



BİLGİ TEKNOLOJİLERİ K İ T A P L A R I

ISA Server 2004 ® Sistem Yöneticisi'nin El Kitabı

Microsoft ISA Server®

Microsoft Internet Security and Acceleration (ISA) Server, Microsoft'un kurumsal şirketlerin network güvenliğini sağlamak için geliştirilmiş paket ve uygulama katmanlı bir firewall, VPN ve Web Caching (proxy) çözümlerinde kullanılan önemli bir server yazılımıdır.

Hemen hemen tüm şirketler, çalışanları için değişik düzeylerde Internet'e girmelerini istemektedir. ISA Server, kullanıcıların **Internet'e güvenli olarak erişmesini sağlar**. Bunun dışında birçok şirket uzak kullanıcılarının (remote user) şirket network'üne erişmesini de istemektedir. Örnek olarak şubelerden yapılan uzak bağlantılarını gösterebiliriz. Ayrıca birçok şirket kendi Web sitelerini kendi network'ü içinde host etmektedir. Bu durumda Web server'a erişimin güvenli olması gerekir. İşte ISA Server, geliştirilmiş paket ve uygulama katmanlı firewall, Web Caching ve VPN çözümleriyle şirket network'lerinin güvenliğini sağlar.

ISA Server 2004, birçok firewall'un belirleyemediği HTTP gibi internet protokollerinin de olarak filtrelemesini gerçekleştirmektedir.

ISA Server 2004, özellikle Active Directory, RRAS, Share Point Portal 2003, Outlook Web Access, Microsoft Outlook gibi Microsoft ürünleriyle birlikte çalışmalara da tam koruma sağlamaktadır.

ISA Server 2004'ün Yenilikleri

ISA Server 2004, gelişmiş çok katmanlı bir firewall, VPN Server, Web Proxy server ve cache'leme özellikleri ile şirket network'ü ve internet arasında güvenli bir iletişim ortamı sağlamaktadır.

Özellikleri:

- **Çok katmanlı paket denetimi**
- **Uygulama-katmanı filtreleme**
- **Birleşik Firewall ve VPN Server**
- **Birden çok network desteği**

Çok katmanlı paket denetimi

ISA Server 2004, üzerinden geçen her paketi gelişmiş çok katmanlı firewall özelliği sayesinde inceler. Bu işi paket filtreleme, stateful filtreleme ve uygulama filtreleme özellikleri sayesinde gerçekleştirmektedir. Bu özelliği ile ayrıca IIS, Exchange Server, Microsoft Share Point ve diğer tüm şirket içi network kaynaklarını virüs, trojan ve yetkisiz kullanıcılara karşı korumada da yardımcı olmaktadır.

Uygulama-katmanı filtreleme

Uygulama katmanında çalışan prosesler güvenlik tehlikesi oluşturmaktadır. ISA Server 2004 geliştirilmiş application-layer filtreleme özelliği ile Internet'ten gelen saldırılara karşı yüksek düzeyde koruma sağlamaktadır. Örnek olarak HTTP trafiğinin ayrıntılı olarak filtrelenmesini gösterebiliriz.

Birleşik firewall ve VPN Server

ISA Server 2004 üzerinde firewall, Web caching ve VPN Server özellikleri birleştirilmiştir. Ayrıca, ISA Server 2004, şirket network'üne giriş yapan kullanıcıların ve geliştirilmiş Firewall ve VPN Server fonksiyonlarının yönetimini tek bir noktadan yapılmasını sağlar.

Birden Çok Network'ü Desteklemek

ISA Server 2004, birden çok network'ün güvenlik gereksinimlerini ve tüm networkler arası trafiğin firewall kurallarına göre kontrol edilmesini sağlar.

ISA Server 2004'ün Edition'ları

ISA Server 2004 iki versiyonu (editions) vardır.

- **Standart Edition**
- **Enterprise Edition**

Her iki Edition'da bulunan özellikler çok benzerdir. Ancak Enterprise Edition, Load Balancing ve Cache Array Routing Protocol (CARP) gibi birden çok ISA Server desteğine sahiptir.

Tek bir ISA Server'ın tipik bir firewall ve bir Web Proxy server senaryolarında kullanılacağı durumlarda Standart Edition tercih edilmelidir. Örneğin, bir şirket için Web Proxy Server ve firewall olarak tek bir ISA Server kuruyorsanız ya da merkezi ofistekine ek olarak bir ya da daha çok şubede ISA Server kurulacaksa yine **Standart Edition** tercih edilebilir.

Bununla beraber, her bir rol için **birden çok server** kurulacaksa, Enterprise Edition tercih edilir. Örneğin; merkez ofiste Web Proxy ve caching server olarak kurulmuş birden çok serverın kullanıldığı geniş bir organizasyon için Enterprise Edition kullanılır. ISA Server 2004, Enterprise Edition, birden fazla server üzerinde yaratılmış ve paylaşılmış Web Caching'i destekler. Bu özellik için CARP (Cache Array Routing Protocol) ile sağlanır.

Sistem Gereksinimleri

ISA Server 2004'ün kurulumu yapabilmek için öncelikle işletim sistemi ve doğru bir sistem konfigürasyonuna gereksinim vardır. ISA Server 2004, yalnızca Windows Server 2000 ve **Windows Server 2003** işletim sistemlerine kurulabilmektedir.

ISA Server 2004, Windows 2000 Server işletim sistemine yüklenebilmesi için; Microsoft Windows 2000 Service Pack 4, Microsoft Internet Explorer 6 ve gerekli yamaların (patch) yüklenmesi gerekir.

NOT: ISA Server 2004, Windows Server 2000 işletim sistemi üzerine yüklendiğinde "L2TP IPsec pre-shared key" konfigürasyonu ve "RADIUS policy" kullanıldığı zaman VPN Client'lar için Quarantine Mode'u desteklememektedir.

ISA Server 2004 Sistem Gereksinimleri

ISA Server 2004'ün çalışabilmesi için gerekli (minimum) özellikler:

- 500 MHz ya da daha gelişmiş CPU
- 256 MB RAM
- İç network ile iletişim için network kartı (network interface card)
- ISA Server ile bağlanan her network için bir adet network interface card
- 150 MB boş disk alanı (NTFS Dosya Sistemi ile formatlanmış)

Kurulum

ISA Server 2004 kurulumuna ISA Server 2004 kaynak CD'si ile başlanır. **ISAAUTORUN.EXE** ya da otomatik başlatma ile ISA Server 2004 kurulumuna başlanır.

>ISAAUTORUN.EXE

Kurulum programının ilk ekranında ISA Server 2004'ün kurulumu ve ISA Server 2000'den taşınması (migration) için bölümler yer alır:

- **Install ISA Server 2004**
- **Run Migration Wizard**

"Install ISA Server 2004" ile ISA Server 2004 kurulumuna başlanır. Sırasıyla kurulum şekli, bileşenler, ISA Server'ın yeni bir kurulum için mi olduğu yoksa mevcut bir ISA Server'a ek bir ISA Server mı kurulacak ayrıca internal network'e ilişkin bilgiler sorulur.

Client Kurulumu

Firewall Client olarak yapılandırılmış bir bilgisayar ISA Server'a bağlandığında, Firewall client, Server üzerindeki yeni konfigürasyon ayarlarını kontrol eder. Bu da **ISA Server Management** konsolunu kullanarak **Firewall Client** ayarlarını değiştirebilme anlamına gelmektedir.

Yapılan değişiklikler daha sonra client'a uygulanır. Yapılan bir değişiklik client bağlandığında uygulanır ya da client bilgisayar her altı saatte bir konfigürasyon dosyasını güncellemek üzere firewall servisine bağlandığında bu değişiklikleri günceller.

ISA Server Management konsolundaki **Firewall Client** ayarları:

Application Settings: Bu ayar Firewall Client'ın özel uygulamalar için ISA Server'a nasıl bağlanabileceğini tanımlamaktadır.

Internal network and local domains: Bu ayarlar, firewall client'ın lokal olarak tanıdığı IP adres setlerini ve domainleri tanımlamaktadır. Firewall client bu IP adres aralığındaki kaynaklara ISA Server üzerinden değil, direk olarak erişmesi için gerekli ayarlamaların yapıldığı yerdir.

Automatic Discovery: Bu seçeneğin aktif hale getirilmesi firewall client'ların otomatik olarak uygun ISA Server bilgisayarı bulması sağlanmış olmaktadır.

Firewall Client'lar için Web Browser Ayarları: Firewall Client uygulaması Web Proxy ayarlarını otomatik olarak güncelleyebilmektedir. Bu ayarlar, firewall client update edildiğinde ISA Server'dan alınabilir.

Firewall Konfigürasyonu

Firewall şirket network'ünü ya da bir bölümünü Internet'ten korumak için kullanılır. Genellikle network perimeter'de kurulan firewall'ların ana amacı Internet gibi public bir network'ten şirket network'üne erişimin engellenmesidir. ISA Server'ın Active Directory entegrasyonunu olması kullanıcıların kontrolünde çok büyük yararlar sağlar. Örneğin şirketin bir Web server'ı olabilir ve belli kullanıcılar Internet üzerinden bu server'a erişmek isterler. Bunun yanı sıra, Firewall trafiği yalnızca Internet Web server'a erişmek üzere ve belli kullanıcılar için kısıtlayabilir.

ISA Server, firewall fonksiyonu ile varsayım olarak bağlı olduğu network (iç network, perimeter network) ile Internet arasındaki trafiği filtreler. ISA Server network trafiğini

bloklamak ya da izin vermek için üç tür filtreleme yapar: **paket filtreleme**, **stateful filtreleme** ve **application-katmanı filtreleme**.

Kurallar

Tanımlanan bir Access Rule'un farklı bileşenleri (elemanları) vardır. **ISA Server Management** konsolu ve ilgili **Toolbox** aracılığıyla bu özellikler düzenlenebilir.

Access rule özellikleri:

- **Protocols**
- **Users**
- **Content Types**
- **Schedules**
- **Network objects**

Protocols (Protokoller)

Bu rule elemanı access rule'da kullanılacak protokollerin tanımlanmasını sağlar. Örneğin, bir ya da daha çok protokol üzerinde erişime izin verebilir ya da engellenir.

Birçok durumda, client'ın kullandığı protokole dayanarak internet erişimine izin veren ya da engelleyen bir access rule oluşturmak istenebilir. Bunun için, ISA server tarafından sağlanan protokollerden birini kullanabilir ya da yeni protokol tanımlaması oluşturulur.

ISA Server, access rule oluştururken çok sayıda protokollerden istenilenleri kullanılabilir. Birçok durumda, önceden yapılandırılmış protokollerle bir access rule oluşturulurken, istendiğinde ek protokol tanımlamaları yapılır.

Örneğin, belirli bir port numarasını kullanan özel bir uygulama kullanıyor olabilirsiniz. Bu port numarasını kullanan bir protokol elemanı oluşturabilir ve daha sonra bu protokolü bir access rule 'da kullanabilirsiniz.

Yeni bir protokol kuralı yaratmak için;

1. **ISA Server Management** 'tan **Firewall Policy**'i tıklayın.

Toolbox tabında, **Protocols**'u tıklayın.

2. **New**'i tıklayın ve daha sonra **Protocol**'ü ya da **RPC Protocol**'ü tıklayın. Örneğin, **Protocol**'ü seçin.

3. **Welcome to the New Protocol Definition Wizard**'da , **Protocol definition name:** kutusunda protokol adını girin. **Next**'i tıklayın.

4. **Primary Connection Information** sayfasında, protokol için protokol tipi, direction (yön) ve port numaralarını yapılandırmak için **New**'i tıklayın.

5. **Secondary Connections** sayfasında, secondary (ikincil) bağlantı kullanmak isteyip istemediğinizi seçin. Protokol secondary (ikincil) bağlantıya gereksinim duyuyorsa, **Yes**'i tıklayın ve daha sonra secondary bağlantı için protokol türü, direction ve port numaralarını yapılandırmak için **New**'i tıklayın. Ardından **Next**'ile konfigürasyonu tamamlayın.

Users (Kullanıcılar)

Bu rule elemanı kuralların uygulanacağı ya da kurallardan muaf tutulacak (hariç tutulacak) kullanıcıların tanımlanmasını sağlar. Örneğin, bir şirket içindeki geçici çalışanlar dışındaki tüm kullanıcılara internet erişimi sağlayan bir erişim kuralı (access rule) oluşturmak istenebilir.

Kimlik denetimi bir Active Directory sistemi ya da RADIUS server kullanarak, **Domain Users** grubuna internet erişim izni verip, örneğin **FC-Saticilar** diye grubu engelleyen bir access rule

yapılandırılabilir.

User Set

Kullanıcıların ya da grupların internet kaynaklarına erişmesini kısıtlamak için bir user elemanının yaratılması gerekmektedir. Bu kullanıcı ya da gruplar için hazırlanmış bir Access rule var ise kimlik denetiminin doğrulanması gerekmektedir. Kimlik denetimi başarılı bir şekilde yapıldıktan sonra izin verildiği ölçüde internet kaynaklarına erişimi yapılır.

User set'ler ile karma kimlik denetimi yapılabilir. Örneğin, bir kullanıcıya Windows tabanlı kimlik doğrulaması yapılırken, diğer bir kullanıcı bir RADIUS server kimlik doğrulaması bir diğer kullanıcı SecurID kimlik doğrulaması ile giriş yapabilmektedir.

ISA Server kurulumu sonrası üç tür **user set** oluşur.

All authenticated Users

All Users

System and Network Service

All authenticated Users

Bu User set'i, tüm authentication tiplerini kullanan tüm kullanıcıları içerir. VPN-SecureNAT clientları bu user set'e dahil değildir.

All Users

Bu user set'i, aynı authentication tipini kullanan ve authentication olmamış kullanıcıları içerir.

System and Network Service

Bu user set'i ISA Server'in çalıştığı bilgisayardaki local system service ve network service kullanıcılarını içerir. Bu user set, system policy rules'ta tanımlıdır.

Yeni bir **User set** oluşturmak için aşağıdaki yol izlenebilir:

1. Microsoft **ISA Server Management** konsolundan **Firewall Policy**'e tıklayın.
2. **Toolbox** tabından, **Users**'a tıklayın.
3. **New** tuşuna basın. **Welcome to the New User Sets Wizard** penceresinde **User set name** kutusuna bir isim yazarak **Next**'i tıklayın. Örneğin FarukCubukcu-Kural1.
4. **User** sayfasında, **Add**'i tıklayın ve üç seçenekten birini seçip **Add**'i tıklayın. Bunlar;
 - a. **Windows Users and Groups**. Bu kullanıcı grubu, ISA Server bilgisayardaki local kullanıcı hesapları ya da bir Windows domainindeki kullanıcı ve grup hesaplarını gösterir.
 - b. **RADIUS**. RADIUS server name space'inde belirtilmiş kullanıcı ve grupların eklenmesi için
 - c. **SecurID**. SecurID name space'inde belirtilmiş kullanıcı ve grupların eklenmesi için kullanılır.
5. **OK**'i tıklayın ve daha sonra **Next** ile ilerleyin.

Content Types (İçerik türü)

Bu rule elemanı uygulamak istenilen yaygın content type'lar sağlamaktadır. Örneğin, .exe ya da vbs uzantılarını içeren indirmeleri (download) engellemek için bir **content type** kuralı kullanılır.

Content type elemanları, MIME(Multipurpose Internet Mail Extensions) tiplerini ve dosya adı uzantılarını tanımlar. Client'lar internetten, HTTP ya da FTP protokollerini kullanarak download yapmak istediklerinde, download edilen içerik ya MIME formatında ya da özel bir dosya uzantısı formatında olmaktadır.

Content type elemanı, yalnızca HTTP ve FTP trafiği için kullanılır. Client, Internetten HTTP isteğinde bulunduğu ISA Server, bu isteği Web Servera gönderir. Web server bu içeriği gönderdiğinde ise ISA Server bu içeriği yapılandırılmış bir "content type" filtresi ile kontrol eder. İzin verilmeyen bir içerik bulunduğu ise bu isteği client'a göndermez.

ISA Server, Application, Application data dosyaları, Audio, Compressed dosyaları, Document dosyalar, Hypertext Markup Language (HTML) dokümanları, Image, Macrolar, Text, Video, ve

Virtual Reality Modeling Language (VRML) içerik türlerini destekler.

Schedules (Takvim)

Bu rule elemanı da rule'un haftanın hangi saatlerinde uygulanacağını tasarlanmasını sağlar. Örneğin yalnızca belirli saatlerde internet erişim hakkı sağlayan bir access rule oluşturmak isteniyorsa, bu saatleri tanımlayan bir schedule rule elemanı yaratılır ve daha sonra bu schedule rule elemanı access rule oluştururken kullanılır.

Birçok şirket, internet erişimini belirli zamanlarda kullanılması ister. Böyle bir durumda yaratılan bir Access rule'u **Schedule** elemanı ile belirtilen saatlerde izin verilip ya da engellenebilecek şekilde konfigüre edebilme olanağı bulunmaktadır.

Yeni bir **Schedule** oluşturmak için aşağıdaki yol izlenebilir:

1. Microsoft **ISA Server Management** konsolundan **Firewall Policy** tıklanır.
2. **Toolbox** tabından **Schedules**'a tıklayın.
3. **New** ve **New Scheduled** diyalog kutusunda gerekli konfigürasyonu yapın.
4. OK'i tıklayın.

İzleme

ISA Server, **ISA Server Management** yönetim aracılığıyla ulaşılabilecek çok sayıda izleme (monitoring) seçeneği sunar.

İzleme (monitoring) işlemine duyulan gereksinimi şu şekilde açıklayabiliriz:

Networkler arası trafik akışını izlemek için

Erişim (access) kurallarının doğru konfigüre edildiğinden ve ISA Server'da beklenen trafiğin aktığından emin olmak için network trafiğini izlemek gerekir.

NOT: İzlem süreci zaman içinde normal trafikle anormal trafiği ayırt edecek kalitede olmalıdır.

Bağlantılarda oluşan sorunları gidermek için

Network bağlantı sorunlarının çözümünde önemli bileşenlerden biri de ISA Server'ın izlenmesidir. Örneğin eğer bir kullanıcı internetteki bazı kaynaklara erişemediğini bildiriyorsa, yardım etmek için ISA Server'a bağlanabilirsiniz. Bu senaryoda sorun ya kullanıcının (client) konfigürasyonundan ya ISA Server'ın konfigürasyonundan, internet kaynağının çalışıyor ya da açık olup olmadığından kaynaklanabilir. ISA Server'ı izleyerek, probleme neden olan olayı büyük ölçüde belirleyebilir ve sorunu çözmeye başlayabilirsiniz.

Atakların (saldırıların) araştırılması.

Eğer ISA Server firewall olarak kullanılıyorsa ataklara karşı daha hassas olur. Doğru olarak konfigüre edilirse birçok atağı bulabilir ve engelleyebilir. Ancak ISA Server atakları başarıyla bloke etse de atakların devam ettiğini (occur) ve çeşitli atak modellerini (Intrusion Detection) bilmek ve yorumlamak gerekir.

ISA Server'a karşı yeni bir atak olduğunda, gelişmekte olan bu ataktan mümkün olduğunca çabuk alert mesajı oluşturulması ve bu sayede bu atakla nasıl başa çıkabileceğinizi belirlemeye çalışmak gerekir.

İzleme ve raporlama için ISA Server 2004 Management konsolu çok sayıda bileşene sahiptir.

- **Dashboard**
- **Alerts**
- **Sessions**

- **Services**
- **Configuration status**
- **Logs**
- **Reports**
- **Connectivity**
- **Performance monitor**

Dashboard

ISA Server 2004'deki Dashboard görünümü izleme bilgisinin özet görünümünü (hepsini birden) sunar. Dashboard ekranında şunlar görülür: Sessions, alerts, services, reports, connectivity ve genel sistem durumu.

Varsayım Dashboard görünümü şu bilgileri gösterir:

Connectivity: ISA Server'ın diğer bilgisayarlara olan bağlantılarını kontrol eder.

Alerts: ISA Server üzerinde oluşan olayları (events) listeler.

Services: ISA Server bilgisayarı üzerindeki servisleri ve mevcut durumlarını listeler.

Sessions: Toplam client oturum sayısını listeler.

Reports: Yeni yaratılmış raporları listeler.

Sistemin durumu (System health): ISA Server bilgisayarı üzerindeki performans bilgisini görüntüler.

Her Dashboard alanında görsel durum simgeleri bulunur. Kırmızı bir daire içindeki X işareti bir sorun olduğunu belirtir. Sarı simge uyarıları (warning) ve yeşil daire içindeki onay işaretleri de normal (sağlıklı) durumu belirtir.

NOT: Dashboard üzerinde yer alan pencereler kapatılarak dashboard üzerindeki görünüm özelleştirilebilir.

Alerts

Alert'ler belli bir olay (event) oluştuğunda sistem yöneticisini uyarmayı sağlar. Alert sistemi varsayım olarak birçok olayı izlemek üzere konfigüre edilmiştir. Ancak sistem yöneticisi kendi alert'lerini de geliştirilebilir. Örneğin bağlantı sayısı belli bir değeri aştığında bir e-mail mesajı ile sistem yöneticisinin uyarılması gibi. Bunun dışından özellikle tipik "intrusion detection" durumlarında Alert'ler kullanılır.

Sessions

Bir session (oturum) bir client'ın IP adresi ve kullanıcı adının benzersiz bileşimiyle oluşturulan bir bilgidir. ISA Server kimlik denetimine gereksinim duymadığında aynı IP adresinden gelen bütün trafiği tek bir oturum olarak düşünür. Bir Web browser aynı IP adresine birden çok TCP bağlantısı açarsa ISA Server bunun tek bir oturum olduğunu bilir.

ISA Server şu tür oturumları listeler: Firewall client, SecureNAT, virtual private network (VPN) client, VPN site-to-site ve Web Proxy.

Services

ISA Server 2004 kurulduğunda aşağıdaki servisler (Windows işletim sistemi servisleri) yüklenir:

- Microsoft Firewall servisi
- Microsoft ISA Server Control servisi
- Microsoft ISA Server Job Scheduler servisi
- ISA Server Storage servisi

- Microsoft SQL Server 2000 Desktop Engine servisi

Services bölümü ile Microsoft Firewall servisi, Microsoft ISA Server Job Scheduler servisi ve Microsoft SQL Server 2000 Desktop Engine servisi durdurulabilir (stop) ya da başlatılabilir. Diğer servisler için komut satırından **net start** ve **net stop** komutları ya da **services.msc** konsolu kullanılır.

Örnek:

Microsoft ISA Server Control servisini (mispadmin) durdurmak için:

net stop isactrl

Configuration status

Configuration status görünümü sistem yöneticisinin bütün array içindeki server'ların konfigürasyon bilgisini **Configuration Storage server**'dan aldığı doğrulamayı sağlar. Öncelikle array üyelerinin hangisinin tam olarak senkronize olmadığını gösterir.

Logs

ISA Server 2004 kurulduğunda bütün bileşenler için **logging** (loglama) işlemi varsayım olarak **enabled** durumdadır.

ISA Server'da mevcut olan ya da daha önceki işlemleri izlemek için bu loglar kullanılabilir.

Belli bir bileşen için (Web Proxy, Microsoft Firewall servisi ya da SMTP Message Screener) loglama seçeneği **disable** edilebilir.

Log bilgileri bir dosya, bir SQL veritabanı ya da bir MSDE 2000 veritabanına kaydedilmek üzere düzenlenebilir.

Varsayım olarak Web Proxy ve Firewall servisi için log bilgisi Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) veritabanına kaydedilir.

Reports

ISA Server'ın kullanım şekli hakkında bilgileri özetler. Örneğin erişilen web sitelerin istatistikleri gibi. Ayrıca hangi protokol ve uygulamaların daha fazla kullanıldığını özetleyen raporlar oluşturulabilir.

Network güvenliğini izlemek için de raporlardan yararlanılabilir. Örneğin, iç network üzerindeki kaynaklara kötü niyetli erişim denemelerinden oluşan bir rapor hazırlanabilir.

Connectivity

ISA Server'ın kurulu olduğu bir bilgisayar ile network üzerindeki diğer bir bilgisayarın ya da bir URL'nin düzenli olarak izlenmesini sağlar. Örneğin bağlanabilirlik seçeneklerini; Domain controller'ların, DNS server'ların aktif haldeki Web server'ların ve external web server'larının bağlantılarını izlemek için kullanabilirsiniz. Gerekli bir servis durduğunda ya da bir networkün bağlantısı çöktüğünde bu hizmet size büyük yararlar sağlar.

Bağlanılabilirliği belirlemede kullanılacak metot seçilebilir:

- Ping
- TCPConnect
- HTTP Request

Ping: Bu metot seçildiğinde, ISA Server belirtilen server'a ICMP ECHO_REQUEST mesajı gönderir ve ICMP ECHO_REPLY mesajı bekler. Bu metot bir server'ın ISA server tarafından

erişilebilir olduğunu doğrulamada kullanılır.

TCP connect: Bu metot seçildiğinde ISA Server belirtilen porta bir TCP bağlantısı oluşturmayı dener. Bu metot belli bir servisin çalışıyor ve ISA server tarafından erişilebilir olduğunu doğrulamada kullanılır.

HTTP request: Bu metot seçildiğinde ISA Server bir HTTP Get request mesajı gönderir ve yanıt bekler. Bu metot bir Web server'ın ISA server tarafından erişilebilir olduğunu doğrulamada kullanılır.

Performance Monitor

ISA Server kurulu bilgisayarda performans verisi toplar. Server performansını gerçek zamanlı olarak izleyebilirsiniz. Detaylı analizler için server performansını uzun vadeli izleyebilen bir log yaratabilirsiniz, ya da counter'lar (sayaç) çok yüksek rakamlara ulaştıklarında bunlarla başa çıkabilmek için performans alert'leri oluşturabilirsiniz. Bu olaylar log kayıtları yaratabilir, bir network mesajı gönderebilir ya da bir program çalıştırabilir.

ISA Server performans verilerini ISA Server Management üzerindeki **Dashboard** ya da **ISA Server Performance Monitor** aracılığıyla görebilirsiniz.

TESCİLLİ MARKALAR

Tescilli markalar ve ürünler aşağıda listelenmiştir. Örneklerde adı geçen kullanıcı, kurum adları, e-mail adresleri vb. bilgiler tümüyle hayalidir. Herhangi bir gerçek kişi ya da kurumla ilgisi yoktur. Tescilli markalar kendi imtiyazlarına sahiptir. Kitapta bilgi amaçlı kullanılmıştır.

Okuyucular kitaptaki bilgileri kendi istekleriyle kullanmayı kabul etmiş sayılırlar.

Tescilli Markalar:

- MCSE, MCSE 2003, Microsoft Corporation firmasının tescilli markasıdır.
- 70-290 : Managing and Maintaining a Microsoft Windows Server 2003 Environment, 70-291, 70-293, 70-294 gibi sınav kodları ve adları Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Windows Server 2003, Microsoft Windows 2000, Microsoft Windows XP, Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Exchange Server 2003, Microsoft Systems Management Server 2003, Microsoft Corporation firmasının tescilli markasıdır.
- .NET, Visual Studio .NET, C# .NET, Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft SQL Server, Microsoft SQL Server 6.x, Microsoft SQL Server 7.0, Microsoft SQL Server 2000, Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Visual Basic 6.0, Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Windows NT, Microsoft Windows NT 3.xx ve Microsoft Windows NT 4.0, Widnows NT 5.0, Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Word, Excel, Access, PowerPoint, Outlook Microsoft Corporation firmasının tescilli markasıdır.
- Microsoft Office 2000, Word 2000, Excel 2000, Access 2000, PowerPoint 2000, Outlook 2000 Microsoft Corporation firmasının tescilli markasıdır.
- ASP, ASP .NET, VBScript, Microsoft Corporation firmasının tescilli markasıdır.
- ActiveX, IntelliSense, Visual InterDev, Visual Studio, Publisher, BackOffice, Windows, Microsoft firmasının tescilli markasıdır.
- MS-DOS, Microsoft Corporation firmasının tescilli markasıdır.

DİKKAT: Bu kitap Faruk Çubukçu tarafından yazılmıştır. Yayın ve dağıtım hakkı Faruk Çubukçu'ya aittir. T.C. Kültür ve Turizm Bakanlığı, Fikir ve Sanat Eserleri ilgili yasalarıyla; eser, yazarın izni olmadan elektronik, mekanik, fotokopi, kayıt cihazı vb sistemler kullanılarak kısmen ya da tamamen kopyalanamaz. COPYRIGHT (c) 2003 FARUK ÇUBUKÇU. Faruk Çubukçu, Tel: 232-4830050, faruk@farukcubukcu.com.