System Center Endpoint Protection

Yükleme El Kitabı ve Kullanıcı Kılavuzu

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

İçindekiler

Giriş 3

Ana işlevsellik 3

Sistemin temel özellikleri 3

Terminoloji ve kısaltmalar 5

Yükleme 6

Mimariye Genel Bakış 7

Dosya Sistemi hizmetleriyle tümleştirme 8

İsteğe bağlı tarayıcı 8

Dazuko tarafından desteklenen gerçek zamanlı koruma 8

Çalışma ilkesi 8

Yükleme ve yapılandırma 9

İpuçları 9

Önyüklemeli LIBC kitaplığı kullanılarak gerçek zamanlı koruma 9

Çalışma ilkesi 9

Yükleme ve yapılandırma 10

İpuçları 10

Önemli SCEP mekanizmaları 11

Nesne İşleme İlkesi 11

Kullanıcıya Özel Yapılandırma 11

Zamanlayıcı 12

Web Arabirimi 12

Gerçek zamanlı koruma yapılandırması örneği 13

İsteğe bağlı tarayıcı 14

Zamanlayıcı 15

İstatistikler 16

Günlüğe kaydetme 16

SCEP Güvenlik sistemi güncellemesi 17

SCEP güncelleme yardımcı programı 17

SCEP güncelleme işlemi açıklaması 17

Bize bildirin 18

Ek A. PHP Lisansı 19

Giriş

System Center Endpoint Protection ürününü kullandığınız için teşekkür ederiz. Microsoft'un son derece gelişmiş tarama motoru, çok küçük parmak izi ile birlikte olağanüstü tarama hızına ve algılama oranlarına sahiptir ve bu da onu herhangi bir Linux OS sunucusu için ideal tercih haline getirir.

Ana işlevsellik

İsteğe bağlı tarayıcı

İsteğe bağlı tarayıcı; komut satırı arabirimi, web arabirimi aracılığıyla ayrıcalıklı bir kullanıcı (genellikle bir sistem yöneticisi) tarafından veya işletim sisteminin otomatik zamanlama aracı (örn. cron) tarafından başlatılabilir. *İsteğe bağlı* terimi, kullanıcı veya sistem isteğiyle taranmakta olan dosya sistemi nesnelerini ifade eder.

Gerçek zamanlı koruma

Bir kullanıcı ve/veya işletim sistemi, dosya sistemi nesnelerine erişmeyi her denediğinde Gerçek zamanlı koruma çağrılır. Dosya sistemi nesnelerine erişme girişiminde bulunulduğunda bir tarama tetiklendiğinden, bu, *Aktif* teriminin kullanımını da netleştirir.

Sistemin temel özellikleri

Gelişmiş altyapı algoritmaları

Microsoft antivirus tarama altyapısı algoritmaları, en yüksek algılama oranını ve en hızlı tarama sürelerini sağlar.

Çoklu işleme

System Center Endpoint Protection, tekli ve çoklu işlemci birimlerinde çalışacak şekilde geliştirilmiştir.

Gelişmiş Sezgisel Tarama

System Center Endpoint Protection; Win32 solucanları, arka kapı programı bulaşmaları ve diğer kötü amaçlı yazılım biçimleri için benzersiz gelişmiş sezgisel tarama işlevi içerir.

Yerleşik özellikler

Yerleşik arşivleyiciler, herhangi bir dış program gerektirmeden arşivlenmiş nesnelerin paketini açar.

Hız ve verimlilik

Sistemin hızını ve verimliliğini artırmak için, System Center Endpoint Protection uygulamasının mimarisi tüm tarama isteklerinin gönderildiği çalışmakta olan daemon'ı (yerel program) temel alır.

Gelişmiş güvenlik

Tüm yönetim daemon'ları (scep_dac dışında), güvenliği artırmak için ayrıcalıklı olmayan bir kullanıcı hesabı altında çalışır.

Seçmeli yapılandırma

Sistem, kullanıcıyı veya istemci/sunucuyu temel alan seçmeli yapılandırmayı destekler.

Birden çok günlüğe kaydetme düzeyi

Sistem etkinliği ve sızıntılar hakkında bilgi almak için birden çok günlüğe kaydetme düzeyi yapılandırılabilir.

Web arabirimi

Sezgisel ve kullanıcı dostu bir web arabirimi yoluyla yapılandırma ve yönetim sunulur.

Dış kitaplık yoktur

System Center Endpoint Protection yüklemesi, LIBC dışında dış kitaplıklar veya programlar gerektirmez.

Kullanıcı tarafından belirtilen bildirim

Sistem, bir sızıntı algılanması durumunda veya diğer önemli durumlarda belirli kullanıcılara bildirim gönderecek şekilde yapılandırılabilir.

Düşük sistem gereksinimleri

System Center Endpoint Protection uygulamasının verimli şekilde çalışması için 16MB sabit disk alanı ve 32MB RAM gerekir. 2.2.x, 2.4.x ve 2.6.x Linux OS çekirdek sürümlerinde sorunsuz şekilde çalışır.

Performans ve ölçeklenebilirlik

System Center Endpoint Protection, düşük güçlü, küçük ofis sunucularından binlerce kullanıcıya sahip kurumsal sınıf ISP sunucularına kadar her ölçekte sunucuya bir UNIX tabanlı sunucudan beklediğiniz performans ve ölçeklenebilirliği ve Microsoft güvenlik ürünlerinin benzersiz güvenliğini sunar.

Terminoloji ve kısaltmalar

Bu bölümde, bu belgede kullanılan terim ve kısaltmaları gözden geçireceğiz. Ürün bileşen adları ve yeni tanımlanan terimler ve kısaltmalar için kalın yazı tipi kullanıldığını unutmayın. Bu bölümde tanımlanan terim ve kısaltmalar, bu belgenin ilerleyen bölümlerinde açıklanmaktadır.

SCEP

SCEP, Linux işletim sistemleri için Microsoft tarafından geliştirilen güvenlik ürününün standart kısaltmasıdır. Bu aynı zamanda ürünleri içeren yazılım paketinin de adıdır.

SCEP daemon

Ana SCEP sistem denetimi ve tarama daemon'ı: *scep_daemon*.

SCEP temel dizini

Virüs imza veritabanını içeren SCEP yüklenebilir modüllerinin depolandığı dizin. Gelecekte bu dizini ifade etmek için *@BASEDIR@* kısaltması kullanılacaktır. *@BASEDIR@* değeri (işletim sistemine bağlı olarak) aşağıda listelenmektedir:

```
Linux: /var/opt/microsoft/scep/lib
```

SCEP yapılandırma dizini

System Center Endpoint Protection yapılandırmasıyla ilgili tüm dosyaların depolandığı dizin. Gelecekte bu dizini ifade etmek için *@ETCDIR@* kısaltması kullanılacaktır. *@ETCDIR@* değeri (işletim sistemine bağlı olarak) aşağıda listelenmektedir:

```
Linux: /etc/opt/microsoft/scep
```

SCEP yapılandırma dosyası

Ana System Center Endpoint Protection yapılandırma dosyası. Dosyanın mutlak yolu şu şekildedir:

@ETCDIR@/scep.cfg

SCEP ikili dosya dizini

İlgili System Center Endpoint Protection ikili dosyalarının depolandığı dizin. Gelecekte bu dizini ifade etmek için *@BINDIR@* kısaltması kullanılacaktır. *@BINDIR@* değeri (işletim sistemine bağlı olarak) aşağıda listelenmektedir:

```
Linux: /opt/microsoft/scep/bin
```

SCEP sistem ikili dosyaları dizini

İlgili System Center Endpoint Protection sistem ikili dosyalarının depolandığı dizin. Gelecekte bu dizini ifade etmek için *@SBINDIR@* kısaltması kullanılacaktır. *@SBINDIR@* değeri (işletim sistemine bağlı olarak) aşağıda listelenmektedir:

```
Linux: /opt/microsoft/scep/sbin
```

SCEP nesne dosyaları dizini

İlgili System Center Endpoint Protection nesne dosyaları ve kitaplıklarının depolandığı dizin. Gelecekte bu dizini ifade etmek için *@LIBDIR@* kısaltması kullanılacaktır. *@LIBDIR@* değeri (işletim sistemine bağlı olarak) aşağıda listelenmektedir:

```
Linux: /opt/microsoft/scep/lib
```

Yükleme

System Center Endpoint Protection, ikili dosya olarak dağıtılır:

```
scep.i386.ext.bin
```

Yukarıda gösterilen ikili dosyada *'ext'*, bir Linux işletim sistemi dağıtımına bağımlı sonektir; örneğin Debian için 'deb', RedHat ve SuSE için 'rpm', diğer Linux OS dağıtımları için 'tgz'.

Ürünü yüklemek veya yükseltmek için aşağıdaki komutu kullanın:

```
sh ./scep.i386.ext.bin
```

ürünün Kullanıcı Lisans Kabulü Sözleşmesi'ni görüntülemek için. Kabul Sözleşmesi'ni onaylamanızın ardından yükleme paketi geçerli çalışma dizinine yerleştirilir ve paketin yüklenmesi, kaldırılması veya yükseltilmesiyle ilgili bilgiler ekranda görüntülenir.

Paket yüklendikten sonra, aşağıdaki komutu kullanarak ana SCEP hizmetinin çalıştığını doğrulayabilirsiniz:

```
ps -C scep_daemon
```

ENTER tuşuna bastıktan sonra aşağıdaki (veya benzeri) iletiyi görmeniz gerekir:

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

Arka planda en az iki SCEP daemon işlemi çalışmaktadır. Birinci PID, işlemi ve sistemin iş parçacığı yöneticisini temsil eder. Diğeri, SCEP tarama işlemini temsil eder.

Dil paketi yükleme

System Center Endpoint Protection için gerekli dil paketini yüklemek üzere aşağıdaki komutu kullanın:

```
sh ./scep-lang.lng.bin
```

'lng' dilinin, almak istediğiniz dosya dil koduyla değiştirilmesi gereken yer.

Installation completed successfully bildirimi görüntülendikten sonra, LANG sistem değişkenini uygun şekilde güncelleyin ve gerekirse ortamı güncelleyin. Bu, dil paketi yükleme işlemini sonuçlandırır.

Her bir dil paketi şunları içerir:

- Yerelleştirilmiş Web Arabirimi
- SCEP aracılarının ve komutlarının yerelleştirilmiş konsol çıktıları
- Yerelleştirilmiş PDF Belgesi

Mimariye Genel Bakış

System Center Endpoint Protection başarıyla yüklendikten sonra, bu uygulamanın mimarisini tanımanız gerekir.

Sistem aşağıdaki bölümlerden oluşur:

ÇEKİRDEK

System Center Endpoint Protection uygulamasının çekirdeği, SCEP daemon'dır (scep_daemon). Bu daemon; tarama, aracı daemon işlemlerinin bakımı, örnek gönderim sisteminin bakımı, günlüğe kaydetme, bildirim, vb. gibi temel sistem görevleri sağlamak için libscep.so SCEP API kitaplığını ve em00X_xx.dat SCEP yükleme modüllerini kullanır. Lütfen ayrıntılar için *scep_daemon(8)* el kitabı sayfasına bakın.

ARACILAR

SCEP aracı modüllerinin amacı, SCEP'yi Linux sunucu ortamıyla tümleştirmektir.

YARDIMCI PROGRAMLAR

Yardımcı program modülleri, kolay ve etkili sistem yönetimi sağlar. Bunlar, karantina yönetimi, sistem ayarları ve güncelleme gibi sistem görevlerinden sorumludur.

YAPILANDIRMA

Güvenlik sisteminizin en önemli yönünü uygun yapılandırma oluşturur; bu bölümün geri kalanında tüm ilgili bileşenler açıklanacaktır. *scep.cfg* dosyası, System Center Endpoint Protection yapılandırması için temel olan bilgileri içerdiğinden, bu dosyanın kapsamlı olarak anlaşılması da kesinlikle önerilir.

Ürün başarıyla kurulduktan sonra, ürünün tüm yapılandırma bileşenleri SCEP yapılandırma dizininde depolanır. Dizin aşağıdaki dosyalardan oluşur:

@ETCDIR@/scep.cfg

Bu, ürün işlevselliğinin tüm ana yönlerini denetlediğinden, en önemli yapılandırma dosyasıdır. scep.cfg dosyası, her biri çeşitli parametreler içeren birçok bölümden oluşur. Bu dosya, tüm bölüm adlarının köşeli ayraç içine alındığı bir genel ve birçok "aracı" bölüm içerir. Genel bölümdeki parametreler, SCEP daemon'ın yapılandırma seçeneklerini ve SCEP tarama altyapısı yapılandırmasının varsayılan değerlerini tanımlamak için kullanılır. Aracı bölümlerdeki parametreler, bilgisayardaki ve/veya civarındaki çeşitli veri akışı türlerini kesmek için kullanılan modüllerin yapılandırma seçeneklerini tanımlamak için kullanılır. Sistem yapılandırması için kullanılan çeşitli parametrelere ek olarak, dosyanın düzenlemesini belirleyen kurallar da olduğunu unutmayın. Bu dosyayı düzenlemenin en etkili yolu hakkında ayrıntılı bilgi için lütfen *scep.cfg(5)* ve *scep_daemon(8)* el kitabı sayfalarına ve ilgili aracıların el kitabı sayfasına bakın.

@ETCDIR@/certs

Bu dizin, SCEP web arabirimi tarafından kimlik doğrulaması için kullanılan sertifikaları depolamak için kullanılır. Lütfen ayrıntılar için *scep_wwwi(8)* el kitabı sayfasına bakın.

@ETCDIR@/scripts/daemon_notification_script

'exec_script' SCEP yapılandırma dosyası parametresi tarafından etkinleştirilmişse, antivirus sistemi tarafından bir sızıntı algılanması durumunda bu komut dosyası yürütülür. Sistem yöneticisine olayla ilgili e-posta bildirimi göndermek için kullanılır.

Dosya Sistemi hizmetleriyle tümleştirme

Bu bölümde, virüs ve solucan dosya sistemi bulaşmasına karşı en etkili korumayı sağlayacak İsteğe bağlı ve Gerçek zamanlı koruma yapılandırması açıklanır. System Center Endpoint Protection ürününün tarama gücü, *'scep_scan'* İsteğe bağlı tarayıcı komutu ve *'scep_dac'* Aktif koruma komutundan gelir. System Center Endpoint Protection uygulamasının Linux sürümü, *libscep_pac.so* önceden yüklenmiş kitaplık modülünü kullanan ek bir Aktif koruma tekniği sunar. Tüm bu komutlar, aşağıdaki bölümlerde açıklanmaktadır.

İsteğe bağlı tarayıcı

İsteğe bağlı tarayıcı; komut satırı arabirimi, web arabirimi aracılığıyla ayrıcalıklı bir kullanıcı (genellikle bir sistem yöneticisi) tarafından veya işletim sisteminin otomatik zamanlama aracı (örn. cron) tarafından başlatılabilir. *İsteğe bağlı* terimi, kullanıcı veya sistem isteğiyle taranan dosya sistemi nesnelerini ifade eder.

İsteğe bağlı tarayıcının çalışması için özel yapılandırma gerekmez. SCEP paketi düzgün bir şekilde yüklendikten sonra, komut satırı arabirimi veya Zamanlayıcı aracı kullanılarak İsteğe bağlı tarayıcı hemen çalıştırılabilir. Komut satırından İsteğe bağlı tarayıcıyı çalıştırmak için aşağıdaki sözdizimini kullanın:

```
@SBINDIR@/scep_scan [option(s)] FILES
```

burada FILES, taranacak dizinlerin ve/veya dosyaların bir listesidir.

SCEP İsteğe bağlı tarayıcısı kullanılarak birden çok komut satırı seçeneği kullanılabilir. Tam seçenek listesini görüntülemek için *scep_scan(8)* el kitabı sayfasına bakın.

Dazuko tarafından desteklenen gerçek zamanlı koruma

Gerçek zamanlı koruma, dosya sistemi nesnelerine kullanıcı erişimi ve/veya işletim sistemi erişimi tarafından çağrılır. Bu, *Aktif* terimini de açıklar; tarayıcı yalnızca seçilen bir dosya sistemi nesnesine erişme girişiminde bulunulduğunda tetiklenir.

SCEP Aktif koruma tarafından kullanılan teknik, Dazuko (da-tzu-ko) çekirdek modülü tarafından desteklenir ve çekirdek çağrılarının durdurulmasını temel alır. Dazuko projesi açık kaynaktır; başka bir deyişle, kaynak kodu serbest şekilde dağıtılır. Bu, kullanıcıların kendi özel çekirdekleri için çekirdek modülünü derlemesine olanak sağlar. Dazuko çekirdek modülünün herhangi bir SCEP ürününün parçası olmadığını ve *scep_dac* Aktif komutu kullanılmadan önce derlenmesi ve çekirdeğe yüklenmesi gerektiğini unutmayın. Dazuko tekniği, Aktif korumayı, kullanılan dosya sistemi türünden bağımsız hale getirir. Dosya sistemi nesnelerinin Network File System (NFS), Nettalk ve Samba aracılığıyla taranması için de uygundur.

Önemli: Aktif koruma yapılandırma ve kullanımıyla ilgili ayrıntılı bilgi sağlamadan önce, tarayıcının öncelikle dışarıdan takılan dosya sistemlerini korumak için geliştirildiği ve sınandığı unutulmamalıdır. Dışarıdan takılmayan birden çok dosya sistemi varsa, sistem kilitlenmelerini önlemek için bunları dosya erişim denetimi dışında bırakmanız gerekir. Dışarıda bırakılacak tipik bir dizine örnek olarak *'/dev'* dizini ve SCEP tarafından kullanılan tüm dizinler verilebilir.

Çalışma ilkesi

Gerçek zamanlı koruma *scep_dac* (SCEP Dazuko-powered file Access Controller), dosya sistemi üzerinde sürekli izleme ve denetim sağlayan yerel bir programdır. Her dosya sistemi nesnesi, özelleştirilebilir dosya erişimi olayı türlerine göre taranır. Geçerli sürüm tarafından aşağıdaki olay türleri desteklenir:

Açma olayları

Bu dosya erişimi türünü etkinleştirmek için, *'event_mask'* parametresinin değerini, scep.cfg dosyasının **[fac]** bölümünde açılacak şekilde ayarlayın. Bu, Dazuko erişim maskesinin ON_OPEN bit'ini etkinleştirir.

Kapatma olayları

Bu dosya erişimi türünü etkinleştirmek için, *'event_mask'* parametresinin değerini, scep.cfg dosyasının **[fac]** bölümünde kapanacak şekilde ayarlayın. Bu, Dazuko erişim maskesinin ON_OPEN bit'ini etkinleştirir. Bu, Dazuko erişim maskesinin ON_CLOSE ve ON_CLOSE_MODIFIED bit'lerini etkinleştirir.

Not: Bazı OS çekirdeği sürümleri, ON_CLOSE olaylarının durdurulmasını desteklemez. Bu durumlarda, kapatma olayları *scep_dac* tarafından izlenmez.

Yürütme olayları

Bu dosya erişimi türünü etkinleştirmek için, *'event_mask'* parametresinin değerini, scep.cfg dosyasının **[fac]** bölümünde yürütülecek şekilde ayarlayın. Bu, Dazuko erişim maskesinin ON_EXEC bit'ini etkinleştirir.

Gerçek zamanlı koruma, tüm açılan, kapatılan ve yürütülen dosyaların önce *scep_daemon* tarafından virüslere karşı taranmasını sağlar. Tarama sonuçlarına bağlı olarak, belirli dosyalara erişim reddedilir veya belirli dosyalara erişime izin verilir.

Yükleme ve yapılandırma

scep_dac başlatılmadan önce, Dazuko çekirdek modülü derlenmeli ve çalışmakta olan çekirdek içinde yüklenmelidir. Dazuko'nun derlenmesi ve yüklenmesine ilişkin ayrıntılar için lütfen bkz:

http://www.dazuko.org

Dazuko yüklendikten sonra, SCEP yapılandırma dosyasının (scep.cfg) **[global]** ve **[fac]** bölümlerini gözden geçirip düzenleyin. Gerçek zamanlı korumanın düzgün şekilde çalışmasının, bu dosyanın **[fac]** bölümündeki *'agent_type'* seçeneğinin yapılandırılmasına bağlı olduğunu unutmayın. Ayrıca, Gerçek zamanlı koruma tarafından izlenecek dosya sistemi nesnelerini (örn. dizinler ve dosyalar) tanımlamanız gerekir. **[fac]** bölümünde de bulunan *'ctl_incl'* ve *'ctl_excl'* parametreleri tanımlanarak bu gerçekleştirilebilir. scep.cfg dosyası üzerinde değişiklik yaptıktan sonra, SCEP daemon'ı yeniden yükleyerek yeni oluşturulan yapılandırmayı yeniden okunmaya zorlayabilirsiniz.

İpuçları

scep_dac daemon başlatılmadan önce Dazuko modülünün yüklenmesini sağlamak için şu adımları izleyin:

Çekirdek modülleri için ayrılmış şu dizinlerden birine Dazuko modülünün bir kopyasını yerleştirin:

```
/lib/modules
```

veya

```
/modules
```

Bağımlılıkları işlemek ve yeni eklenen Dazuko modülünü başarıyla başlatmak için 'depmod' ve 'modprobe' çekirdek yardımcı programlarını kullanın (BSD OS için 'kldconfig' ve 'kldload' yardımcı programını kullanın).

'/etc/init.d/scep_daemon' scep_daemon başlatma komut dosyasında, daemon başlatma deyiminin önüne şu satırı ekleyin:

```
/sbin/modprobe dazuko
```

BSD OS için

```
/sbin/kldconfig dazuko
```

satırı, '/usr/local/etc/rc.d/scep_daemon.sh' komut dosyasına eklenmelidir.

Uyarı! Bu adımların tam olarak verilen sırada yürütülmesi çok önemlidir. Çekirdek modülü, çekirdek modülleri dizininde bulunmuyorsa, düzgün şekilde yüklenmeyerek sistemin kilitlenmesine neden olur.

Önyüklemeli LIBC kitaplığı kullanılarak gerçek zamanlı koruma

Önceki bölümlerde, Linux/BSD dosya sistemi hizmetleri ile Dazuko tarafından desteklenen Gerçek zamanlı koruma tümleştirmesini açıkladık. Dazuko'nun kullanılması her durumda uygun olmayabilir; aşağıdaki özellikleri içeren kritik sistemleri koruyan sistem yöneticileri de buna dahildir:

- çalışan çekirdekle ilgili kaynak kod ve/veya yapılandırma dosyalarının kullanılabilir olmadığı,
- çekirdeğin modülerden daha monolitik olduğu,
- Dazuko modülünün söz konusu işletim sistemini desteklemediği.

Bu durumların herhangi birinde, önyüklemeli LIBC kitaplığını temel alan Aktif koruma tekniği kullanılmalıdır. Ayrıntılı bilgi için bu bölümde yer alan aşağıdaki konulara bakın. Bu bölümün yalnızca Linux OS kullanıcıları için geçerli olduğunu ve *'libscep_pac.so'* önyüklemeli kitaplığı kullanılarak Aktif korumanın çalışması, yüklemesi ve yapılandırmasıyla ilgili bilgiler içerdiğini unutmayın

Çalışma ilkesi

Gerçek zamanlı koruma *libscep_pac.so* (SCEP Preload library based file Access Controller), sistem açılışında etkinleştirilen bir paylaşılan nesne kitaplığıdır. Bu kitaplık; FTP sunucusu, Samba sunucusu, vb. gibi dosya sistemi sunucuları tarafından yapılan LIBC çağrıları için kullanılır. Her dosya sistemi nesnesi, özelleştirilebilir dosya erişimi olayı türleri temel alınarak taranır. Geçerli sürüm tarafından aşağıdaki olay türleri desteklenir:

Açma olayları

esest.cfg dosyasındaki (**[fac]** bölümü) *'event_mask'* parametresinde *'open'* sözcüğü varsa bu dosya erişimi türü etkinleştirilir.

Kapatma olayları

scep.cfg dosyasındaki (**[fac]** bölümü) *'event_mask'* parametresinde *'close'* sözcüğü varsa bu dosya erişimi türü etkinleştirilir. Bu durumda, LIBC'nin tüm dosya tanımlayıcısı ve FILE akışı kapatma işlevleri durdurulur.

Yürütme olayları

scep.cfg dosyasındaki (**[fac]** bölümü) *'event_mask'* parametresinde *'exec'* sözcüğü varsa bu dosya erişimi türü etkinleştirilir. Bu durumda, LIBC'nin tüm yürütme işlevleri durdurulur.

Tüm açılan, kapatılan ve yürütülen dosyalar, SCEP daemon tarafından virüslere karşı taranır. Bu tür taramaların sonucuna göre, belirli dosyalara erişim reddedilir veya belirli dosyalara erişime izin verilir.

Yükleme ve yapılandırma

libscep_pac.so kitaplık modülü, önceden yüklenen kitaplıkların standart bir yükleme mekanizması kullanılarak yüklenir. *libscep_pac.so* kitaplığının mutlak yolu ile *'LD_PRELOAD'* ortam değişkenini tanımlamanız gerekir. Daha fazla bilgi için lütfen *ld.so(8)* el kitabı sayfasına bakın.

Not: *'LD_PRELOAD'* ortam değişkeninin yalnızca Gerçek zamanlı koruma denetimi altında olacak ağ sunucusu daemon işlemleri (ftp, Samba, vb.) için tanımlanması önemlidir. Genellikle tüm işletim sistemi işlemleri için LIBC çağrılarının önceden yüklenmesi önerilmez; bu, sistem performansını büyük ölçüde düşürebilir veya sistemin kilitlenmesine yol açabilir. Bu anlamda, '/etc/ld.so.preload' dosyası kullanılmamalı veya 'LD_PRELOAD' ortam değişkeni genel olarak verilmemelidir. Her ikisi de tüm ilgili LIBC çağrılarını geçersiz kılar ve bu da başlatma sırasında sistem kilitlenmelerine yol açabilir.

Belirli bir dosya sisteminde yalnızca ilgili dosya erişim çağrılarının durdurulduğundan emin olmak için, aşağıdaki satır kullanılarak yürütülebilir deyimler geçersiz kılınabilir:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

burada 'COMMAND COMMAND-ARGUMENTS', özgün yürütülebilir deyimdir.

SCEP yapılandırma dosyasının (scep.cfg) **[global]** ve **[fac]** bölümlerini gözden geçirip düzenleyin. Aktif korumanın düzgün şekilde çalışması için, ön yüklemeli kitaplığın denetimi altında olması gereken dosya sistemi nesnelerini (örn. dizinler ve dosyalar) tanımlamanız gerekir. SCEP yapılandırma dosyasının **[fac]** bölümünde *'ctl_incl'* ve *'ctl_excl'* seçeneklerinin parametreleri tanımlanarak bu gerçekleştirilebilir. scep.cfg dosyası üzerinde değişiklik yaptıktan sonra, SCEP daemon'ı yeniden yükleyerek yeni oluşturulan yapılandırmayı yeniden okunmaya zorlayabilirsiniz.

İpuçları

Dosya sistemi açılışından hemen sonra Gerçek zamanlı korumayı etkinleştirmek için, uygun ağ dosya sunucusu başlatma komut dosyasında *'LD_PRELOAD'* ortam değişkeni tanımlanmalıdır.

Örnek: Aktif korumanın, Samba sunucusu başlatıldıktan hemen sonra tüm dosya sistemi erişim olaylarını izlemesini istediğimizi varsayalım. Samba daemon başlatma komut dosyası (/etc/init.d/smb) içinde

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

deyimini şu satırla değiştiririz:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

Böylece, Samba tarafından denetlenen seçili dosya sistemi nesneleri, sistem açılışında taranacaktır.

Önemli SCEP mekanizmaları

Nesne İşleme İlkesi

Nesne İşleme İlkesi mekanizması, taranan nesneler için durumlarına göre filtreleme sağlar. Bu işlevsellik, aşağıdaki yapılandırma seçeneklerini temel alır:

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Bu seçeneklerle ilgili ayrıntılı bilgi için lütfen *scep.cfg(5)* el kitabı sayfasına bakın.

Her işlenen nesne önce, *'action_av'* seçeneğinin yapılandırmasına göre işlenir. Bu seçenek *'accept'* (veya *'defer'*, *'discard'*, *'reject'*) olarak ayarlanırsa, nesne kabul edilir (ya da ertelenir, atılır, reddedilir). Seçenek *'scan'* olarak ayarlanırsa, nesne virüs sızıntılarına karşı taranır ve *'av_clean_mode'* seçeneği *'yes'* olarak ayarlanırsa nesne de temizlenir. Ayrıca nesne işlemeyi daha ayrıntılı değerlendirmek için *'action_av_infected'*, *'action_av_notscanned'* ve *'action_av_deleted'* yapılandırma seçenekleri dikkate alınır. Bu üç eylem seçeneğinin sonucunda bir *'accept'* eylemi uygulandıysa, nesne kabul edilir. Aksi takdirde, nesne engellenir.

Kullanıcıya Özel Yapılandırma

Kullanıcıya Özel Yapılandırma mekanizmasının amacı, daha yüksek özelleştirme ve işlevsellik düzeyi sağlamaktır. Bu, sistem yöneticisinin dosya sistemi nesnelerine erişen kullanıcıyı temel alarak SCEP antivirus tarayıcı parametrelerini tanımlamasına olanak sağlar.

Bu işlevselliğin ayrıntılı bir açıklaması, *scep.cfg(5)* el kitabı sayfasında bulunabilir. Bu bölümde, kullanıcıya özel yapılandırmanın yalnızca kısa bir örneğini sağlayacağız.

Bu örnekte hedef, /home dizininin altında takılı bir dış diske ilişkin ON_OPEN ve ON_EXEC erişim olaylarını denetlemek için *scep_dac* modülünü kullanmaktır. SCEP yapılandırma dosyasının **[fac]** bölümünde modül yapılandırılabilir. Aşağıya bkz:

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Tek bir kullanıcıya ilişkin tarama ayarlarını belirtmek için *'user_config'* parametresi, tek tek tarama kurallarının depolanacağı özel yapılandırma dosya adını belirtmelidir. Burada gösterilen örnekte, özel yapılandırma dosyası *'scep_dac_spec.cfg'* olarak adlandırılır ve SCEP yapılandırma dizini içinde bulunur (Bu dizin, işletim sisteminize bağlıdır. Lütfen Terminoloji ve kısaltmalar sayfasına bakın).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

[fac] bölümünde *'user_config'* dosya parametresi belirtildikten sonra, SCEP yapılandırma dizininde *'scep_dac_spec.cfg'* dosyası oluşturulmalıdır. Son olarak istediğiniz tarama kurallarını ekleyin.

```
[username]
action_av = "reject"
```

Özel bölümün en üst kısmına, tek tek kuralların uygulanacağı kullanıcı adını girin. Bu yapılandırma, dosya sistemine erişmeye çalışan diğer tüm kullanıcıların normal şekilde işlemden geçirilmesine olanak sağlar. Başka bir deyişle, erişimi reddedilecek (engellenecek) *'username'* kullanıcısı dışında diğer kullanıcıların eriştiği tüm dosya sistemi nesneleri, sızıntılara karşı taranacaktır.

Zamanlayıcı

Zamanlayıcının işlevleri arasında, zamanlanan görevlerin belirtilen bir zamanda veya belirli bir olay olduğunda çalıştırılması, önceden tanımlı yapılandırma ve özellikler ile görevlerin yönetilmesi ve başlatılması, vb. yer alır. Başlatma tarih ve saatlerini etkilemek ve görev yürütme sırasında özel profillerin kullanımını sunarak görevlerin uygulamasını geliştirmek için görev yapılandırması ve özellikleri kullanılabilir.

'scheduler_tasks' seçeneği varsayılan olarak açıklamalı olduğundan, varsayılan zamanlayıcı yapılandırmasının uygulanmasına neden olur. SCEP yapılandırma dosyasında tüm parametreler ve görevler noktalı virgülle ayrılır. Diğer tüm noktalı virgüller (ve ters eğik çizgiler), ters eğik çizgi atlatmalı olmalıdır. Her görevin 6 parametresi vardır ve sözdizimi şu şekildedir:

- id - Benzersiz sayı.
- name - Görev açıklaması.
- flags - Belirtilen zamanlayıcı görevini devre dışı bırakmak için özel bayraklar burada ayarlanabilir.
- failstart - Zamanlanan tarihte görev çalıştırılamadığında ne yapılacağını bildirir.
- datespec - 6 (crontab gibi yıl uzatmalı) alan, yinelenen tarih veya bir olay adı seçeneği olan düzenli bir tarih belirtimi.
- command - Ardından '@' önekinin bulunduğu bağımsız değişkenlerin veya özel komut adının geldiği bir komutun mutlak yolu olabilir. (örn. anti-virus güncellemesi: *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Aşağıdaki olay adları, datespec seçeneğinin yerine kullanılabilir:

- start - Daemon başlatması.
- startonce - Daemon başlatması ancak en fazla günde bir defa.
- engine - Başarılı altyapı güncellemesi.
- login - Web arabirimi oturum açma başlatması.
- threat - Tehdit algılandı.
- notscanned - Dosya taranmadı.

Geçerli zamanlayıcı yapılandırmasını görüntülemek için, Web arabirimi'ni kullanın veya aşağıdaki komutu çalıştırın:

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Zamanlayıcının ve parametrelerinin tam açıklaması için, *scep_daemon(8)* el kitabı sayfasının Zamanlayıcı bölümüne bakın.

Web Arabirimi

Web arabirimi, SCEP güvenlik sistemlerinin kullanıcı dosya yapılandırmasına ve yönetimine olanak sağlar. Bu modül ayrı bir aracıdır ve açıkça etkinleştirilmelidir. *Web Arabirimi*'ni hızlı şekilde yapılandırmak için, SCEP yapılandırma dosyasında aşağıdaki seçenekleri ayarlayın ve SCEP daemon'ı yeniden başlatın:

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

İtalik metni kendi değerlerinizle değiştirin ve tarayıcınızı *'https://adres:bağlantı noktası'* adresine yönlendirin (https'yi unutmayın). *'Kullanıcı adı/parola'* ile oturum açın. Temel kullanım talimatları, yardım sayfasında bulunabilir ve *scep_wwwi* ile ilgili teknik ayrıntılar da *scep_wwwi(1)* el kitabı sayfasında bulunabilir.

Web arabirimi, SCEP daemon'a uzaktan erişmenize ve kolayca dağıtmanıza olanak sağlar. Bu güçlü yardımcı program, yapılandırma değerlerinin okunmasını ve yazılmasını kolaylaştırır.

Şekil 6-1. System Center Endpoint Protection - Ana Sayfa ekranı.

System Center Endpoint Protection ürününün web arabirimi penceresi iki ana bölüme ayrılır. Seçilen menü seçeneğinin ve ana menünün içeriklerini görüntüleme görevi gören birincil pencere. En üstteki bu yatay çubuk, aşağıdaki ana seçenekler arasında gezinmenize olanak sağlar:

- **Ana Sayfa** - Temel sistem ve Microsoft ürün bilgilerini sağlar
- **Yapılandırma** - System Center Endpoint Protection sistem yapılandırmasını burada değiştirebilirsiniz.
- **Denetim** - Basit görevler çalıştırmanıza ve scep_daemon tarafından işlenen nesneler hakkındaki genel istatistikleri görüntülemenize olanak tanır.
- **Yardım** - System Center Endpoint Protection web arabirimi için ayrıntılı kullanım talimatlarını sağlar.
- **Oturumu Kapat** - geçerli oturumunuzu sonlandırmak için kullanılır

Önemli: Web arabiriminin **Yapılandırma** bölümünde herhangi bir değişiklik yaptıktan sonra, yeni ayarlarınızı kaydetmek için **Değişiklikleri kaydet** düğmesini tıklattığınızdan emin olun. Ayarlarınızı uygulamak için, sol bölmedeki **Değişiklikleri uygula** seçeneğini tıklatarak SCEP daemon'ı yeniden başlatmanız gerekir.

Gerçek zamanlı koruma yapılandırması örneği

SCEP'yi yapılandırabilmenizin iki yolu vardır. Örneğimizde, Önyüklemeli LIBC kitaplığı kullanılarak gerçek zamanlı koruma bölümünde açıklanan Erişim Denetleyicisi modülünü ayarlamak için bunlardan herhangi birinin nasıl kullanılacağını göstereceğiz. Size en uygun seçeneği belirleyebilirsiniz.

- SCEP yapılandırma dosyasını kullanma:

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Web arabirimini kullanma:

Şekil 6-3. SCEP - Yapılandırma > Aktif koruma.

Web arabiriminde ayarları değiştirirken her zaman **Değişiklikleri kaydet**'i tıklatarak yapılandırmanızı kaydettiğinizden emin olun. Yeni değişikliklerinizi uygulamak için, **Yapılandırma** bölümleri panelinde **Değişiklikleri uygula** düğmesini tıklatın.

İsteğe bağlı tarayıcı

Bu bölüm, virüs taraması yapmak için İsteğe bağlı tarayıcının nasıl çalıştırılacağına ilişkin bir örnekten oluşur:

- **Denetim > İsteğe Bağlı Tarama** seçeneğine gidin.
- Taramak istediğiniz dizinin yolunu girin
- **Dosyaları tara** düğmesini tıklatarak komut satırı tarayıcısını yürütün

Şekil 6-4. SCEP - Denetim > İsteğe Bağlı tarayıcı.

Microsoft Komut satırı tarayıcısı otomatik olarak arka planda çalışacaktır. Taramanın ilerleme durumunu görüntülemek için **Görüntüle** bağlantısını tıklatın. Yeni bir tarayıcı penceresi açılır.

Zamanlayıcı

SCEP yapılandırma dosyası (Zamanlayıcı bölümüne bakın) aracılığıyla veya web arabirimini kullanarak zamanlayıcı görevlerini yönetebilirsiniz.

Şekil 6-5. SCEP - Genel > Zamanlayıcı.

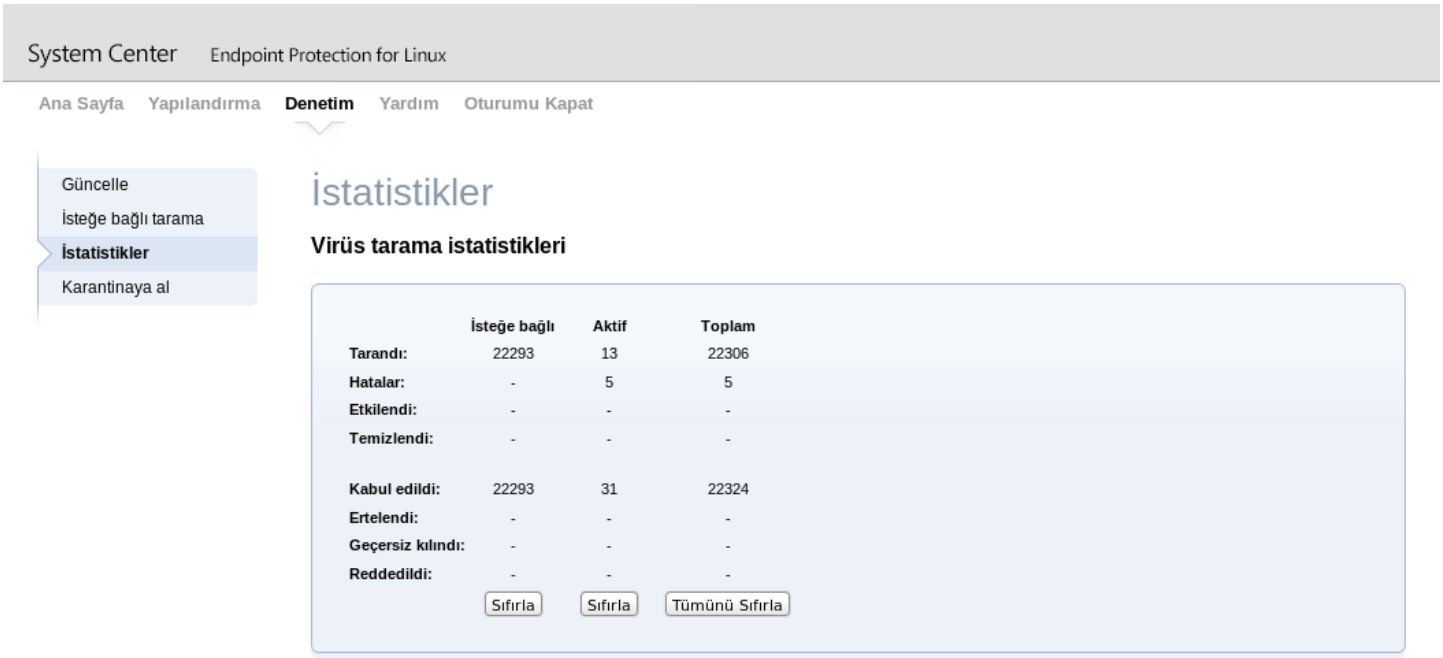
Zamanlanan bir görevi etkinleştirmek/devre dışı bırakmak için onay kutusunu tıklatın. Varsayılan olarak, aşağıdaki zamanlanan görevler görüntülenir:

- **Günlük bakımı** - Program, sabit disk alanından tasarruf etmek için eski günlükleri otomatik olarak siler. Zamanlayıcı, günlüklerin birleştirilmesini başlatır. Bu işlem sırasında tüm boş günlük girdileri kaldırılır. Böylece günlüklerle daha hızlı çalışılabilir. Günlükler çok sayıda girdi içeriyorsa, bu iyileştirme daha belirgin olarak gözlenir.
- **Başlangıçta dosya denetimi** - Virüs imza veritabanının başarıyla güncellenmesinin ardından belleği ve çalışan hizmetleri tarar.
- **Haftalık tarama** - Tüm dosya sistemini haftalık olarak tarar (varsayılan olarak Pazartesi günleri 2:00'da). Bu görev kullanıcı tarafından özelleştirilebilir.
- **Düzenli otomatik güncelleme** - System Center Endpoint Protection ürününün düzenli olarak güncellenmesi, bilgisayarınızda maksimum güvenlik düzeyine ulaşmak için en iyi yöntemdir. Daha fazla bilgi için bkz. SCEP güncelleme yardımcı programı.
- **Tehdit bildirimi** - Varsayılan olarak her tehdit, sistem günlüğüne kaydedilir. Ayrıca SCEP, sistem yöneticisine tehdit algılamasıyla ilgili e-postayla bildirim göndermek için bir dış (bildirim) komut dosyası çalıştıracak şekilde yapılandırılabilir.

İstatistikler

Tüm etkin SCEP aracıları için istatistikleri buradan görüntüleyebilirsiniz. **İstatistikler** özeti her 10 saniyede bir yenilenir.

Şekil 6-6. SCEP - Denetim > İstatistikler.



Günlüğe kaydetme

SCEP, syslog aracılığıyla sistem daemon günlüğe kaydetme işlevi sağlar. *Syslog*, program iletilerinin günlüğe kaydedilmesine yönelik bir standart olup ağ ve güvenlik olayları gibi sistem olaylarını günlüğe kaydetmek için kullanılabilir.

İletiler bir olanağa başvurur:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

İletilere, ileti göndereni tarafından bir öncelik/düzey atanır:

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

Bu bölümde, sistem günlüğü günlüğe kaydetme çıkışının nasıl yapılandırılacağı ve okunacağı açıklanmaktadır. *'syslog_facility'* seçeneği (*'daemon'* varsayılan değeri), günlüğe kaydetme için kullanılan sistem günlüğü olanağını tanımlar. Sistem günlüğü ayarlarını değiştirmek için SCEP yapılandırma dosyasını düzenleyin veya Web arabirimi'ni kullanın. Günlüğe kaydetme sınıfını değiştirmek için *'syslog_class'* parametresinin değerini değiştirin. Yalnızca sistem günlüğünü biliyorsanız bu ayarları değiştirmenizi öneririz. Örnek bir sistem günlüğü yapılandırması için aşağıya bakın:

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

Günlük dosyasının adı ve konumu, sistem günlüğü yükleme ve yapılandırmanıza bağlıdır (örn. rsyslog, syslog-ng, vb.). syslog çıkış dosyaları için standart dosya adları örneğin, *'syslog'*, *'daemon.log'*, vb.'dir. Sistem günlüğü etkinliğini izlemek için, konsoldan aşağıdaki komutlardan birini çalıştırın:

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Önemli: Linux SCEP ürününün System Center Operations Manager kullanımıyla izlenmesi işleminin düzgün çalışması için öncelikle SCEP yapılandırma dosyasında 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.

SCEP Güvenlik sistemi güncellemesi

SCEP güncelleme yardımcı programı

System Center Endpoint Protection uygulamasının etkinlik düzeyini korumak için, virüs imza veritabanı güncel tutulmalıdır. *scep_update* yardımcı programı özellikle bu amaç için geliştirilmiştir. Ayrıntılar için *scep_update(8)* el kitabı sayfasına bakın. Sunucunuzun HTTP proxy aracılığıyla Internet'e erişmesi durumunda, *'proxy_addr'*, *'proxy_port'* ek yapılandırma seçenekleri tanımlanmalıdır. HTTP proxy'ye erişim için bir kullanıcı adı ve parola gerekiyorsa, bu bölümde *'proxy_username'* ve *'proxy_password'* seçenekleri de tanımlanmalıdır. Bir güncelleme başlatmak için aşağıdaki komutu girin:

@SBINDIR@/scep_update

Son kullanıcı için olası en yüksek güvenliği sağlamak üzere Microsoft ekibi sürekli olarak dünyanın dört bir yanından virüs tanımlarını toplar; virüs imza veritabanına çok kısa aralıklarla yeni desenler eklenir. Bu nedenle, düzenli aralıklarla güncellemelerin başlatılmasını öneririz. Güncellemelerin sıklığını belirtebilmek için, SCEP yapılandırma dosyasının **[global]** bölümündeki *'scheduler_tasks'* seçeneğinde *'@update'* görevini yapılandırmanız gerekir. Güncelleme sıklığını ayarlamak için Zamanlayıcı'yı da kullanabilirsiniz. Virüs imza veritabanını başarıyla güncellemek için SCEP daemon'ın çalışır durumda olması gerekir.

SCEP güncelleme işlemi açıklaması

Güncelleme işlemi iki aşamadan oluşur: İlk olarak, önceden derlenmiş güncelleme modülleri Microsoft sunucusundan yüklenir.

Güncelleme işleminin ikinci aşaması, yerel yansıtmada depolananlardan System Center Endpoint Protection tarayıcısı tarafından yüklenebilen modüllerin derlenmesidir. Genellikle şu SCEP yükleme modülleri oluşturulur: yükleyici modülü (em000.dat), tarayıcı modülü (em001.dat), virüs imza veritabanı modülü (em002.dat), arşiv destek modülü (em003.dat), gelişmiş sezgisel tarama modülü (em004.dat), vb. Modüller şu dizinde oluşturulur:

@BASEDIR@

Bize bildirin

Bu kılavuzun, System Center Endpoint Protection yüklemesi, yapılandırması ve bakımına yönelik gereksinimleri tamamen anlamanızı sağladığını umuyoruz. Ancak hedefimiz, belgelerimizin kalite ve etkinlik düzeyini sürekli olarak artırmaktır. Bu Kılavuzda herhangi bir bölümün belirsiz veya eksik olduğunu düşünüyorsanız, lütfen Müşteri Desteği ile iletişim kurarak bunu bize bildirin:

support.microsoft.com

En yüksek düzey desteği sağlamaya kendimizi adadık ve bu ürünle ilgili herhangi bir sorun yaşamanız durumunda size yardımcı olmayı umuyoruz.

Ek A. PHP Lisansı

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.