System Center Monitoring Pack - Endpoint Protection Linux Sürümü

Microsoft Corporation

Yayımlanma tarihi: 10/26/2015

Bu belge ile ilgili geribildirim veya önerilerinizi mpgfeed@microsoft.com adresine gönderin. Lütfen geri bildiriminizle birlikte yönetim paketi kılavuzunun adını da belirtin.

Operations Manager ekibi, Management Pack Catalog (Management Pack Kataloğu) (http://go.microsoft.com/fwlink/?LinkID=82105) adresinde bulunan yönetim paketi sayfasında bir inceleme sağlayarak izleme paketi ile ilgili geri bildirim sağlamanız için sizi teşvik eder.

İçindekiler

SCEP Management Pack Kılavuzu

Bu yönetim paketi, System Center 2012 Operations Manager içindeki System Center Endpoint Protection (SCEP) ürününü iş istasyonları ve sunucular dahil olmak üzere bir ağ ortamında merkezi bir konumdan yönetmenize olanak tanır. Operations Manager görev yönetim sistemi ile; SCEP'i uzak bilgisayarlarda yönetebilir, uyarıları ve sistem durumlarını görüntüleyebilir ve yeni sorunlarla tehditlere hızlı bir şekilde yanıt verebilirsiniz.

System Center 2012 Operations Manager kötü amaçlı koda karşı başka hiçbir koruma biçimi sağlamaz. System Center 2012 Operations Manager Linux işletim sisteminin yüklü olduğu bilgisayarlarda SCEP çözümünün varlığına bağlıdır.

Bu kılavuz, SCEP için Management Pack'in 4.5.10.1 sürümü temel alınarak yazılmıştır.

Kılavuz Geçmişi

Sürüm	Sürüm Tarihi	Değişiklikler
4.5.9.1	05/16/2012	Bu kılavuzun orijinal sürüm tarihi.
4.5.10.1	11/06/2012	Yeni Linux dağıtımları desteklenmektedir. Bazı yönetim paketi araçları için daha iyi açıklamalar bulunmaktadır.

4.5.10.1 Sürümündeki Değişiklikler

System Center Endpoint Protection için yönetim paketinin 4.5.10.1 sürümü şu değişiklikleri içerir:

- Yeni Linux dağıtımları desteklenmektedir:
  - Red Hat Enterprise Linux Server 5
  - SUSE Linux Enterprise 10
  - CentOS 5, 6
  - Debian Linux 5, 6
  - Ubuntu Linux 10.04, 12.04
  - Oracle Linux 5, 6

  Not: Bu yeni dağıtımlar yalnızca System Center 2012 Operations Manager Service Pack 1 ve üstü kullanıldığında desteklenir.
- Aşağıdakiler için daha iyi açıklamalar eklenmiştir:
  - Etkin Kötü Amaçlı Yazılım izleyicisi
  - Etkin Kötü Amaçlı Yazılım (Kuraldan) uyarısı

Desteklenen Yapılandırmalar

Genel olarak, desteklenen yapılandırmalar Operations Manager 2007 R2 Supported Configurations (Operations Manager 2007 R2 Desteklenen Yapılandırmalar) (http://go.microsoft.com/fwlink/?LinkId=90676) içinde özetlenir.

Bu yönetim paketi, System Center 2012 Operations Manager 2007 R2 veya sonraki sürümünü gerektirir. Aşağıdaki tablo bu yönetim paketi için desteklenen işletim sistemleri ayrıntılarını vermektedir:

İşletim Sistemi Adı	x86	x64
Red Hat Enterprise Linux Server 5, 6	Evet	Evet
SUSE Linux Enterprise 10, 11	Evet	Evet
CentOS 5, 6	Evet	Evet
Debian Linux 5, 6	Evet	Evet
Ubuntu Linux 10.04, 12.04	Evet	Evet
Oracle Linux 5, 6	Evet	Evet

Ön Koşullar

Bu yönetim paketinin çalıştırılması için aşağıdaki gereksinimlerin karşılanması gerekir:

- System Center Operations Manager 2007 R2 Cumulative Update 5
  (http://support.microsoft.com/kb/2449679)

Aşağıda listelenen SCEP için yönetim paketleri System Center 2012 Operations Manager 2007 R2 ile tümleştirilmiştir veya çevrimiçi katalogdan indirilebilir.

Kimlik	Ad	Sürüm
Microsoft.Linux.Library	Linux İşletim Sistemi Kitaplığı	6.1.7000.256

Microsoft.SystemCenter.InstanceGroup.Library	Örnek Grubu Kitaplığı	6.1.7221.0
Microsoft.SystemCenter.Library	System Center Çekirdek Kitaplığı	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	WS-Management Kitaplığı	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Data Warehouse Kitaplığı	6.1.7221.0
Microsoft.Unix.Library	Unix Çekirdek Kitaplığı	6.1.7000.256
Microsoft.Unix.Service.Library	Unix Hizmeti Şablon Kitaplığı	6.1.7221.0
Microsoft.Windows.Library	Windows Çekirdek Kitaplığı	6.1.7221.0
System.Health.Library	Sistem Durumu Kitaplığı	6.1.7221.0
System.Library	Sistem Kitaplığı	6.1.7221.0

Önemli: Linux SCEP ürününün System Center 2012 Operations Manager kullanımıyla izlenmesi işleminin düzgün çalışması için öncelikle yapılandırma dosyasında */etc/opt/microsoft/scep/scep.cfg* veya SCEP Web arabirimi aracılığıyla etkinleştirilmesi gerekir. Lütfen yukarıda söz edilen yapılandırma dosyasındaki 'scom_enabled' parametresinin *'scom_enabled = yes'* olarak ayarlandığından emin olun veya **Yapılandırma** > **Genel** > **Daemon seçenekleri** > **SCOM etkin** altındaki Web arabiriminde bulunan uygun ayarı değiştirin.

Bu Management Pack'teki Dosyalar

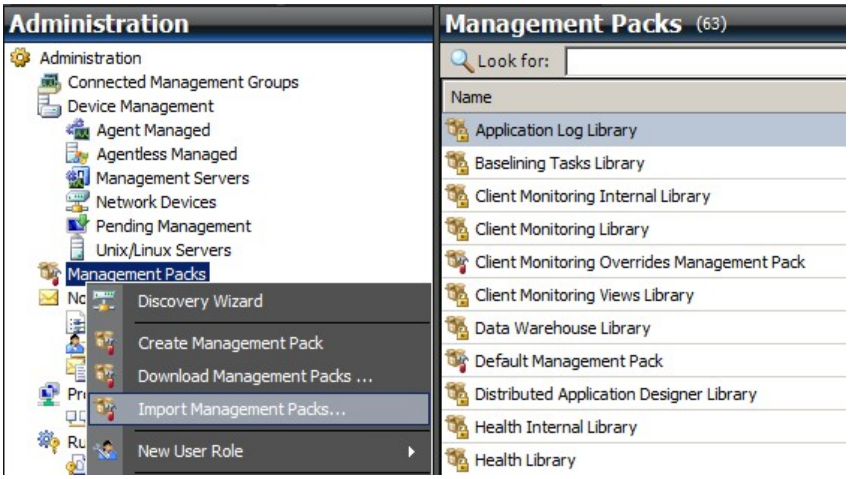
SCEP için Management Pack şu dosyaları içerir:

Dosya adı	Tanım
Microsoft.SCEP.Linux.Library.mp	Sınıf tanımları ile bunların karşılıklı ilişkilerinin yanı sıra izleyici türleri ile modül türleri tanımlarını da içerir.
Microsoft.SCEP.Linux.Application.mp	İzleme ve uyarı ile görevler ve görünümleri uygular.

Hızlı Başlangıç

SCEP'yi izlemeye başlamak için ön koşul, yönetim paketlerinin Operations Manager içine alınması ve izlenecek olan bilgisayarların tanımlanmasıdır ("keşif" olarak anılan işlem).

Yönetim paketlerini alma

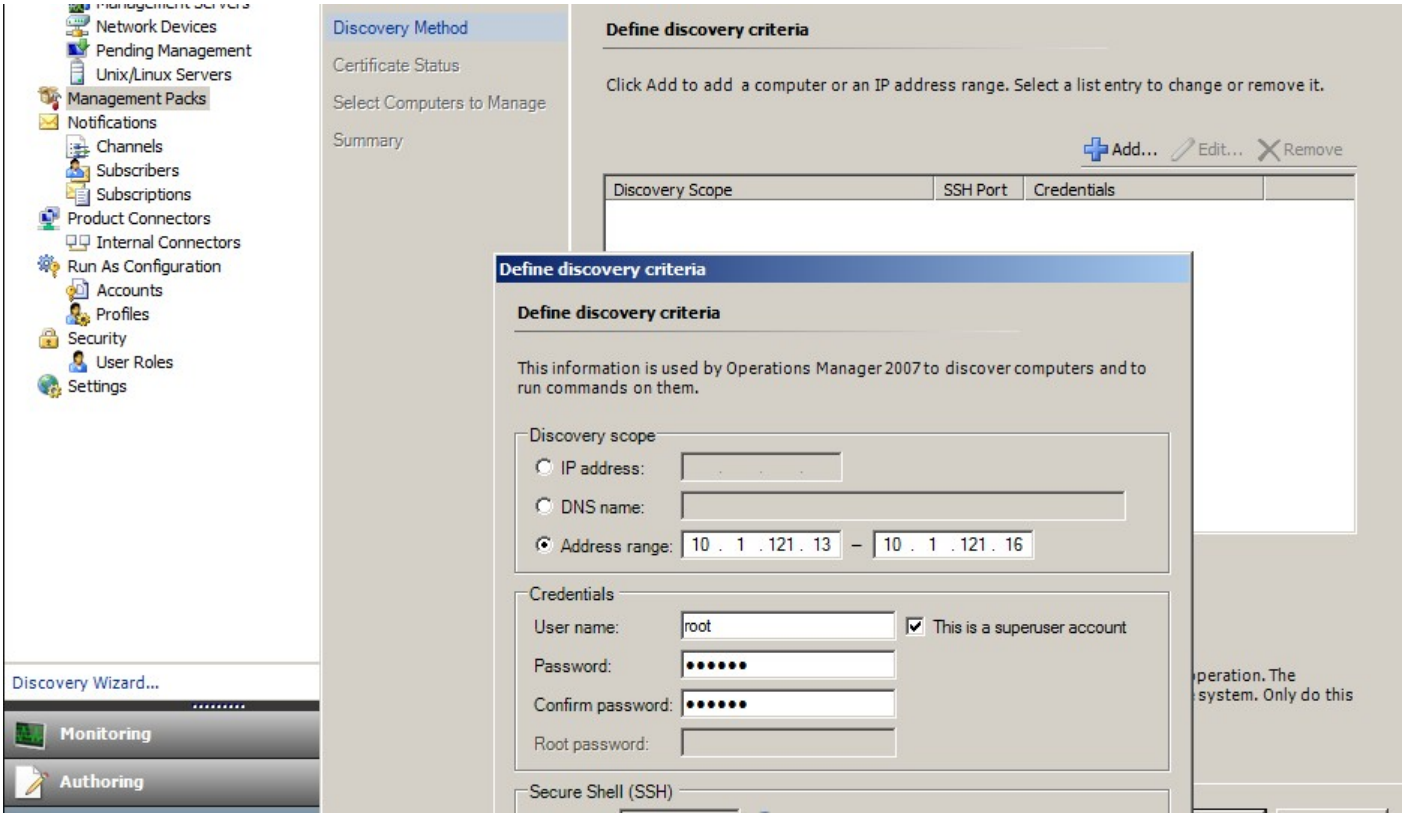


1. İşlem Konsolu penceresinin sol bölmesindeki **Administration** çalışma alanını tıklatın.
2. **Management Packs** öğesini sağ tıklatın ve içerik menüsünde **Import Management Packs...** seçeneğini belirleyin.
3. Management Packs penceresinde **Add** düğmesini tıklatın ve açılır menüden **Add from disk...** seçeneğini belirleyin.
4. Operations Manager uygulamasının yerel diskte bulunmayan bağımlılıkları da aramasını ve yüklemesini istediğinizi şu şekilde onaylayın: **Online Catalog Connection** açılır penceresinde **Yes** seçeneğini tıklatın.
5. Listelenen her iki dosyanın da seçili olduğundan emin olun (Microsoft.SCEP.Linux.Application.mp, Microsoft.SCEP.Linux.Library.mp) ve **Install** öğesini tıklatın.

Not: Yönetim paketini alma ile ilgili daha fazla talimat için bkz. How to Import a Management Pack in Operations Manager 2007 (Operations Manager 2007'de Management Pack'i Alma) (http://go.microsoft.com/fwlink/?LinkId=142351).

Keşif

*.mp dosyaları başarıyla alındıktan sonra bilgisayar keşfini gerçekleştirmeniz gerekir.



1. **Administration** çalışma alanında (İşlem Konsolu penceresinin sol bölmesinde) **Discovery wizard...** bağlantısını (sol bölmenin altında) tıklatın.
2. Bilgisayar ve Aygıt Yönetimi Sihirbazı'nda **Unix/Linux computers** seçeneğini belirleyin ve devam etmek için **Next** öğesini tıklatın.
3. Keşif ölçütlerini tanımla bölümü içinde **Add** düğmesini tıklatın.
4. System Center 2012 Operations Manager uygulamasının aracısını yükleyeceği taranacak bir IP **Address range** ve bilgisayarlara uygulanabilen SSH **Credentials** belirleyin.
5. **OK** öğesini tıklayarak kapsam ve kimlik bilgileri ölçütlerinizi doğrulayın ve keşif işlemini başlatmak için **Discover** düğmesini tıklatın.
6. Tamamlanmanın ardından, izleme/yönetim sistemlerini belirlemenize olanak tanıyan bir liste görüntülenir.

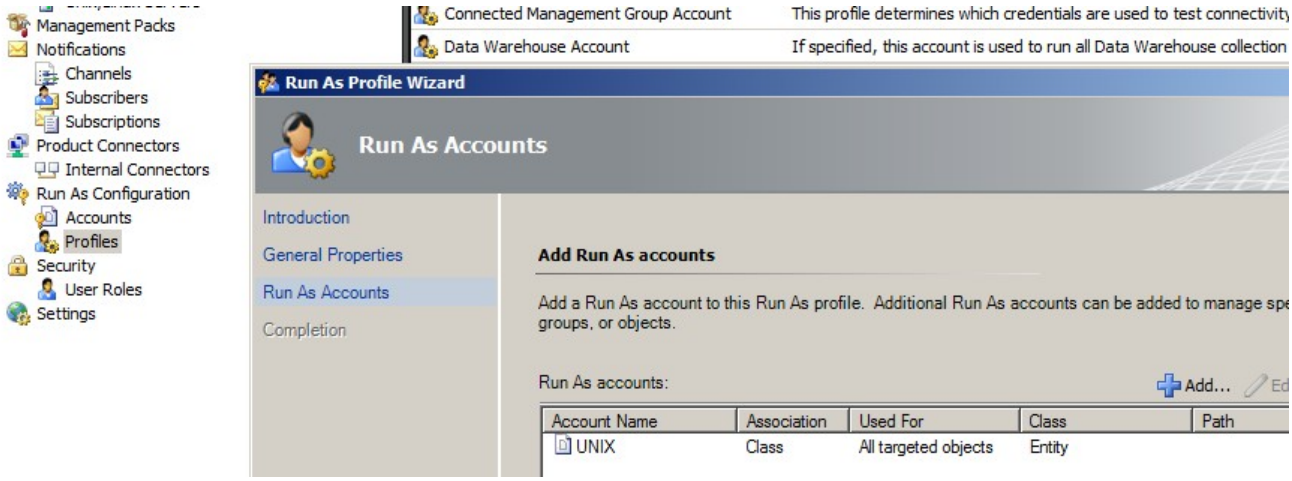
Not: Linux Aracısı'nın yüklenmesi aşağıdaki Linux Dağıtımları tarafından desteklenir. Linux Aracısı, Keşif kullanımıyla yüklenemiyorsa, lütfen Manually Installing Cross Platform Agents (Çapraz Platform Aracılarını El İle Yükleme) (http://technet.microsoft.com/en-us/library/dd789016.aspx) Microsoft makalesindeki el ile yükleme talimatlarına bakın.

Not: SCEP yüklemesine sahip Linux sunucularının keşfi, Operations Manager ile yönetilen tüm Linux Bilgisayarlarda 8 saat aralıklarla otomatik olarak çalışır (yani sistem dağıtımları için bilgisayarlarında uygun Linux yönetim paketi yüklüdür). Keşif, tüm hizmet modülü varlıklarını oluşturur: Korumalı Linux Sunucusu ve iç içe geçmiş varlıklar veya Korunmayan Linux sunucusu (uygun bölümlerde bulunabilir). "scep_daemon" hizmeti varsa (durdurulmuş veya çalışır durumda) SCEP'in tamamen yüklendiği kabul edilebilir. Bu nedenle keşif döngüsü ile ilgili olarak ilk keşif, yönetim paketi yüklenirken ortaya çıkar ancak sonraki keşif 8 saat içinde gerçekleşir. SCEP ürünü kaldırılmışsa, ilgili sunucu otomatik olarak Korunmayan'a (SCEP'i olmayan Sunucular) taşınır. Bunun tersi de geçerlidir.

Farklı Çalıştırma Hesapları yapılandırması

Unix hesabı oluşturmak için lütfen aşağıdaki talimatları uygulayın:

1. **Administration** çalışma alanında (sol bölme) **Run As Configuration** > **Accounts** seçeneğine gidin.
2. Yeni bir hesap oluşturmak için **Eylemler** bölmesindeki (sağ bölme) **Actions** bölümünü açın ve **Farklı Çalıştırma Hesabı Oluştur...** öğesini tıklatın.
3. Genel Özellikler penceresinde, **Run As Account type** açılır menüsünden **Basic Authentication** seçeneğini belirleyin.
4. Hesap oluşturduktan sonra dağıtımın ortaya çıkması için yeni hesabı bir profile eklemeniz gerekir. Bunu yapmak için **Run As Configuration** > **Profiles** altındaki **Unix Privileged Account** profilini tıklatın, **Properties** seçeneğini belirleyin ve yeni oluşturulan hesabı ataması için sihirbazı tamamlayın.



Not: Farklı Çalıştırma Hesabı oluşturma ile ilgili daha fazla bilgi için System Center 2012 Operations Manager 2007 R2 çevrimiçi kitaplığındaki Configuring a Cross Platform Run As Account (Çapraz Platform Farklı Çalıştırma Hesabı Yapılandırma) (http://go.microsoft.com/fwlink/?LinkId=160348) konusuna bakın.

Yukarıda söz edilen adımların hepsi tamamlandıktan sonra, yeni keşfedilen Linux sunucuları **Monitoring** > **System Center Endpoint Protection Linux** > **SCEP'ye Sahip Sunucular** altında kısa bir süre içinde (birkaç dakika içinde) kullanılabilir duruma gelir.

SCEP için Dil paketi yükleme

Dil paketinin biçimi şu şekildedir:
Microsoft.SCEP.Linux.Application.LNG.mp ve Microsoft.SCEP.Linux.Library.LNG.mp

Dil paketini yüklemek için yukarıdaki **Management Pack'leri Alma** bölümünde açıklanan adımların aynısını kullanın. System Center 2012 Operations Manager içinde yüklü olan dili görüntülemek için lütfen aşağıdaki talimatları kullanın:

1. Windows **Başlat** simgesini tıklatın ve **Denetim Masası** öğesine gidin.
2. Denetim Masası içinde **Bölge ve Dil Seçenekleri** öğesini tıklatın.
3. **Yönetim** sekmesinde sistem yerel ayarını Unicode olmayan programlar için değiştirin. **Konum** sekmesinde, Geçerli konumu yüklenen Dil paketine göre değiştirin.

Management Pack Amacı

SCEP için Management Pack şu işlevselliklere sahiptir:

- Güvenlik sorunları ve güvenlik sistem durumu için gerçek zamanlı izleme ve uyarı.
- Güvenlikle ilgili görevleri sunucularında uzaktan gerçekleştirmeleri için sunucu yöneticilerini etkinleştirme. Bu görevlerin ana amacı güvenlikle ilgili kullanılabilirlik sorunlarını düzeltmektir.

Görünümler

Sunucu yöneticisi, Operations Manager konsolunu kullanarak SCEP yüklü tüm bilgisayarları izleyebilir. Aşağıdaki Görünümler, "System Center Endpoint Protection Linux" için kullanılabilir:

- **Etkin Uyarılar** - Tüm önem derecesi seviyelerinin SCEP Etkin Uyarıları. Kapalı uyarıları içermez.
- **Pano** - Hem SCEP'ye Sahip Sunucular hem de Etkin Uyarılar çalışma alanlarını görüntüler.
- **SCEP'ye Sahip Sunucular** - Tüm Korumalı Linux Sunucuları'nı görüntüler.
- **SCEP'si Olmayan Sunucular** - Tüm Korunmayan Linux Sunucuları'nı görüntüler.
- **Görev Durumu** - Yürütülen tüm Görevleri listeler.

System Center 2012 Operations Manager yönetim paketi ile SCEP durumunu izlediğinizde, SCEP sistem durumunun anlık bir görünümünü elde edebilirsiniz.

Bir uyarı verilmesini beklemektense, SCEP bileşenlerinin özet durumunu Operations Manager İzleme konsolunun **Monitoring** > **System Center Endpoint Protection Linux** > **SCEP'ye Sahip Sunucular** bölmesini tıklatarak istediğiniz zaman görüntüleyebilirsiniz. Bir bileşenin durumu, Durum alanında renkli simgelerle gösterilir:

Simge	Durum	Tanım
	Healthy	Yeşil bir simge, başarıyı veya eylem gerektirmeyen kullanılabilir bilgi olduğunu gösterir.
	Warning	Sarı bir simge, hata veya uyarıyı gösterir.
	Critical	Kırmızı bir simge, kritik bir hatayı veya güvenlik sorununu ya da bir hizmetin kullanılamaz olduğunu gösterir.
	Not monitored	Yok simgesi durumu etkileyen hiçbir verinin toplanmadığını gösterir.

Görünüm, nesnelerin uzun bir listesini içerebilir. Belirli bir nesneyi veya nesne grubunu bulmak için Operations Manager araç çubuğundaki Kapsam, Ara ve Bul düğmelerini kullanabilirsiniz. Daha fazla bilgi için How to Manage Monitoring Data Using Scope, Search, and Find (Kapsam, Ara ve Bul Kullanımıyla İzleme Verilerini Yönetme) (http://go.microsoft.com/fwlink/?LinkId=91983) konusuna bakın.

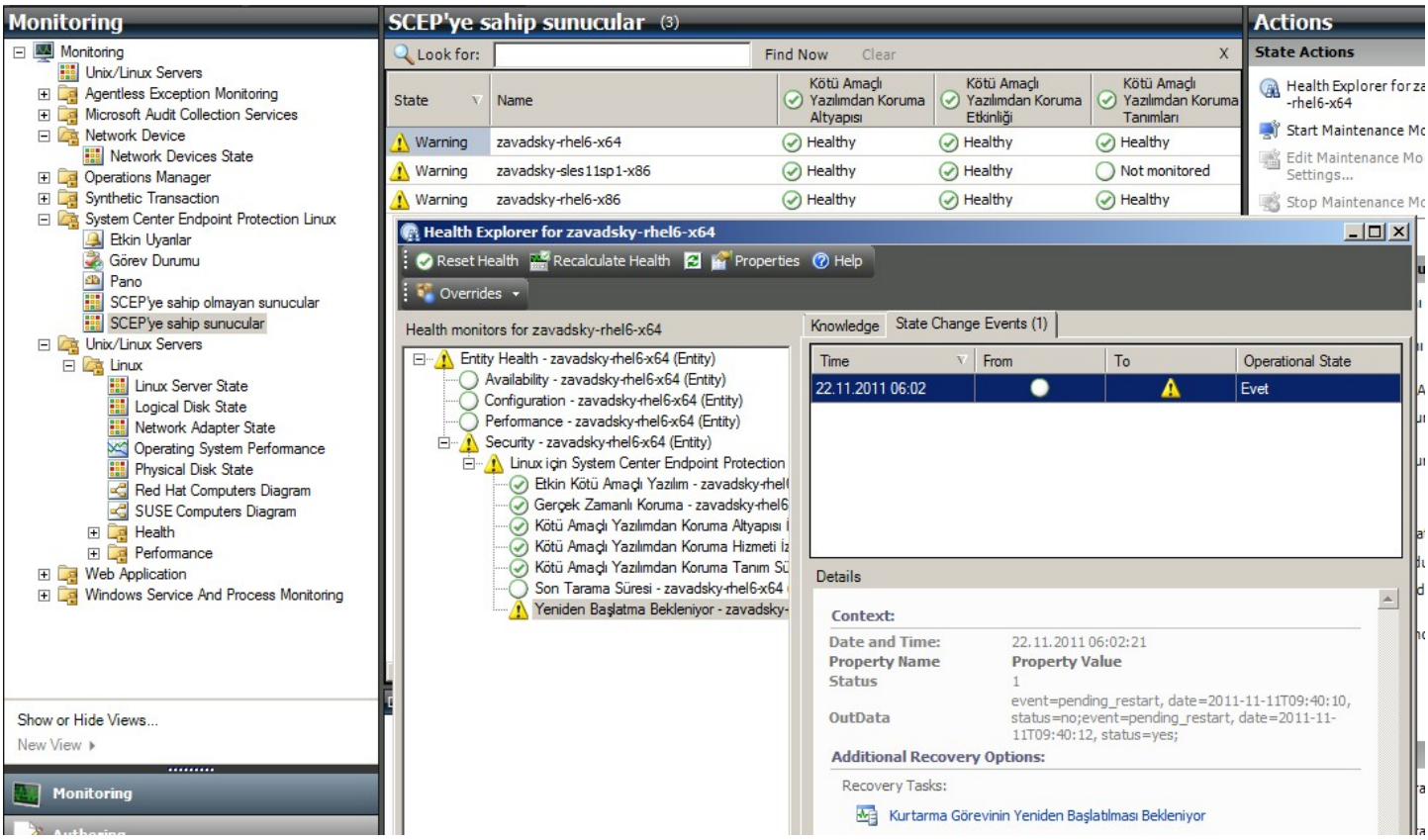
İzleyiciler

Operations Manager 2007'de izleyiciler, izlenen nesnelerde oluşabilen çeşitli koşulları değerlendirmek için kullanılabilir.

SCEP için kullanılabilir toplam 17 izleyici vardır:

- 9 Ünite izleyicisi - Ana izleme bileşenleri; belirli sayaçları, olayları, betikleri ve hizmetleri izlemek amacıyla kullanılır.
- 2 Toplam değer izleyicisi - Birden fazla izleyiciyi bir izleyicide gruplamak ve ardından bu izleyiciyi sistem durumunu ayarlayıp bir uyarı oluşturmak amacıyla kullanmak üzere bir toplam değer oluşturmak için kullanılır.
- 6 Bağımlılık izleyicisi - Varolan izleyicilerin durum verilerini içeren başvurular.

Not: İzleyicilerle ilgili daha fazla bilgi için lütfen Operations Manager 2007 R2 Yardımı'na başvurun (System Center 2012 Operations Manager içinde F1 tuşuna basın).



SCEP Sistem Durumu izleyicileri aşağıdaki tanımlanan yapı ve özelliklere sahiptir.

Etkin Kötü Amaçlı Yazılım

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	Metin günlük dosyasını izler: /var/log/scep/eventlog_scom.dat
Aralık	Olay denetimli

İzleyici türü	Ünite izleyicisi
Uyarı	Evet. Otomatik çözümleme yok
Sıfırlama davranışı	8 saatlik bir süreden sonra Sorunsuz durumuna otomatik olarak dönülür. Uyarı, işlenmeyen kötü amaçlı yazılımla ilgili bilgileri tutmak için etkin kalır.
Notlar	Bu izleyici, kötü amaçlı yazılım bulunduğunda ve bu kötü amaçlı yazılım temizlenmediğinde durumu Kritik olarak değiştirir. Durum 8 saat sonra otomatik olarak Sorunsuz durumuna geri döner (bunun nedeni kötü amaçlı yazılımın temizlenip temizlenmediğinin veya silinip silinmediğinin tam olarak belirlenmesinin mümkün olmamasıdır). Koşulları değerlendirmek ve çağrıyı el ile kapatmak için yöneticinin müdahale etmesi gerekir.
Durum	Sorunsuz - Kötü Amaçlı Yazılım Yok Kritik - Etkin Kötü Amaçlı Yazılım
Etkin	Doğru
Kurtarma görevi	Hayır

Bu izleyici başarısız olan kötü amaçlı yazılım temizleme işlemlerini izler. İstemcinin, kötü amaçlı yazılımı temizleyemediğini bildirmesi durumunda bu izleyici bir Kritik durum bildirir.

Kötü Amaçlı Yazılımdan Koruma Tanım Süreleri

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	İzleme verilerini elde etmek için kullanılan komut: /opt/microsoft/scep/sbin/scep_daemon --status
Aralık	Her 8 saatte bir
Uyarı	Evet. Otomatik çözümleme
Durum	Sorunsuz - süre <= 3 gün Uyarı - süre > 3 VE süre <= 5 gün Kritik - süre > 5 gün
Etkin	Doğru
Kurtarma görevi	Evet, el ile (Otomatik çözümleme yok)

Güncel tanımlar bilgisayarın en yeni kötü amaçlı yazılım tehditlerine karşı korunduğundan emin olmanıza yardımcı olur.

Kötü Amaçlı Yazılımdan Koruma Altyapısı

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	Metin günlük dosyasını izler: /var/log/scep/eventlog_scom.dat
Aralık	Olay denetimli
Uyarı	Evet. Otomatik çözümleme
Durum	Sorunsuz - Etkin Devre Dışı - Uyarı
Etkin	Doğru
Kurtarma görevi	Evet, el ile (Otomatik çözümleme yok)

Kötü amaçlı yazılıma karşı korumanın her zaman etkin tutulması önerilir.
Not: Bu izleyici, Gerçek Zamanlı koruma ile aynı olmayan Antivirus korumasının durumunu izler. Kötü Amaçlı Yazılımdan Koruma altyapısı devre dışı bırakılmışken İsteğe Bağlı tarama başlatılamaz.

Kötü Amaçlı Yazılımdan Koruma Hizmeti

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	İşlem durumunu izler: scep_daemon
Aralık	Her 10 dakikada bir
Uyarı	Evet. Otomatik çözümleme
Durum	Sorunsuz - Çalışıyor Kritik - Çalışmıyor
Etkin	Doğru
Kurtarma görevi	Evet, el ile (Otomatik çözümleme yok)

İstemci makinesindeki kötü amaçlı yazılımdan koruma hizmeti (scep_daemon) çalışmadığında veya yanıt vermediğinde ya da kötü amaçlı yazılımdan koruma altyapısı düzgün bir şekilde çalışmadığında izleyici Kritik durum bildirir.

Son Tarama Süresi

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	İzleme verilerini elde etmek için kullanılan komut: /opt/microsoft/scep/sbin/scep_daemon --status
Aralık	Her 8 saatte bir
Uyarı	Hayır
Durum	Sorunsuz - süre <= 7 Uyarı - süre > 7
Etkin	Doğru
Kurtarma görevi	Evet, el ile (Otomatik çözümleme yok)

Bu izleyici, son bilgisayar taramasından itibaren geçen süreyi izler (tarama türüne bakılmaksızın). Her hafta çalıştırılacak bir tarama zamanlamanızı öneririz.

Yeniden Başlatma Bekleniyor

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	Metin günlük dosyasını izler: /var/log/scep/eventlog_scom.dat
Aralık	Olay denetimli
Uyarı	Evet. Otomatik çözümleme
Durum	Hayır - Sorunsuz Evet - Uyarı
Etkin	Doğru
Kurtarma görevi	Evet, el ile (Otomatik çözümleme yok)

Bu izleyici, yapılandırma değişikliklerinin geçerli olması için sistemin yeniden başlatılması gereksinimini izler (genellikle Gerçek Zamanlı korumanın etkinleştirilmesi / devre dışı bırakılması sırasında). İzleyici, bu durumun isteğe bağlı güncellemesi için aşağıdaki çağrıyı uygular: /opt/microsoft/scep/sbin/scep_daemon --status.

Gerçek Zamanlı Koruma

İzleyici türü	Ünite izleyicisi
Hedef	Korumalı Linux Sunucu
Veri Kaynağı	Metin günlük dosyasını izler: /var/log/scep/eventlog_scom.dat İzleyici, isteğe bağlı bir durum güncellemesi için aşağıdaki çağrıyı da kullanabilir: /opt/microsoft/scep/sbin/scep_daemon --status.
Aralık	olay denetimli
Uyarı	Evet. Otomatik çözümleme
Durum	Etkin - Sorunsuz Devre Dışı - Uyarı
Etkin	Doğru
Kurtarma görevi	Evet, el ile (otomatik çözümleme yok)

Gerçek Zamanlı korumanın durumunu izler. Gerçek zamanlı koruma; virüsler, casus yazılım veya diğer istenmeyen türden olabilecek uygulamalar kendilerini bilgisayarınıza yüklemeye çalıştığında sizi uyarır.

Linux için System Center Endpoint Protection

İzleyici türü	Toplam değer izleyicisi
Hedef	Korumalı Linux Sunucu
Durum	En kötü
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

Bu izleyici, tüm SCEP 7 Korumalı Linux Sunucusu güvenlik ünitesi izleyicileri için Sistem Durumu toplamasıdır (en kötü durum). Durum başlatılmamışsa, bu nesne için izleme başlamamıştır veya bu nesne için tanımlanmış güvenlik izleyicisi yoktur.

Kötü Amaçlı Yazılımdan Koruma Altyapısı

İzleyici türü	Bağımlılık izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Altyapısı

Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

İzlenen bilgisayarlar listesindeki Korumalı Linux Sunucusu/Kötü Amaçlı Yazılımdan Koruma Altyapısı ünite izleyicisi durumunu görüntüler.

Kötü Amaçlı Yazılımdan Koruma Hizmeti

İzleyici türü	Bağımlılık izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Altyapısı
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

İzlenen bilgisayarlar listesindeki Korumalı Linux Sunucusu/Kötü Amaçlı Yazılımdan Koruma Hizmeti Ünite izleyicisi durumunu görüntüler.

Kötü Amaçlı Yazılımdan Koruma Tanımları

İzleyici türü	Bağımlılık izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Tanımları
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

İzlenen bilgisayarlar listesindeki Korumalı Linux Sunucusu/Kötü Amaçlı Yazılımdan Koruma Tanımları Süresi izleyicisi durumunu görüntüler.

Etkin Kötü Amaçlı Yazılım

İzleyici türü	Bağımlılık izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Etkinliği
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

Kötü Amaçlı Yazılımdan Koruma Etkinliği'nin Sistem Durumu Gezgini'ndeki Korumalı Linux Sunucusu/Etkin Kötü Amaçlı Yazılım izleyicisi durumunu görüntüler.

Makine Ping'i

İzleyici türü	Ünite izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Etkinliği
Aralık	Her 60 dakikada bir
Uyarı	Hayır
Durum	Ulaşılabilir - Sorunsuz Ulaşılamaz - Kritik
Etkin	Yanlış
Kurtarma görevi	Hayır

Sunucudan yanıt gelmediğinde durumunu Kritik olarak değiştirir.

Kötü Amaçlı Yazılım Etkinliği

İzleyici türü	Ünite izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Etkinliği
Veri Kaynağı	Metin günlük dosyasını izler: /var/log/scep/eventlog_scom.dat
Aralık	Olay denetimli
Uyarı	Hayır
Durum	Kötü Amaçlı Yazılım Yok - Sorunsuz Kötü Amaçlı Yazılım Etkinliği Algılandı - Kritik
Etkin	Doğru
Kurtarma görevi	Hayır

Bu izleyici, kötü amaçlı yazılım algılamasından (temizlenmiş veya işlenmemiş) sonra 5 dakika içinde Kritik duruma geçer ve sonraki 60 dakika boyunca Kritik olarak kalır. Kritik durum, her yeni pozitif algılamada kendisini ve uyarı süresinin uzunluğunu yeniler. Başka bir deyişle, 60 dakika boyunca sistemde kötü amaçlı yazılım algılanmazsa izleyici, Sorunsuz durumuna döner.

Sunucuda Kötü Amaçlı Yazılım Oluşumu

İzleyici türü	Toplam değer izleyicisi
Hedef	Kötü Amaçlı Yazılımdan Koruma Etkinliği
Durum	En iyi
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

Toplanmış izleyiciler: Kötü Amaçlı Yazılım Etkinliği, Makine Ping'i.
Sunucudan 60 dakika içinde bir yanıt gelmezse durumunu pozitif kötü amaçlı yazılım algılaması yerine (temizlenmiş veya işlenmemiş) Kritik olarak değiştirir. Sunucudan bir süre boyunca yanıt alınmamasını takiben bağlantı yenilenmesinden kısa bir süre sonra kötü amaçlı yazılım algılanırsa durumun Kritik olarak değiştirilmesi de tetiklenebilir.

Kötü Amaçlı Yazılım Oluşumu

İzleyici türü	Bağımlılık izleyicisi
Hedef	Korumalı Sunucular İzleyicisi
Durum	%95'in en kötüsü
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

Kötü Amaçlı Yazılımdan Koruma Etkinliği/Sunucuda Kötü Amaçlı Yazılım Oluşumu izleyicisi durumunu görüntüler.
Geçen 60 dakika içinde Linux Bilgisayarların (Korumalı ve Korunmayan) %5'inden fazlası kötü amaçlı yazılım algılaması kaydederse bu izleyici Kritik duruma geçer.

SCEP Linux Bilgisayar Rolü Sistem Durumu Toplaması

İzleyici türü	Bağımlılık izleyicisi
Hedef	Linux Bilgisayar
Uyarı	Hayır
Etkin	Doğru
Kurtarma görevi	Hayır

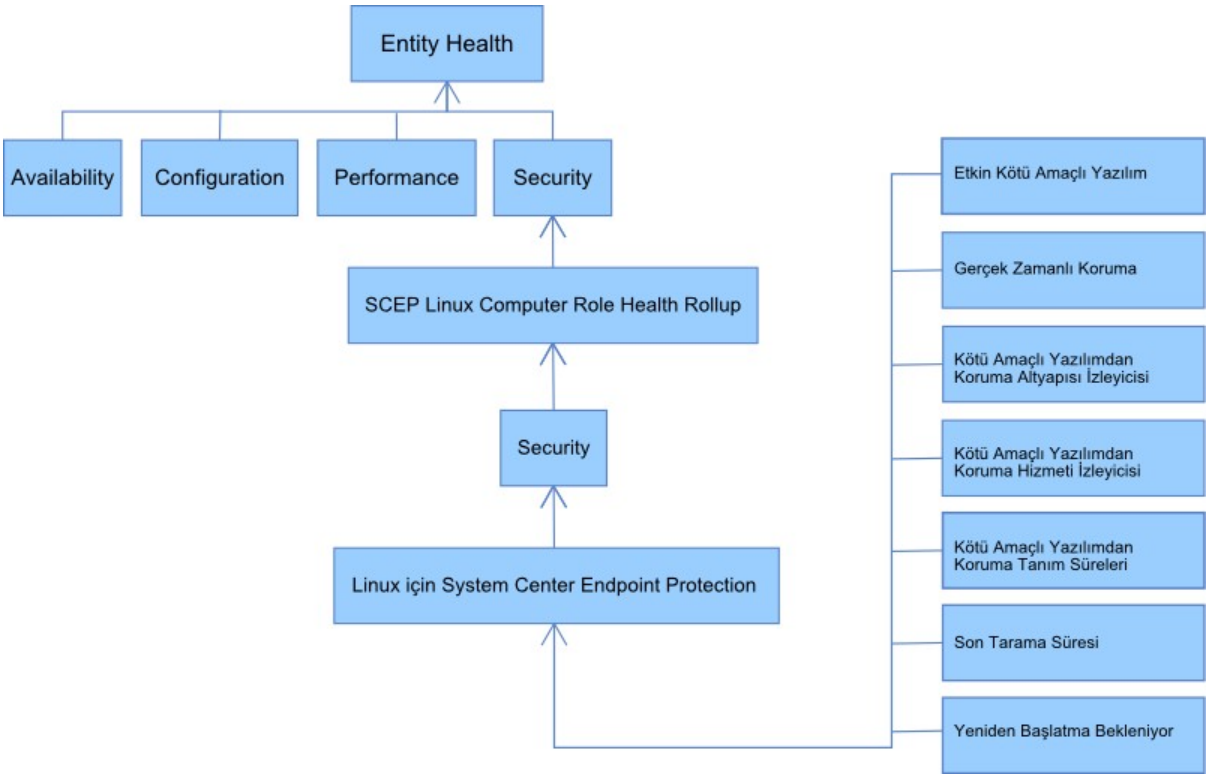
Korumalı Linux Bilgisayarı varlık durumunu, Linux Bilgisayarına/Güvenlik ana izleyicisine yayar.

Sistem Durumu Toplama Biçimi

Bu yönetim paketi, Linux işletim sistemini izleme işlemini her katmanın sorunsuz olması için alt katmana bağlı olduğu katmanlı bir yapı olarak genişletir. Bu yapının en üstü Varlık Sistem Durumu ortamının tamamıdır ve Güvenlik ortamlarının en alt düzeyi izleyicilerin tümüdür. Katmanlardan biri durum değiştirdiğinde onun üstündeki katman da eşleşmek için durum değiştirir. Bu eyleme sistem durumunu toplama denir.

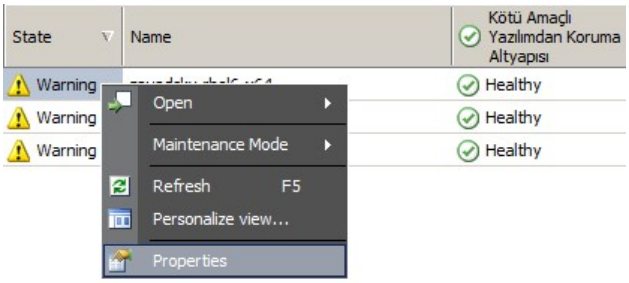
Örneğin Gerçek Zamanlı koruma, Uyarı durumunu döndürürse ve diğer tüm bileşenler Sorunsuzsa Uyarı durumu, Uyarı durumunu alan ağaç yapısı tarafından köke (Varlık Sistem Durumu) aktarılır.

Aşağıdaki diyagram, nesnelerin sistem durumlarının bu yönetim paketinde nasıl toplandığını göstermektedir.



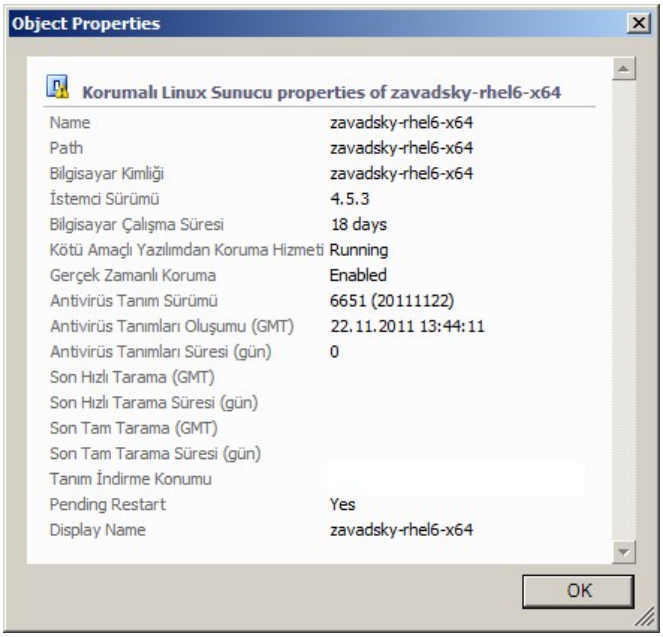
Nesne Özellikleri

Bir nesnenin özelliklerini görüntülemek için nesneyi sağ tıklatın ve **Properties** öğesini seçin.



Korumalı Linux Sunucusu nesnesi şu özelliklere sahiptir:

- **Bilgisayar Kimliği** - Sunucu tanımlayıcı, etki alanı adı.
- **Görüntüleme Adı** - Sunucu adı, etki alanı adı.
- **İstemci Sürümü** - Yüklü SCEP ürününün sürümü.
- **Bilgisayar Çalışma Süresi** - Sunucunun çalışma süresi (makinenin hiç kapanmadan açık kaldığı süre ölçüsü), bir yönetim paketinin düzgün çalışması için önemli olan veri değildir. Bu eksiklik, yönetim paketinde hata gösterilmesine neden olur.
- **Kötü Amaçlı Yazılımdan Koruma Hizmeti** - Kötü amaçlı yazılımdan koruma durumu (Çalışıyor/Çalışmıyor).
- **Gerçek Zamanlı Koruma** - Gerçek zamanlı koruma durumu, eksikliği SCEP sorunları belirtir.
- **Antivirüs Tanımları...** - Virüs veritabanı durumu verileri (sürüm, oluşturulma tarihi, süre), verilerin eksikliği SCEP sorunları belirtir.
- **Son Hızlı/Tam Tarama...** - Son bilgisayar taraması ile ilgili veriler. Tarama (Hızlı Tarama/Tam Tarama) henüz gerçekleştirilmediyse hiçbir veri görünmez.
- **Tanım İndirme Konumu** - Güncelleme sunucusu adresi/adı. İlk başarılı güncellemeden sonra bilgiler görüntülenir.
- **Yeniden Başlatma Bekleniyor** - Yeni bir yükleme veya SCEP yapılandırmasındaki değişiklikler nedeniyle beliren, değişikliklerin geçerli olması için yeniden başlatma işleminin gerekliliği ile ilgili bilgiler.



Uyarılar

Uyarı, belirli önem derecesine (ciddiyet) sahip önceden tanımlı bir durumun izlenen bir nesnede ortaya çıktığını gösteren öğedir. Uyarılar, kurallarla tanımlanır. Operations Manager konsolundaki bir görünüm, konsol kullanıcısının belirli bir nesneyi görme hakkının olduğu uyarıları görüntüleyen **Monitoring** > **System Center Endpoint Protection Linux** > **Etkin Uyarılar** içinde mevcuttur.

Not: Aynı sunucudan aynı türde daha fazla uyarı tekrar tekrar oluşturulursa (örn. Etkin Kötü Amaçlı Yazılım) bunlardan yalnızca ilki görüntülenir (gereksiz uyarılar yoksayılır).

Uyarı	Aralık	Öncelik	Önem Derecesi	Tanım
Tekrarlanan Kötü Amaçlı Yazılımdan Etkilenme Durumu	Olay denetimli	Yüksek	Kritik	Belirtilen zaman aralığı içinde (30 dakika) tekrarlanan kötü amaçlı yazılım algılaması durumunda (3 oluşum) uyarı oluşturulur. Uyarı, sunucu ile ilgili verileri ve kötü amaçlı yazılımla ilgili temel bilgileri içerir.
Kötü Amaçlı Yazılım Temizlendi	Olay denetimli	Düşük Orta	Bilgi - Kötü amaçlı yazılım başarıyla temizlendi Uyarı - Kullanıcı müdahalesi gerekli; örn. sunucunun yeniden başlatılması	Kötü amaçlı bir yazılımla ilgili uyarılar başarıyla temizlendi. Belirli kötü amaçlı yazılımla ilgili kullanılabilir tüm verileri içerir. Algılanan her kötü amaçlı yazılım tek bir olay oluşturur. SCEP Linux, temizleme işlemi verisine göre şu durumlarda öncelik ve önem derecesi atar: Temizlendi = Düşük + Bilgi Temizlendi ancak eylem (örn. yeniden başlatma) gerekli = Orta + Uyarı.
Etkin Kötü Amaçlı Yazılım (İzleyiciden)	Olay denetimli	Yüksek	Kritik	Temizlenmeyen kötü amaçlı yazılımla ilgili uyarılar. Belirli kötü amaçlı yazılımla ilgili kullanılabilir tüm verileri içerir.
Etkin Kötü Amaçlı Yazılım (Kuraldan)	Olay denetimli	Yüksek/Orta/ Düşük	Kritik/Orta/Düşük - Kötü Amaçlı Yazılım türüne bağlı	Yukarıdakiyle aynı. Diğer izleme/çağrı açma sistemlerinin bağlayıcıları için kullanılır. **Not:** Bu kural (uyarı) varsayılan olarak devre dışı bırakılmıştır.
System Center Endpoint Protection kötü amaçlı yazılımdan koruma hizmeti çalışmıyor	300 saniye	Orta	Kritik	Kötü Amaçlı Yazılımdan Koruma hizmeti SCEP'in (scep_daemon) uygun olmaması ile ilgili uyarılar. İlgili sunucu adını ve SCEP sürümünü içerir.
Kötü Amaçlı Yazılımdan Koruma Devre Dışı	Olay denetimli	Orta	Uyarı	Kötü Amaçlı Yazılımdan Korumanın devre dışı bırakılmasıyla ile ilgili uyarılar. İlgili sunucu adını içerir.

Gerçek Zamanlı Koruma Devre Dışı	Olay denetimli	Orta	Uyarı	Gerçek Zamanlı korumanın devre dışı bırakılmasıyla ile ilgili uyarılar. İlgili sunucu adını içerir.
Tanımlar Güncel Değil	Her 8 saatte bir	Orta	Uyarı (süre <= 5 gün VE (süre > 3 gün) Kritik (süre > 5 gün)	3 günden daha fazla bir süredir güncellenmeyen virüs imza veritabanı ile ilgili uyarılar. İlgili sunucu adını ve virüs imza veritabanının süresini içerir.
Kötü Amaçlı Yazılım Oluşumu	Olay denetimli	Yüksek	Kritik	Forefront Endpoint Protection, bilgisayarlarınızda %5'ten daha fazla oranda etkin kötü amaçlı yazılım algıladı. Kötü amaçlı yazılım bilgisayarlarınıza yayılıyor olabilir. Tüm sunucuların en güncel tanımları kullandığından emin olmanız önerilir. Bu uyarıya neden olan etkin tehdit sayısını değiştirmeniz gerekirse Kötü Amaçlı Yazılım Oluşumu izleyicisinin parametresini geçersiz kılın (bkz. Geçersiz Kılmalar bölümü).

Görevler

SCEP için Management Pack, 13 görev uygular. Bu görevlerin yürütülme işlemi hemen gerçekleştirilir. Çıktılar, görev yürütüldükten hemen sonra görüntülenir veya daha sonra Görev Durumu penceresinden görüntülenebilir. Görevin yürütülmesi için gereken maksimum süre 180 saniyedir. Geçersiz kılma kullanılamıyor. Tüm görevler, SSH aracılığıyla yürütülen BASH komutlarıdır.

Görevler, İşlem Konsolu penceresinin sağ bölmesindeki **Monitoring** > **System Center Endpoint Protection Linux** > **SCEP'ye Sahip Sunucular** altında çağrılabilir.

- **Antivirüs Korumasını Devre Dışı Bırak** - Antivirüs korumasının tüm bileşenlerini devre dışı bırakır, İsteğe bağlı taramayı devre dışı bırakır.
- **Antivirüs Korumasını Etkinleştir** - Antivirüs korumasının tüm bileşenlerini etkinleştirir.
- **Gerçek Zamanlı Korumayı Devre Dışı Bırak** - Gerçek zamanlı korumayı devre dışı bırakır.
- **Gerçek Zamanlı Korumayı Etkinleştir** - Gerçek zamanlı korumayı etkinleştirir.
- **Tam Tarama** - Virüs imza veritabanını günceller ve tam bir bilgisayar taraması çalıştırır.
- **Hızlı Tarama** - Virüs imza veritabanını günceller ve hızlı bir bilgisayar taraması çalıştırır.
- **Taramayı Durdur** - Çalışan tüm bilgisayar taramalarını durdurur.
- **Sunucu Ayarlarını Al** - Geçerli SCEP ürünü durumunu görüntüler, görüntülenen parametrelerin listesi Korumalı Linux Sunucusu varlığının özellikleri ile aynıdır. Görüntülenen veriler Korumalı Linux Sunucusuna aktarılmaz.
- **Kötü Amaçlı Yazılımdan Koruma Hizmetini Yeniden Başlat** - SCEP Kötü Amaçlı Yazılımdan Koruma hizmetini (scep_daemon) yeniden başlatır.
- **Kötü Amaçlı Yazılımdan Koruma Hizmetini Durdur** - SCEP Kötü Amaçlı Yazılımdan Koruma hizmetini (scep_daemon) durdurur.
- **Kötü Amaçlı Yazılımdan Koruma Hizmetini Başlat** - SCEP Kötü Amaçlı Yazılımdan Koruma hizmetini (scep_daemon) başlatır.
- **Kötü Amaçlı Yazılımdan Koruma Tanımlarını Güncelle** - Virüs imza veritabanı güncellemesini başlatır.
- **Yeniden Başlat** - Linux bilgisayarını yeniden başlatır.

SCEP için Management Pack'i Yapılandırma

En İyi Uygulama: Özelleştirmeler İçin Management Pack Oluşturma

Varsayılan olarak Operations Manager, Varsayılan Management Pack'i geçersiz kılma gibi tüm özelleştirmeleri kaydeder. En iyi uygulama olarak, özelleştirmek istediğiniz korumalı her bir yönetim paketi için ayrı bir yönetim paketi oluşturmanız gerekir.

Korumalı yönetim paketi için özelleştirilmiş ayarları depolamak üzere bir yönetim paketi oluştururken, yeni yönetim paketinin adını özelleştirilen yönetim paketinin adına (örn. "SCEP 2012 Özelleştirmeleri") dayandırmanız yararlı olur.

Korumalı her bir yönetim paketi için özelleştirmeleri depolamak üzere yeni bir yönetim paketi oluşturmak, özelleştirmeleri test ortamından üretim ortamına verme işlemini kolaylaştırır. Ayrıca, bir yönetim paketini silmeden önce tüm bağımlılıkları silmeniz gerektiğinden, yönetim paketini silme işlemini de kolaylaştırır. Tüm yönetim paketi özelleştirmeleri Varsayılan Management Pack içinde kayıtlı ise ve tek bir yönetim paketini silmeniz gerekiyorsa, öncelikle Varsayılan Management Pack'i silmelisiniz. Bu işlem, diğer yönetim paketlerinin özelleştirmelerini de siler.

Güvenlik Yapılandırması

Bilgisayar, SSHD hizmetini çalıştırmalıdır ve SSH bağlantı noktası (varsayılan değer 22) açık olmalıdır. System Center 2012 Operations Manager, **Basic Authentication** türü ile birlikte uygun Run As Account (Operations Manager İzleme konsolunun **Administration** > **Run As Configuration** bölmesinde bulunan) öğesini kullanarak bağlantı noktası aracılığıyla uzak Linux bilgisayarlara bağlanır.

Farklı Çalıştırma Profili Adı	Notlar
Unix Privileged Account	Unix sunucusunu uzaktan izlemek ve ayrıcalıklı hakların gerektiği işlemleri yeniden başlatmak için kullanılır.

Bu yönetim paketi, Unix Action Account kullanmaz.

Uyarı: Kök hesabın kullanımıyla bilgisayarları izleme, parolanın bozuk olması gibi bir durumda olası bir güvenlik riski oluşturur.

İzleme ve yönetim için kök hesabı kullanmak istemiyorsanız, standart bir kulllanıcı hesabı kullanabilirsiniz; ancak bu hesabın *sudo* komutlarını yürütme haklarına sahip olması gerekir. Bu nedenle, seçili kullanıcı hesabı için sudo geçişini yetkilendirmek üzere her bir Linux SCEP ile izlenen iş istasyonundaki /etc/sudoers dosyasında aşağıdaki yapılandırma bulunmalıdır. Bu user1 kullanıcı adı için örnek niteliğindeki bir yapılandırmadır:

```
#--------------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

Performans Eşik Kuralları Ayarı

Aşağıdaki tablo, ortamınıza uyum sağlaması için ek ayar gerektirebilecek varsayılan eşiklere sahip performans eşik kurallarını listelemektedir. Varsayılan eşiklerin ortamınız için uygun olup olmadığına karar vermek için bu kuralları değerlendirin. Varsayılan bir eşik, ortamınız için uygun değilse eşiklere bir geçersiz kılma uygulayarak eşikleri ayarlayabilirsiniz.

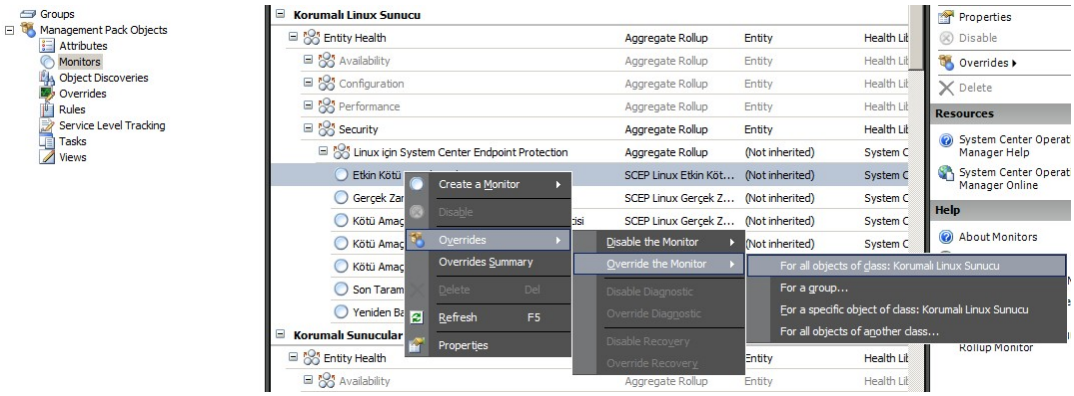
Kural Adı	Geçersiz Kılma Parametresi	Varsayılan Eşik	Ayar Sınırlamaları
Tekrarlanan Kötü Amaçlı Yazılımdan Etkilenme Durumu Kuralı	Tekrarlanan Etkilenme Durumu Sayımı Eşiği	3 oluşum	2'den daha düşük bir değer ayarlamak kuralı geçersiz kılar.

Tekrarlanan Kötü Amaçlı Yazılımdan Etkilenme Durumu Kuralı	Tekrarlanan Etkilenme Durumu Zaman Penceresi	30 dakika	Çakışma bir uyarıyı engelleyebileceğinden değeri, İsteğe Bağlı tarama süresinden daha düşük bir değer olarak ayarlamanız önerilmez.
Etkin Kötü Amaçlı Yazılım Uyarısı Kuralı	Etkin	Yanlış	Diğer izleme/çağrı açma sistemlerine bağlayıcılar kullanırsanız, bu uyarıyı etkinleştirebilirsiniz.

Geçersiz Kılmalar

Geçersiz kılmalar, System Center 2012 Operations Manager içindeki bir izleme nesnesinin ayarlarını iyileştirmek için kullanılabilir. Bu, alınan yönetim paketlerindeki izleyiciler, kurallar, nesne keşifleri ve özellikleri içerir.

Bir izleyiciyi geçersiz kılmak için İşlem Konsolu içinde **Authoring** düğmesini tıklatın ve **Management Pack Objects** > **Monitors** öğelerini genişletin. İzleyiciler bölmesinde bir nesne türü bulun ve tamamen genişletin, ardından bir izleyiciyi tıklatıp **Overrides** öğesini tıklatın.



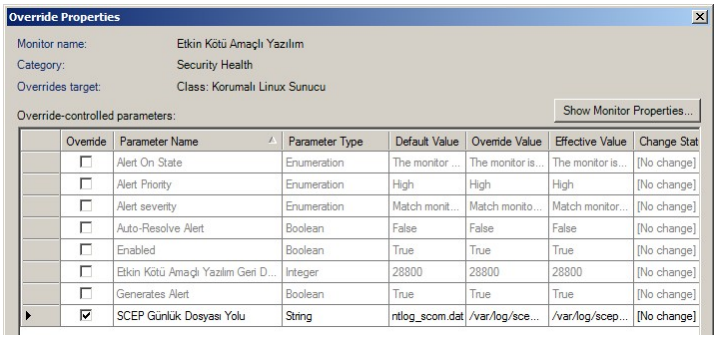
Aşağıdaki parametrelerin herhangi birinin oluşumu için bir geçersiz kılma oluşturmak veya değiştirmek için Geçersiz Kılmalar penceresini kullanın:

- **Etkin Kötü Amaçlı Yazılım İzleyicisi Geri Dönüş Süresi** (yalnızca Etkin Kötü Amaçlı Yazılım izleyicisi ile ilgilidir)
- **Kötü Amaçlı Yazılımdan Koruma Tanımları Süresi** (yalnızca Kötü Amaçlı Yazılımdan Koruma Tanım Süresi izleyicisi ile ilgilidir)
- **Algılama Aralığı** (yalnızca Son Tarama Süresi izleyicisi ile ilgilidir)
- **Durum Uyarısı**
- **Uyarı Önceliği**
- **Uyarı Önem Derecesi**
- **Otomatik Çözümleme Uyarısı**
- **Etkin** - Seçili izleyicinin etkin mi yoksa devre dışı mı olduğunu belirler.
- **Uyarı Oluşturur**
- **SCEP Günlük Dosyası Yolu**

Varsayılan bir geçersiz kılma ortamınız için uygun değilse, bir geçersiz kılma uygulayarak eşikleri ayarlayabilirsiniz:

Geçersiz Kılma Parametresi	İzleyici Adı	Varsayılan Değer	Ayar Notları
Ping Aralığı	Makine Ping'i	3600 saniye	Korumalı Linux Sunucusu'nun kullanılabilirliğini denetleyecek bir aralık. Daha kısa süre, makine bir saldırıdan dolayı yanıt vermeyi keserse Sunucuda Kötü Amaçlı Yazılım Oluşumu izleyicisinde Hata durumunu daha hızlı tetikler. Sonuç olarak ağ, izlenen bilgisayar ve System Center 2012 Operations Manager sunucusundaki yükleme artar.

Kötü Amaçlı Yazılım Oluşum Zamanı Penceresi	Kötü Amaçlı Yazılım Etkinliği	3600 saniye	Kötü amaçlı yazılım etkinliğinden sonra izleyicinin Sorunsuz durumuna geri dönmesi için gerekli olan bir aralık. Zaman Penceresi izleyici değeri, bileşimin düzgün çalışması için Makine Ping'inden/ Ping Aralığından yüksek olmalıdır. Kötü Amaçlı Yazılım Oluşumu Zaman Penceresi aralığı sırasında, belirlenen Kötü Amaçlı Yazılım Oluşumu yüzde değerinden (bkz. Kötü Amaçlı Yazılım Oluşumu) daha fazla miktarda bilgisayar kötü amaçlı yazılım etkinliği kaydederse Kötü Amaçlı Yazılım Oluşumu uyarısı oluşturulur. Not: Bu, uyarı oluşturmayan Sunucuda Kötü Amaçlı Yazılım Oluşumundan farklıdır.
Etkin Kötü Amaçlı Yazılım İzleyicisi Geri Dönüş Süresi	Etkin Kötü Amaçlı Yazılım	28800 saniye	Kötü amaçlı yazılımın temizlenmiş kabul edilmesinden sonraki kötü amaçlı yazılım algılamasından itibaren olan zaman aralığı.
SCEP Günlük Dosyası Yolu	Etkin Kötü Amaçlı Yazılım	/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager olaylarının kaydedildiği dosyaya giden yol. Sorun çıkana dek bu parametreyi değiştirmeyin.
Kötü Amaçlı Yazılımdan Koruma Tanımları Kritik Süresi	Kötü Amaçlı Yazılımdan Koruma Tanım Süreleri	5 gün	Bu aralıktan sonra güncel olmayan SCEP ürünü ile ilgili bildirimde bulunan bir Hata uyarısı oluşturulur.
Kötü Amaçlı Yazılımdan Koruma Tanımları Sağlıklı Süre	Kötü Amaçlı Yazılımdan Koruma Tanım Süreleri	3 gün	Kötü amaçlı yazılımdan koruma tanımlarının güncel kabul edilebileceği azami izin verilen süre. Bu değer her zaman Kötü Amaçlı Yazılımdan Koruma Tanımları Kritik Süresi değerinden daha düşük olmalıdır.
Aralık	Kötü Amaçlı Yazılımdan Koruma Tanım Süreleri	28800 saniye	Kötü amaçlı yazılımdan koruma tanımları süresini denetleme aralığı.
Aralık	Kötü Amaçlı Yazılımdan Koruma Hizmeti	300 saniye	Kötü Amaçlı Yazılımdan Koruma hizmetinin kullanılabilirliğini denetleme aralığı.
İşlem Adı	Kötü Amaçlı Yazılımdan Koruma Hizmeti	scep_daemon	Kötü amaçlı yazılımdan koruma hizmetinin adı. İzleyici işlevsel ise bu değeri değiştirmeyin.
Algılama aralığı	Son Tarama Süresi	28800 saniye	Son tarama yürütme işlemini denetleme aralığı.
Maksimum tarama süresi	Son Tarama Süresi	7 gün	SCEP ürünü ayarlarına göre ayarlanması için. Tarama, her 7 günde gerçekleşecek şekilde zamanlanmışsa bu değeri 7 gün olarak ayarlayın.
Günlük Dosyası Yolu	Yeniden Başlatma Bekleniyor	/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager olaylarının kaydedildiği dosyaya giden yol. Sorun çıkana dek bu parametreyi değiştirmeyin.
SCEP Günlük Dosyası Yolu	Gerçek zamanlı koruma	/var/log/scep/ eventlog_scom.log	System Center 2012 Operations Manager olaylarının kaydedildiği dosyaya giden yol. Sorun çıkana dek bu parametreyi değiştirmeyin.
Yüzde	Kötü Amaçlı Yazılım Oluşumu	95%	İzlenen grubun tamamının Sorunsuz kabul edilmesi için, Sorunsuz durumunu döndürmesi gereken Linux Sunucuları (Korumalı + Korunmayan) yüzdesi. Toplamın %5'inde veya daha fazlasında kötü amaçlı yazılım algılanırsa Kötü Amaçlı Yazılım Oluşumu oluşturulur.



Not: Geçersiz Kılmalar ile ilgili daha fazla bilgi için bkz. How to Monitor Using Overrides (Geçersiz Kılmaların Kullanımını İzleme) (http://go.microsoft.com/fwlink/?LinkID=117777).

Bağlantılar

Aşağıdaki bağlantılar sizi, bu yönetim paketiyle ilişkili olan genel görevlerle ilgili bilgilere yönlendirir:

- Administering the Management Pack Life Cycle (Management Pack'in Ömrünü Yönetme) (http://go.microsoft.com/fwlink/?LinkId=211463)
- How to Import a Management Pack in Operations Manager 2007 (Operations Manager 2007'de Management Pack'i Alma) (http://go.microsoft.com/fwlink/?LinkID=142351)
- How to Monitor Using Overrides (Geçersiz Kılmaların Kullanımını İzleme) (http://go.microsoft.com/fwlink/?LinkID=117777)
- How to Create a Run As Account in Operations Manager 2007 (Operations Manager 2007'de Farklı Çalıştırma Hesabı Oluşturma) (http://go.microsoft.com/fwlink/?LinkID=165410)
- Configuring a Cross Platform Run As Account (Çapraz Platform Farklı Çalıştırma Hesabı Oluşturma) (http://go.microsoft.com/fwlink/?LinkId=160348)
- How to Modify an Existing Run As Profile (Varolan Farklı Çalıştırma Profilini Değiştirme) (http://go.microsoft.com/fwlink/?LinkID=165412)
- How to Export Management Pack Customizations (Management Pack Özelleştirmelerini Verme) (http://go.microsoft.com/fwlink/?LinkId=209940)
- How to Remove a Management Pack (Management Pack'i Kaldırma) (http://go.microsoft.com/fwlink/?LinkId=209941)
- How to Manage Monitoring Data Using Scope, Search, and Find (Kapsam, Ara ve Bul Kullanımıyla İzleme Verilerini Yönetme) (http://go.microsoft.com/fwlink/?LinkId=91983)
- Monitoring Linux Using SCOM 2007 R2 (SCOM 2007 R2 Kullanımıyla Linux'u İzleme) (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Manually Installing Cross Platform Agents (Çapraz Platform Aracılarını El İle Yükleme) (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configuring sudo Elevation for UNIX and Linux Monitoring with System Center 2012 - Operations Manager (System Center 2012 ile UNIX ve Linux İzleme için sudo Geçişi'ni yapılandırma - İşlem Yöneticisi) (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

Operations Manager ve izleme paketleri ile ilgili sorular için bkz. System Center Operations Manager community forum (System Center Operations Manager topluluk forumu) (http://go.microsoft.com/fwlink/?LinkID=179635).
System Center Operations Manager Unleashed blog (System Center Operations Manager Unleashed web günlüğü) (http://opsmgrunleashed.wordpress.com/), belirli izleme paketleri için "Örnek" gönderiler içeren yararlı bir kaynaktır.

Operations Manager ile ilgili ek bilgi için aşağıdaki web günlüklerine bakın:

- Operations Manager Team Blog (Operations Manager Ekibi Web Günlüğü) (http://blogs.technet.com/momteam/default.aspx)
- Kevin Holman's OpsMgr Blog (Kevin Holman'ın OpsMgr Web Günlüğü) (http://blogs.technet.com/kevinholman/default.aspx)
- Thoughts on OpsMgr (OpsMgr ile İlgili Düşünceler) (http://thoughtsonopsmgr.blogspot.com/)
- Raphael Burri's blog (Raphael Burri'nin web günlüğü) (http://rburri.wordpress.com/)
- BWren's Management Space (BWren'in Yönetim Alanı) (http://blogs.technet.com/brianwren/default.aspx)
- The System Center Operations Manager Support Team Blog (System Center Operations Manager Destek Ekibi Web Günlüğü) (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++ (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Notes on System Center Operations Manager (System Center Operations Manager'la İlgili Notlar) (http://blogs.msdn.com/mariussutara/default.aspx)

Sorun giderme için aşağıdaki Forum yazılarını ziyaret edin:

- Microsoft.Unix.Library is missing (Microsoft.Unix.Library eksik) (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)