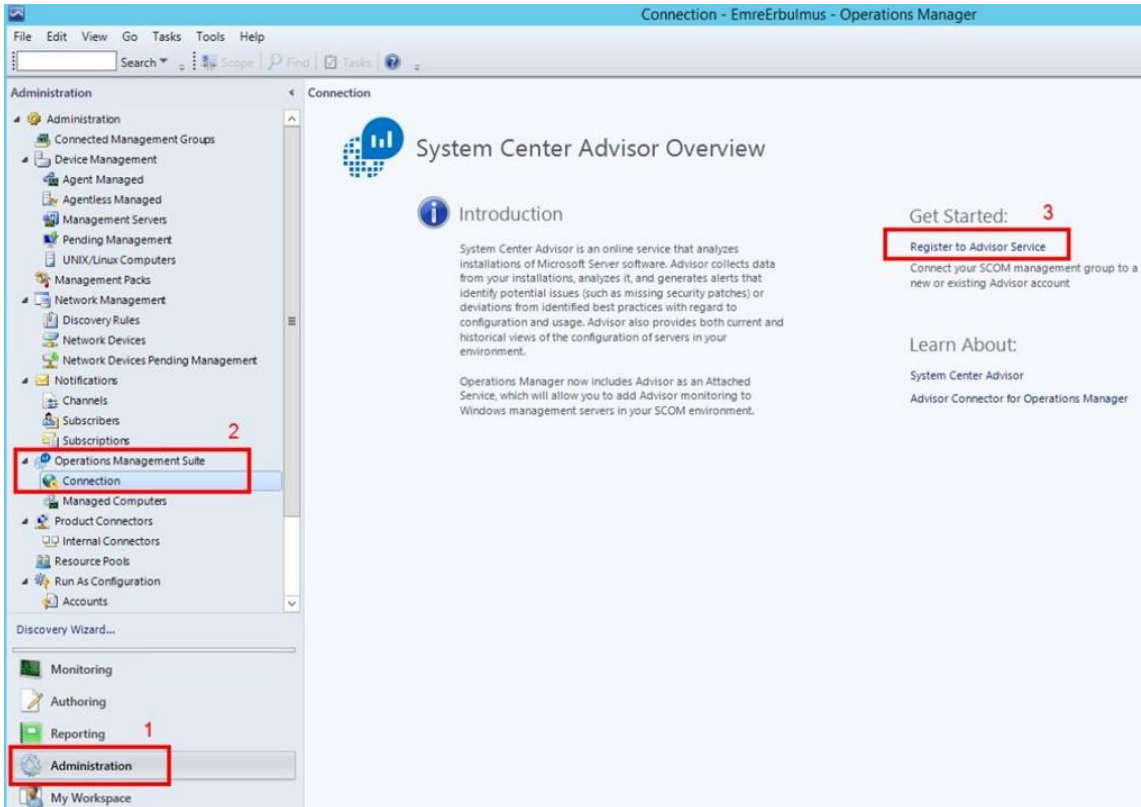
Rollup Update;

1. Operations Manager consolundan Administration **tıklanır**.
2. **Ardından** Administration **altında** Management Pack linkini **göreceksiniz**.
3. Management Pack **sağ** click Import Management Packs **'e tıklanır**.
4. Select Management Packs – Add diyerek **“Program Files\Microsoft System Center\Service Manager 2016\Operations Manager 2016 Management Packs” Klasörüne** indirdiğiniz rollup’ı **gösteriyoruz**.
5. **Yâda** Dwnload Mangement Packs **link’i** ile indirebilirsiniz.

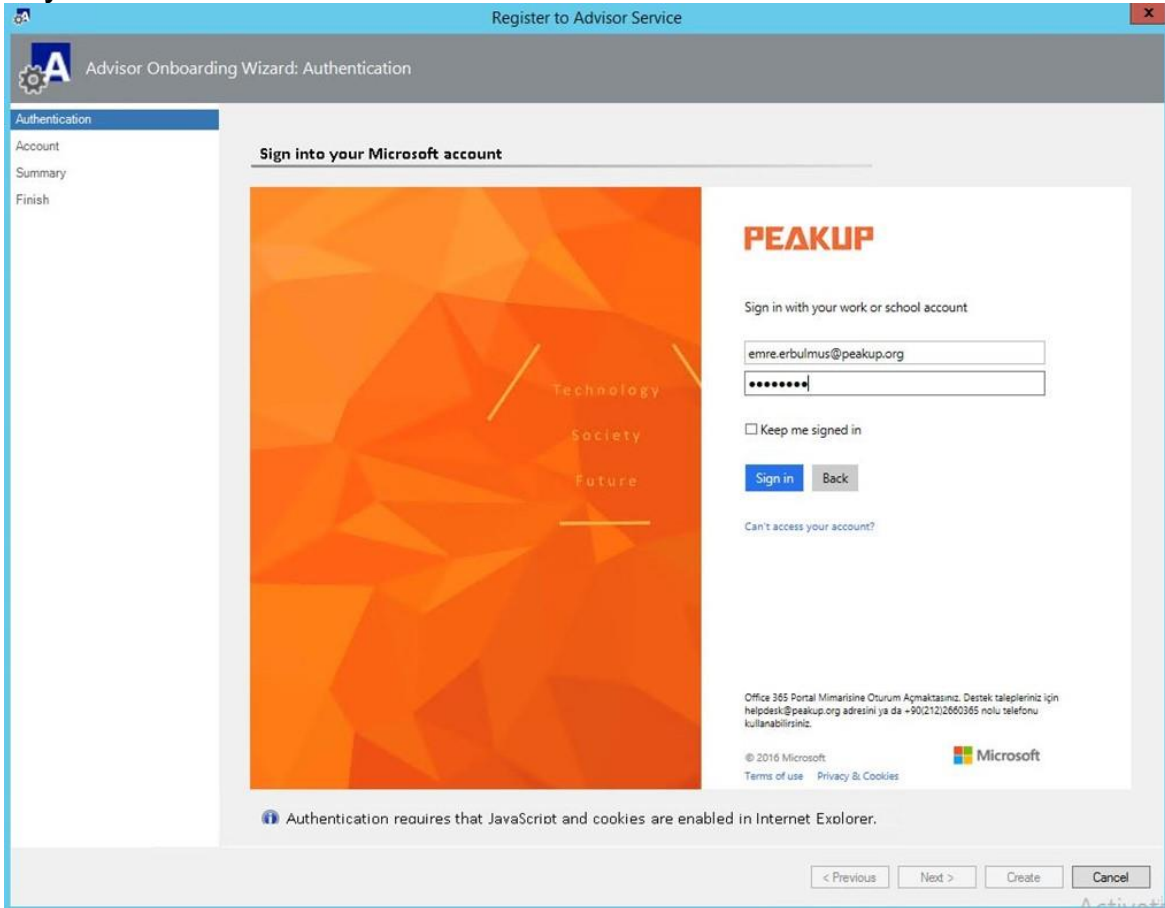




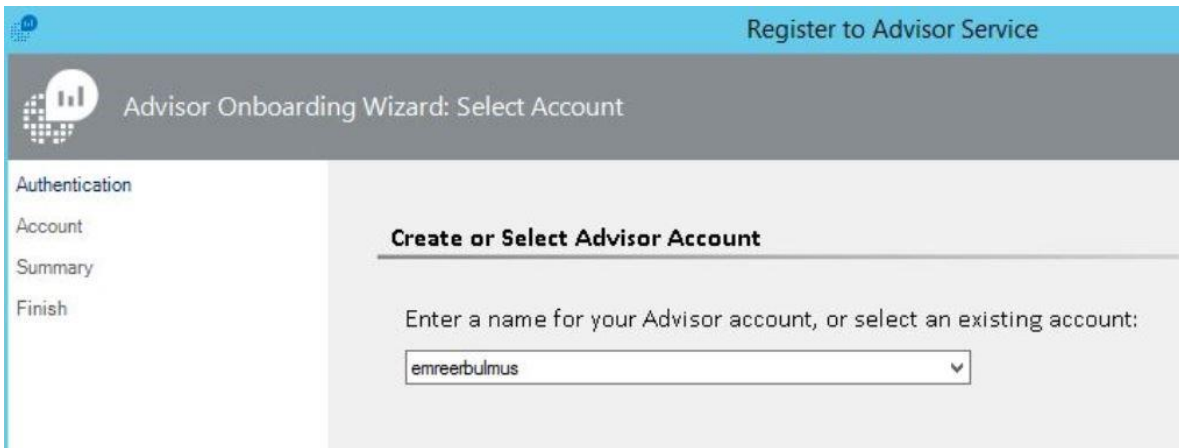
Install butonu ile Rollup'larımı başarılı bir şekilde yüklüyoruz.



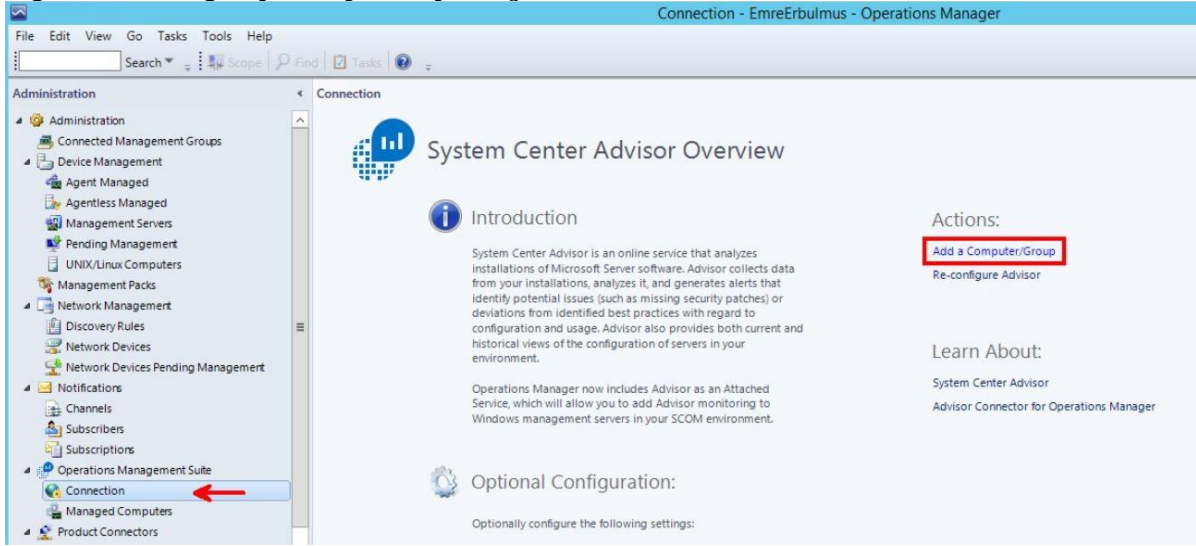
Güncelleştirmelerimizi ve Rollup'larımızı yükledikten sonra sunucumuzu yeniden **başlatıp**, System Center Operation Manager consolunu **açtığımızda**, Administration tabı **altından** Operations Management Suite link'inin eklediğini **göreceksiniz**. Operations Management Suite ile **bağlantı sağlamak için** aynı pencere **üzerinden** Register to Advisor Service link'ine **tıklıyoruz**.



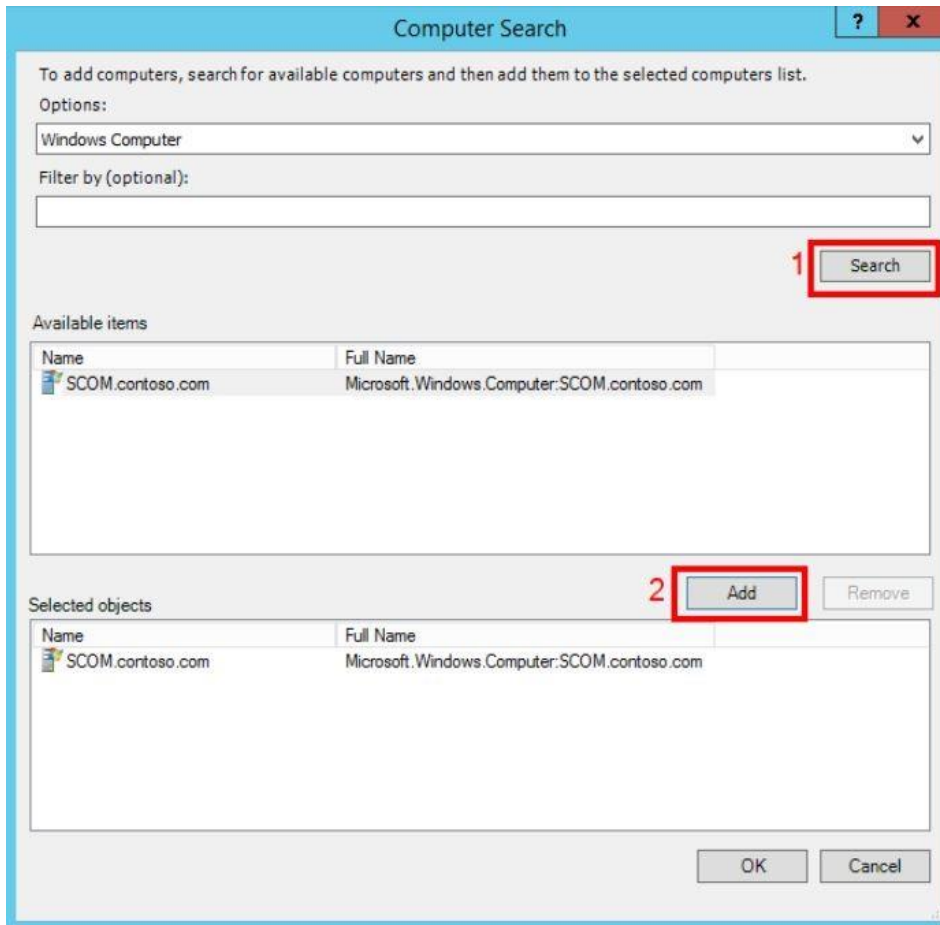
Karşımıza gelen pencerede ise Operations Management Suite kullanıcı adı ve şifremiz ile **giriş yapıyoruz**.



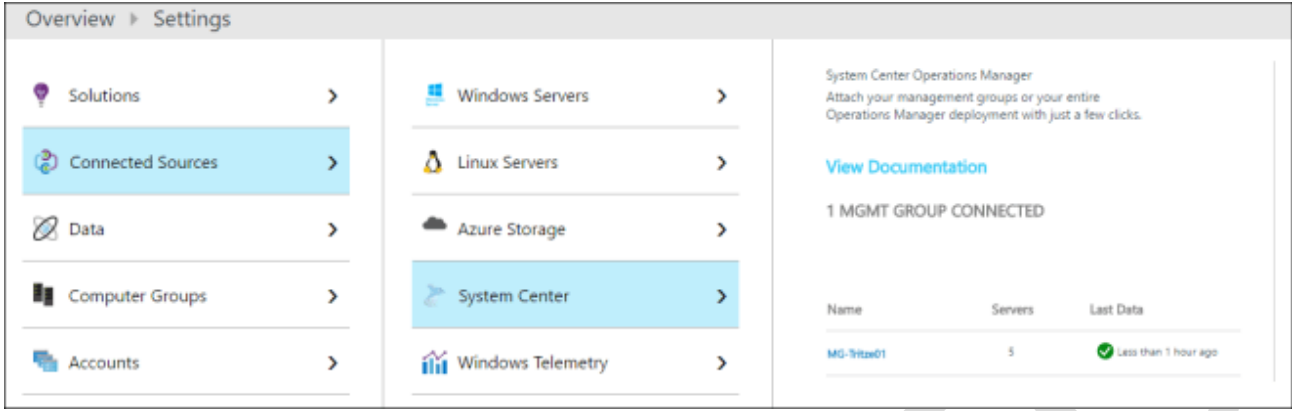
Ardında Varolan Workspace hesabımızı gösteriyoruz. Böylece Scm ile OMS bağlantımızı gerçekleştirmiş oluyoruz.



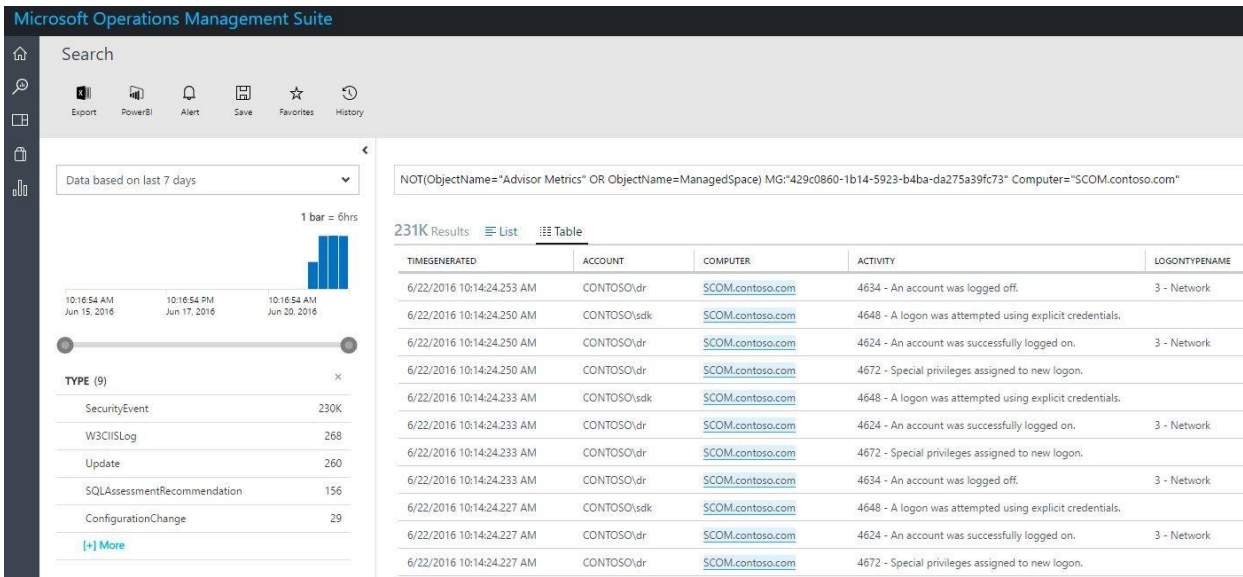
Şuan sadece OMS ile bağlantı sağladık, Fakat Scm makinemizi OMS ile entegrasyonunu tamamlanamadık. Operations Management Suite – Connection link'i üzerinde Add a Computer/Group tıklıyoruz.



Search ederek Scm makinasını bulunup, eklenir.



OMS portal üzerinden Settings - Connected Sources – System Center tablalarını izleyerek sağlıklı bir şekilde bağlandığını görebilirsiniz. Eklenen link'in üzerine tıkladığımızda SCOM tarafında toplanan log'ları OMS dashboard'ına aktarıldığını göreceksiniz.



















Bu sayede System Center Operations Manager **makinamız** ile ilgili **tüm** verilere **kısa süre içinde** sahip olup, gerekli analizleri yapabiliriz.



## Operations Management Suite **lisanslama ve Fiyatlandırma**

Operations Management Suite Insight & Analytics'i seçerken, ücretsiz ve tek başına Log Analytics veya OMS Insight & Analytics arasında seçimler yapılabilir.

F Free	S Standalone	O OMS
 500MB Daily upload limit	 Unlimited Daily upload limit	 Insight + Analytics
 7 Days Data Retention	 31 days Data Retention	 Automation + Control
 90 days Activity Log	 90 days Activity Log	 Security + Compliance
 500 min/month Runbooks	 10+ Management solutions	 Unlimited Daily upload limit
	 Unlimited Azure metrics	 31 days Data Retention
	 Unlimited Azure diagnostics logs	 Unlimited min Runbooks
<b>0.00</b> (USD)	<b>2.30</b> COST PER 1GB (USD)	<b>10.00</b> STARTING COST PER NODE (USD)

OMS lisanslama modelleri 3 ana başlıkta inceleyebilirsiniz.

- ✓ F (Free) model: Ücretsiz, günde toplam 500 MB dolaşım sağlar ve 7 gün süreyle saklama (yalnızca Log Analytics için) sunar.
- ✓ S (Standalone) model: 30 günlük saklama ile GB başına 2,30 \$ 'lık sınırsız alım sağlar (yalnızca Log Analytics için). Azure Monitor entegrasyonu ile Azure etkinlik günlüklerine, ölçümlerine ve log günlüklerine 90 günlük erişim sağlanabilir.
- ✓ (OMS) model: OMS'in sunmuş olduğu E1 – E2 aboneliklerin hepsini kapsamaktadır. Bunu seçerseniz, lisanslama yoluyla Log Analytics, Application Dependency Monitor ve Network Performance Monitor gibi OMS'nin bir parçası olarak hizmetleri kullanabilirsiniz.

- **Operations Management Suite aboneliği**

Operations Management Suite iki abonelik seçeneği sunar, Bunlar Operations Management Suite E1 ve Operations Management Suite E2 abonelikleridir.

	E2	E1
Insight and Analytics	●	●
Automation and Control	●	●
Security and Compliance	●	
Backup	●	
Site Recovery	●	
System Center: Configuration Manager, Operations Manager, Orchestrator, Data Protection Manager, Virtual Machine Manager, Service Manager	●	●
<b>Tahmini Perakende Fiyatı:</b>	<b>Düğüm başına ayda 106,75 TL*</b>	<b>Düğüm başına ayda 61,00 TL*</b>

\*Yıllık taahhülle sanal makine başına aylık tahmini perakende fiyatı. Fiyatlar TRY cinsindedir ve ülkeye göre değişebilir. Fiyat teklifi almak için lütfen iş ortağınız veya Microsoft temsilciniz ile iletişime geçin.

Her iki seçenek de Operations Management Suite çözümlerindeki önemli teknolojilere erişimin yanı sıra System Center yazılımlarını kullanma hakları içerdiğinden hibrit ortamlarınız için eksiksiz bir çözüm sağlar. Operations Management Suite abonelikleri, yıllık bir taahhülle node başına aylık olarak fiyatlandırılır.

## • Çözümüne göre Operations Management Suite fiyatlandırması

Solutions	Features	Price
Insight & Analytics	<ul style="list-style-type: none"><li>Gain visibility across workloads, giving customers all the information needed on what's happening in the environment</li><li>Includes log collection and search, application and server dependency mapping, as well as network health monitoring</li><li>Rights to use System Center Operations Manager</li></ul>	\$15/node*
Automation & Control	<ul style="list-style-type: none"><li>Enable consistent control and compliance across environments for both Azure, 3rd-party clouds and on-premises datacenters</li><li>Includes services to assist with process automation, desired state configuration, change tracking and update management</li><li>Rights to use System Center Service Manager, System Center Orchestrator, and System Center Configuration Manager</li></ul>	\$10/node*
Security & Compliance	<ul style="list-style-type: none"><li>Drive security across every area of the organization, delivering sophisticated threat intelligence capabilities, malware detection, and information on how systems may have been compromised</li><li>Includes advanced security and audit functionality and malware threat analysis</li><li>Azure Security Center availability for deep security management of Azure services</li></ul>	\$15/node*
Protection & Recovery	<ul style="list-style-type: none"><li>Ensure availability of important applications and data. Protection and Recovery helps you keep critical data protected through integrated cloud backup, and applications available, while minimizing the impact of disruptions to the business</li><li>Includes both backup and site recovery services for an integrated experience</li><li>Rights to use System Center Virtual Machine Manager and System Center Data Protection Manager</li></ul>	\$30/node*

### Insight and Analytics

- Müşterinin farklı iş yüklerine görsellik ekleyerek, ortamlarında olup biten tüm bilgileri gözlemleyebilirsiniz.
- Log toplama, arama, uygulama ve sunucu bağımlılığının yanı sıra network durumunu da inceleyebilirsiniz.
- Ayrıca System Center Operations Manager kullanma hakkı sunar.

### Automation & Control (Otomasyon ve Denetim)

- Azure, Cloud ve kurum içi veri merkezleri için ortamlar arası tutarlı denetim ve uyumluluk sağlar.
- Otomasyon, istenen durum yapılandırması, farklı izleme ve güncelleştirme yönetimi konusunda yardımcı olan hizmetler içerir.
- System Center Service Manager, System Center Orchestrator ve System Center Configuration Manager kullanma hakları sunar.

### Security and Compliance (Güvenlik ve Uyumluluk)

- Şirketin her daim güvenliğini artırarak olabilecek tehditleri ve sistemlerin gizliliğinin nasıl tehlikeye girebileceği konusunda bilgi sahibi olabilirsiniz.
- İleri düzey güvenlik ve denetim işlevselliğinin yanı sıra malware tehdit analizi içerir.
- Azure hizmetlerine yönelik derin güvenlik yönetimi sunulmaktadır. (Azure Security Center)

## Protection and Disaster Recovery ( **Koruma ve Olağanüstü Durum Kurtarma** )

- **Önemli uygulamaların ve verilerin erişilebilir olması gerekir.** Protection and Recovery, önemli verilerinizi Azure Backup Vault aracılığıyla güvenli tutmanıza, uygulamalarınızın her daima kullanılabilir olmasını sağlamanıza ve iş kesintilerinin etkisini olabildiğince azaltmanıza yardımcı olur.
- **Güvenlik için** hem yedekleme hem de site kurtarma hizmetleri içerir.
- System Center Virtual Machine Manager ve System Center Data Protection Manager kullanma hakları sunar.
- Microsoft Operations Management Suite **Hesaplaması**

### Microsoft Operations Management Suite Calculator

#### Estimated Pricing

Based on your inputs, the breakdown of estimated costs is below. You can adjust your inputs at the top of this page by clicking any of the boxes. This will recalculate costs in real time.

[Click to review assumptions ?](#)

Number of Nodes	<input type="text" value="6"/>	System Center	<input type="text" value="No"/>
<small>from 1 to 1,000,000</small>			
Insight & Analytics	<input checked="" type="checkbox"/>	Automation & Control	<input type="checkbox"/>
Security & Compliance	<input type="checkbox"/>	Backup	<input checked="" type="checkbox"/>
Site Recovery	<input type="checkbox"/>		

Pay As You Go		
Insight & Analytics	\$15.00 per node/month	\$180.00 Annually
Backup	\$10.00 per node/month	\$120.00 Annually
	<b>\$25.00</b> Total price per node, per month	<b>\$300.00</b> Total annual price per node

To maximize flexibility, enterprise customers can purchase OMS services separately or through an annual commitment. Customers who choose to purchase services through an annual commitment have rights to the corresponding System Center 2016 components.

OMS Subscription Suite - E2		
Insight & Analytics		<input checked="" type="checkbox"/>
Automation & Control		<input checked="" type="checkbox"/>
Security & Compliance		<input checked="" type="checkbox"/>
Backup		<input checked="" type="checkbox"/>
Site Recovery		<input checked="" type="checkbox"/>
	<b>\$35.00</b> Total price per node, per month	<b>\$420.00</b> Total annual price per node

Microsoft OMS Calculator ile oms sunduğu paketleri çok daha kolay ve pratik bir şekilde hesaplayabilirsiniz. [Buradan](#) online olarak hesaplama yapabilirsiniz. Yukarıdaki resimde görüldüğü üzere, sunucu sayınızı, System Center ürünü ile birlikte kullanıp, kullanmayacağınızı ve son olarak ortamınız için kullanacağınız paketleri işaretleyerek gerçek zamanlı bir hesaplama yapabilirsiniz. OMS abonelikleri, hibrid bulut ortamlarına komple bir çözüm sağlamak için System Center bileşenleri için haklar içerir.



## Additional Expenses

Based on typical industry usage, we've chosen LRS blob storage for Backup, and GRS for Site Recovery. If you require alternative storage configurations, please reference the expandable pricing details table below.

Storage costs per year			Total annual storage commit
Azure Backup	LRS	\$864.00	\$2,592.00
Azure Site Recovery	GRS	\$1,728.00	

**Yıllık Maliyet Karşılaştırmaları** ve Ek harcamalar gibi raporlar sunulmaktadır. Microsoft Operations Management Suite ile anlatacaklarım şimdilik bu kadar. Ben araştırmaktan ve yazmaktan çok keyif aldım, umarım sizde incelerken keyif alırsınız.

Teşekkürler.