

# epati

## SysLog Ayarları

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı  
Kılavuzlar

## SysLog Ayarları

Sunucu sistem loglarının kayıt edileceği sunucunun/sunucuların eklendiği bölümdür. 26 farklı log çeşidi ve 7 farklı log formatını desteklemektedir. Tercih edilen ham veya yapısal log formatlarında kullanıcının sağlayacağı log toplayıcısına veya SIEM'e iletilebilmektedir.

Syslog Ayarları

Yenile Ekle

XLS CSV PDF

Göster/Gizle

Sayfa Başı Kayıt Sayısı

Tümünü

Filtrele

Filtreyi Temizle

#	Durum	Açıklama	Log Çeşitleri	Filtre Metni	Gönderim Formatı	Sunucu Adresi	Protokol	Port	İşlemler
1	Aktif	Antispam	Antispam Logları		CEF (Common Event Format)	10.2.4.55	UDP	514	Düzenle Sil
2	Aktif	All Logs	Antispam Logları Arayüz Erişimi Yasaklanan IPler Balküğü Logları Cluster Logları DHCP Olay Logları DNS Filtreleme Logları DoS / Flood Engelleme Logları Güvenlik Duvarı - Antispoof Logları Güvenlik Duvarı - DMZ Trafik Logları Güvenlik Duvarı - Dinamik NAT Trafik Logları Güvenlik Duvarı - Global NAT Trafik Logları Güvenlik Duvarı - Güvenlik Kuralları Trafik Logları Güvenlik Duvarı - Hedefe Göre NAT Trafik Logları Güvenlik Duvarı - Hotspot Varsayılan Engel Logları Güvenlik Duvarı - Port Yönlendirme Trafik Logları Güvenlik Duvarı - Statik NAT Trafik Logları Güvenlik Duvarı - Trafik Normalizasyonu Güvenlik Duvarı - Varsayılan Kural Logları Hotspot Logları Http(s) Sunucu Yönlendirme Logları IPsec Trafik Logları Karadelik Servisi Logları PPP Debug Logları PPP Logları RADIUS Logları SSH Denetimi Logları SSH Koruma Servisi Logları SSH ve Konsol Oturum Logları Saldırı Tespit ve Önleme (IPS) Logları Uygulama Güvenliği Logları VPN - IPsec VPN Logları VPN - PPTP / L2TP Logları VPN - SSL VPN Logları Web Arayüzü Logları Web Erişim Logları Web Filtreleme - Sayfa Yasaklama Logları Web Filtreleme - İçerik ve Antivirüs Tarama Logları Web Oturum Logları Web Uygulama Güvenliği Logları Yönetim Paneli Erişim Trafik Logları	Ham Kayıt	10.2.4.50	UDP	514	Düzenle Sil	

&lt; 1 &gt;

Göt.

### Syslog Ayarları - Yeni Kayıt

X

Durum

Aktif 

Açıklama

Log Çeşitleri

Seçiniz...

Filtre Metni

Gönderim Formatı

Ham Kayıt

Adres Ailesi

 IPv4  IPv6

Sunucu Adresi

IPv4

Protokol

UDP

Port

514

İptal

Kaydet

## Syslog Ayarları - Yeni Kayıt



Durum	<input checked="" type="checkbox"/> Aktif
Açıklama	<input type="text"/>
Log Çeşitleri	<input type="text" value="Seçiniz..."/>
Filtre Metni	<input type="text"/>
Gönderim Formatı	<input type="text" value="Antispam Logları"/>
Adres Ailesi	<input type="text" value="Arayüze Erişimi Yasaklanan IPIler"/>
Sunucu Adresi	<input type="text" value="Cluster Logları"/>
Protokol	<input type="text" value="UDP"/>
Port	<input type="text" value="514"/>

İptal

Kaydet

## Syslog Ayarları - Yeni Kayıt



Durum	<input checked="" type="checkbox"/> Aktif
Açıklama	<input type="text"/>
Log Çeşitleri	<input type="text" value="Seçiniz..."/>
Filtre Metni	<input type="text"/>
Gönderim Formatı	<input type="text" value="Ham Kayıt"/>
Adres Ailesi	<input type="text" value="Ham Kayıt"/>
Sunucu Adresi	<input type="text" value="CEF (Common Event Format)"/>
Protokol	<input type="text" value="EWM (Enterprise Wide Message Model)"/>
Port	<input type="text" value="GELF (Graylog Extended Log Format)"/>

İptal

Kaydet

ALAN	AÇIKLAMA
Açıklama	Syslog ayarının açıklaması yazılır.
Log Çeşitleri	Log çeşitleri seçilir ve seçilen log çeşitleri Syslog sunucuya gönderilir.
Filtre Metni	Gönderilecek loglara uygulanacak filtrelerin yazıldığı alandır.
Gönderim Formatı	Desteklenen 7 farklı log formatından biri seçilerek log toplayıcısına veya SIEM'e iletilebilmektedir.
Adres Ailesi	IPv4 ya da IPv6 adres ailesi seçilir.
Server Adresi	Logların tutulacağı sunucuya ait IP adresi yazılır.
Protokol	Logların gönderilmesinde kullanılacak protokolün seçildiği alandır.
Port	Log'un hangi port numarasını kullanacağı yazılır.

## Gönderim Formatı

ALAN	AÇIKLAMA
Ham Kayıt	Gelen veriler işlenmeden ham olarak gönderildiği formattır.
CEF (Common Event Format)	Ortak olay biçimi (CEF) ArcSight bir günlük ve denetim dosya biçimidir. En gerekli bilgileri sunarak birden fazla cihaz türlerini çözmek için tasarlanmıştır genişletilebilir, metin tabanlı bir formattır.
EWMM (Enterprise Wide Message Model)	Kuruluşların bilgisayar sistemleri arasında semantik olarak kesin mesajlar göndermesine izin veren yayınlanmış kurumsal çapında standartlar kümesidir.
GELF (Graylog Extended Log Format)	Graylog Genişletilmiş Günlük Biçimi (GELF), klasik düz Syslog'un tüm eksikliklerini gidermek için oluşturulmuş benzersiz bir günlük biçimidir. Bu kurumsal özellik, yapılandırılmış olayları her yerden toplamanızı ve ardından bunları göz açıp kapayıncaya kadar sıkıştırmanızı ve parçalamanızı sağlar.
JSON (Javascript Object Notation)	JSON (JavaScript nesne gösterimi) hafif bir veri değişim biçimidir. İnsanların okuması ve yazması kolaydır. Makinelerin ayrıştırılması ve üretilmesi kolaydır.
WELF (WebTrends Enhanced Log File Format)	WELF Başvurusu, WebTrends endüstri standardı günlük dosyası değişim biçimini tanımlar.
CIM (Common Information Model)	Ortak Bilgi Modeli (CIM), bir BT ortamındaki yönetilen öğelerin ortak bir nesne kümesi ve bunlar arasındaki ilişkiler olarak nasıl temsil edildiğini tanımlayan açık bir standarttır.



İeknopark İdarı Bınası Kat: 4 No: 411  
Posta Kodu: 33343 Yenişehir / MERSİN

+90 324 361 02 33  
+90 324 361 02 39

