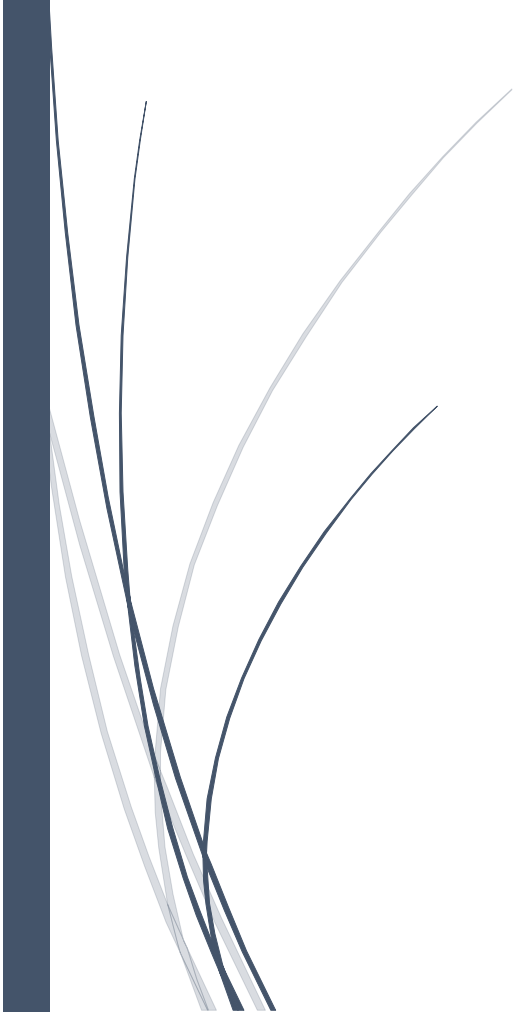
2/7/2013

Ajansız Yedekleme ve Kurtarma Efsanesi

StorageCraft Neden Ajan Kullanıyor



STORAGECRAFT

İçindekiler

Bazı potansiyel StorageCraft müşterileri neden “ajansız” yedekleme ve kurtarma çözümü sunmadığımızı soruyor. Hatta birkaç tanesi ajansız bir çözümü olmadığı için StorageCraft almayacaklarını söylediler. Ne yazık ki kullanıcıların geniş bir bölümünün algılarının yanlış yönlendirici pazarlama mesajları nedeni ile etkilendiğini görüyoruz.

StorageCraft olarak biz yedekleme ve kurtarma çözümlerinde ajan kullanımının önemini belirtmek gereği duyuyoruz. Kullanıcılar ajanların birer yardımcı araç olmaktan öte neden gerekli olduğunu anlamalarına yardımcı olmak istiyoruz.

Ajanlı’mı Ajansız’mı

Ajanlı veya ajansız yedekleme çözümlerini değerlendirebilmek için kavramlar arasındaki farkları iyi anlamamız gerekiyor. İlginç bir şekilde hem ajansız hem de ajanlı çözümler güçlü ve zayıf özelliklerinden bahsederken aynı noktalara değiniyor. Belki de bu nedenle anlaşılır bir kafa karışıklığı mevcut ve kullanıcılar tercihlerini ajansız çözümlere doğru yöneltiyorlar.

Örneğin, ajanlı ve ajansız çözümlerin her ikisi de aşağıdakileri yapabildiklerini söylüyor:

- Yedeği alınacak verinin uzaktan izlenmesi ve yönetilmesi
- Tam (full) yedek imajları ve buna bağlı artımlı (incremental) dosyalar
- Dosya, klasör, birim, disk ve blok bilgisinin yedeklenmesi
- Exchange, SQL, SharePoint uygulamalarının çalışırken yedeklenmesi
- Otomatik yedek imajı doğrulaması

Bununla beraber ajanlı ve ajansız çözümler arasında kayda değer farklılıklar bulunuyor.

Not: Ajansız kolonundaki bilgiler sürekli artımlı yedek alındığı varsayılarak düzenlenmiştir.

Ajanlı	***Ajansız***
Yedeklenmek istenilen her sisteme kalıcı olarak ajan yüklemesi yapılır.	Yedeklenmek istenilen her sisteme geçici olarak çalıştırılabilir modüller yerleştirilir.
Kaynaktaki ajan yedek imajını oluşturur ve önceden tanımlanmış bir depoya gönderir.	Merkezi kontrol istasyonu ajansız kaynaklara bağlanır ve yedeklenecek veriyi toplar.
Microsoft onaylı kernel kurulum yöntemlerini kullanır. Ajan sistem açılırken depolama sürücü yığınının doğal bir parçası olur.	Ya dâhili Microsoft birim gölge kopya sürücüsünü kullanır veya kendine ait bir gölge kopya sürücüsünü IRP Dağıtım Tablosu Kancalama adı verilen yöntem ile yükler.

Ajansız Yedekleme Sistemleri

Ajansız çözümler kaynaktaki yedekleme görevlerini gerçekleştirmek ve yönetmek için dış sistemlere bağımlıdır. Teoride yedekleme, depolama, replikasyon ve diğer tüm işlemler host üzerinde veya merkezi yedekleme yöneticisinde gerçekleşir.

Kullanılan yöntem ne olursa olsun ajansız yedeklemenin avantaj olarak algılanan özellikleri şunlardır:

- İstemci başına lisanslama yok
- Host-temelli operasyon bu yükü istemciden alır
- Yedekleme görevleri her bir istemci yerine host üzerinde yapılandırılır

Ajansız yedekleme çözümlerinin dezavantajları ise şunlardır:

- Yedekleme yapmak için host ajanını kullanır veya geçici olarak kendi ajanını yükler
- Geçici olarak bir ajan veya sürücü yüklenmeden hızlı ve sürekli artımlı yedekleme imkânsızdır.
- Geçici olarak yüklenen "enjekte" edilen sürücüler sistem kararlığını bozabilir ve veri tutarlılığını tehlikeye sokar
- Geçici olarak yüklenen "enjekte" edilen sürücüler sorun giderme işlemlerini zorlaştırır
- Bazı uygulamalarda ücretler host veya yedek yöneticisi tarafından depolanan ve işlenen veri boyutuna göre belirlenir
- Merkezi yönetim tek-arıza-noktasıdır (SPOF) Yönetim sisteminde arıza olduğunda tüm yedekler tehlikeye girer.

Host-Tabanlı Ajansız Yedekleme

Ajansız yedekleme gerçekleştirmenin bir yolu hipervizörü (VMHost) kullanmaktır. Hipervizörün sanal makinelerin dosya ve klasörlerine tam erişim hakkı olduğu için teorik olarak sanal makinenin istenilen zamanda bir kopyasını çıkarabilir. Tüm popüler hipervizörler bunu gerçekleştirmek için araçlar sağlar. Ne yazık ki bu araçların kalitesi ve kapsamı üreticiden üreticiye değişir, bu da host-tabanlı yedeklemenin üreticiden üreticiye farklılık göstermesine neden olur.

Host-tabanlı yedekleme genel olarak şu türden dosyaları koruyabilir:

- Sanal sabit diskler
- Sanal ağ yapılandırma dosyaları
- Host yapılandırma bilgisi
- Sanal makine yapılandırması ve kayıt edilmiş durumdaki dosyalar

Host-tabanlı yedeklemeler tüm sanal makineler için yedekleme görevlerini tek bir yerde toplayarak kullanım kolaylığı sağlar ama bunun için *esneklikten* ve bazı durumlarda *yedek kalitesinden* ödün verir.

Esneklik

Host-tabanlı ajansız yedekleme bazı uygulamalarda esneklikten ödün verir. Örneğin, host-tabanlı bir yedekleme görevi tüm kaynaklar için yalnızca bir zamanlama ve hedef destekler. Diğer yandan ajanlı yedeklemelerde her bir sanal makine için ayrı ayrı benzersiz zamanlama ve hedef belirleyebilirsiniz.

Kalite

Bazı durumlarda hipervizör yedekleme öncesinde sanal makineyi olması gerektiği gibi hazırlayamaz. Bu hazırlıklara uygulamalara verilmesi gereken bellekte tuttukları tüm veri ve işlemleri diske yazma emri gibi kritik görevler dâhildir. Bu durumda yedekleme başarı ile tamamlanır fakat sonuçta elde edilen yedek veri olması gereken ile tutarlı değildir. Dosya verisi ve dosya sistemi meta verilerindeki bu tutarsızlıklar sanal makine kurtarıldıktan sonra çökmelere neden olur. Hipervizör sanal makineyi yedeklenmek üzere hazırlayamadıysa felaket sonrasında elinizdeki yedeklerin hemen hiçbir değeri yoktur.

Koordinasyon Sorunları

Sanal makine diskinin tutarlı olarak yedeğinin alınabilmesi için host, guest, yedekleme çözümü, VSS ve hipervizör arasında koordinasyon olmalıdır. Host birim anlık kopyaları (snapshot) oluşturulmadan önce hipervizör bellekte tutulan tüm veriyi diske yazdırmalıdır. Ayrıca host birimin kopyasını oluşturulana kadar hipervizör yeni oluşacak disk aktivitelerini dondurmalıdır. Hipervizör'ün VSS yazıcısı teorik olarak bunu becerebilir fakat pratikte bu işlem çok da güvenilir olmuyor.

VM-Tabanlı Ajansız Yedekleme

VM-tabanlı ajansız yedekleme her bir sanal makineyi ayrı ayrı ele alır ve bu makinelerin verilerinin yedeğini fiziksel olarak ağdalarmış gibi alır. Ajansız sistemler her bir sanal makinenin üzerinde yüklü olan snapshot sürücülerini kullanır.

Snapshot sürücüleri dosya sisteminin altında Windows kernel depolama yığınında görev yaparlar. Ajansız bir yedekleme çözümü öncelikle bir karar vermelidir; Microsoft'un snapshot sürücüsünü mü kullanacak yoksa kendisi özel bir snapshot sürücüsü mü oluşturacak.

Varsayılan Microsoft snapshot sürücüsü: Windows XP ve sonrasındaki sistemler birim anlık kopyalarını Microsoft'un VolSnap.sys sürücüsü ile destekler (bakınız Ajansız Data Snapshot).

Özel snapshot sürücüsü: Yedekleme yazılımı üreticileri Microsoft'un snapshot sürücüsünün kısıtlamalarına takılmamak için kendi sürücüleri geliştirebilirler. Bu artımlı yedek (incremental) alma zamanının oldukça kısaltır. Yedekleme yazılımı üreticisi özel snapshot sürücüsünü aşağıdaki gibi iki şekilde yükleyebilir:

Birim-Sınıfı Yükleme (Volume-Class Install):

- Dosya sistemi altına bir depolama sürücüsü yüklenir.
- Depolama sürücüsü işletim sistemi tarafından derlenen depolama sürücü yığınına eklenir.
- Microsoft-onaylı teknik
- Sürücü yüklendiğinde veya kaldırıldığında sistemin yeniden başlatılması gerekir.

IRP Dağıtım Tablosu Kancalama (IRP Dispatch Table Hooking):

- Genel olarak zararlı yazılımlar (özellikle rootkitler) tarafından kullanılır.
- Snapshot sürücüsü yeniden başlatmadan sistem çalıştığı sırada enjekte edilir.
- Microsoft kernel takımı tarafından özellikle yapılmaması tavsiye edilir ve desteklenmez.
- Kernel'in kararlılığını kolaylıkla tehlikeye sokabilir sistem kilitlenmelerine ve mavi ekran hatalarına neden olabilir.
- Hem kaynak veri biriminde hem de yedek imajlarında veri kaybına veya bozulmalarına yol açabilir. Bu veri bozulmaları sistem geri yüklenmeden önce fark edilemez.

Daha detaylı bilgi için bakınız: IRP Dağıtım Tablosu Kancalama - Detaylar.

Ajanlı Yedekleme Sistemleri

Ajan-tabanlı yedeklemede, işin tamamı kaynak üzerine yüklenen ve yedeği ön tanımlı bir depolama hedefine gönderen ajan tarafından gerçekleştirilir. Hedef yalnızca yedekler için depo görevi görür ve pasiftir.

Ajanların Avantajları

- Hızlıdırlar
- Kernel tarafından desteklendikleri için güvenilir yedekleme sağlarlar
- Merkezi yedekleme yönetim konsolunda meydana gelebilecek arızalar yedeklerin zamanında ve tutarlı alınmasını etkilemez

Ajanların Dezavantajları

- Korumak istediğiniz her sisteme yazılım yüklenmelidir
- Her bir istemci ayrı ayrı yapılandırılmalıdır

StorageCraft Ajanları

StorageCraft Yedekleme ve Kurtarma çözümlerinde hem veri yedekleme hem de kurtarma süreçlerinin kararlılığını ve güvenilirliğini en üst düzeyde tutmak için yazılım ajanları kullanıyor. ShadowProtect ajanları Microsoft VSS framework'ünün snapshot alırken kullanması için özel tasarlanmış VSS sağlayıcı içerir. (Microsoft tarafından sağlanan fakat ağır ve kısıtlı VolSnap sağlayıcının yerine). ShadowProtect snapshot sağlayıcısı MS VSS Framework ile tam uyumludur.

ShadowProtect ajanı şu avantajları sağlar:

- Olağanüstü hızlı yedek alabilmek için snapshotlar arasındaki sektör değişikliklerini takip eder.
- Zamanda bir nokta şeklinde alınan yedek imajlarını oluşturur ve yönetir.
- Kurtarma sırasında veri güvenilirliğini arttıran VSS-tabanlı yedekleme sağlar.
- Zamanı ve depolama alanını tüketmeyen Tam (full), fark (differential) ve artımlı (incremental) yedekler oluşturur.
- Minimum sistem kaynağı tüketir.

Ajansız üreticiler çoğu zaman ajan kullanmanın sistem kaynaklarında kabul edilemez etkileri olduğunu iddia ederler, fakat bu tür iddialar genelde temelsizdir ve yanlış yönlendirir. Örneğin, bazı yedekleme yazılımı üreticilerinin büyük boyutta ve ağır ajanlarından bahsederler istatistik verirler ve daha sonra bunu genele yayarlar. Ayrıca geçici olarak sisteme enjekte ettikleri ajanlarında aynı şekilde sistem üzerinde olumsuz etkileri olduğundan hiç bahsetmezler.

ShadowProtect ajanı en sık yaptığı işi yaparken yani artımlı (incremental) imaj oluştururken sistem üzerindeki etkisi aşağı yukarı aşağıdaki gibi gerçekleşiyor:

- Yedekleme için hazırlanma: ~10 saniye boyunca CPU kullanımı %12.
- Yedek oluşturma: ~7 saniye boyunca CPU kullanımı %5 – %5,4 CPU (VSS dâhil).
- Yedekler arasında: Önemsiz derecede CPU kullanımı.
- Bellek kullanımı: İş yüküne göre 6MB – 30MB arasında.

Tam (Full) ve Fark (Differential) yedekler CPU ve Bellek kullanımında artışlara neden olur. Fakat tam yedekler iş saatleri dışına zamanlanabilir ve fark yedekleri ise normal şartlarda zaten oluşturulmazlar. (Fark yedekleri elektrik kesintisi gibi sistemin ani kapanmaları sonucunda oluşturulur)

Lisanslama Hakkında

Ajansız yedekleme ve kurtarma çözümlerinin ilk bakışta algılanan faydalarından biri ajan başına lisans parası ödenmemesi. Ajansız çözüm üreticilerinin çoğu host veya soket-tabanlı lisanslama modellerinin faydalı bir şey olduğunu öğrettiler. Fakat herhangi bir çözümün son maliyeti yalnızca ilgili müşterinin ortamı ile birlikte düşünülmelidir. Lisanslama değeri için öncelikle terminolojiyi anlamak gerekir:

> **Ajan-tabanlı lisanslama:** Ajanlı çözümler tarafından kullanılan bu tür lisanslama her bir kaynak için ayrı lisans gerektirir. Ajan tabanlı lisanslama hem fiziksel hem de sanal makinelere uygulanabilir.
>
> **Host-tabanlı lisanslama:** Ajansız çözümler tarafından kullanılan bu tür lisanslama yedekleme çözümünün çalıştırılacağı her bir fiziksel host için lisans gerektirir. Bir lisans host üzerinde çalışan tüm sanal makinelerin yedeğini alır. Host-tabanlı lisanslama yalnızca sanal ortamlarda kullanılabilir.
>
> **Soket-tabanlı lisanslama:** Ajansız çözümler tarafından kullanılan bu tür lisanslama hipervizörün çalıştığı fiziksel makinede kullanılan her bir işlemci için lisans gerektirir. Soket-tabanlı lisanslama yalnızca sanal ortamlarda kullanılabilir.

Yedekleme ve kurtarma çözümünün fiyat-performans oranı kullanılan lisanslama modeli fark etmeksizin korunan, yedeklenen makine başına maliyeti ile ortaya çıkar. Enterprise Management Associates araştırmasına göre enterprise ortamlardaki sanal makine dağılımı (hipervizör başına sanal makine) ortalama 6 adet. Küçük ve orta ölçekli işletmelerde ise bu oran daha az.

Örneğin: Aşağıdaki fiyatlandırma yedekleme ve kurtarma yazılımı üreticilerinin gerçek fiyatlarını yansıtmaktadır. Karşılaştırma için hipervizörün dört çekirdekli tek bir işlemci üzerinde koştuğu bir sunucu temel alınmıştır.

# Sanal Makine Sayısı ->	**1**	**3**	**6**	**12**
Ajan başına * (StorageCraft)	$395	$995	$1295	$1895
Host başına**	$1799	$1799	$1799	$1799
Soket başına***	$1099	$1099	$1099	$1099

*Ajan-tabanlı lisanslar istenildiği kadar hipervisör veya soket üzerine dağıtılabilir.
**Sanal makinelerin tek bir host üzerinde çalışması gereklidir.
***Sanal makinelerin tek işlemcili bir sunucu üzerinde çalışması gereklidir. Ek işlemciler ek lisans gerektirir.

Sonuç

Mark Campbell Mart 2012 tarihinde yayınlanan "Herkes Yalan Söyler: Yedekleme ve Gizli Ajanlar" adlı makalesinde günümüz sanallaştırma eğilimlerinde "Gizli Ajanların" kullanıldığından dem vuruyor. *Gizli ajanlar* bazı sanallaştırma üreticilerinin host veya sanal makine üzerine yükledikleri fakat ajan değil de sadece "altyapısal yazılımlar" olduğunu iddia ettikleri yazılımlara Mark'ın verdiği isim. Tabi ki yalnızca bir kelime oyunu…

Sistem ister ajan ile isterse ajansız çalışsın kaynak işletim sistemi ile yedeklemeyi yöneten sistem arasındaki iletişim bir şekilde bir yerde yapılacak. "Ajansız" çalışan çözümler bu işi üçüncü parti ajanlara devrederek veya geçici olarak kendi ajanını enjekte ederek yapıyor. İşi yapacak bir çeşit ajan olmadan sistem performansını etkilemeyen hızlı artımlı yedek almak imkânsız.

StorageCraft ajansız çalışmak yerine ürünlerinde ajan kullanmayı tercih ediyor. StorageCraft ShadowProtect hızlı, etkili ve piyasadaki en güvenilir yedekleme ve kurtarma seçeneklerinden biri ve üstelik kendi işini gizli ajanlara devretmek gibi bir ihtiyacı yok.

Ajan-tabanlı çözümler sanal ortamlarda bile güçlü, esnek ve en güvenilir çözümlerdir.

Ek Teknik Bilgiler

Bu bölüm yukarıda anlatılan bazı kavramların açıklamalarını içerir.

Ajansız Data Snapshot

Ajansız yedekleme ve kurtarma çözümleri ya Windows volume snapshot sürücüsünü kullanır ya da kendi sürücüsünü geçici olarak sisteme enjekte eder ve işi bitince kaldırır. Bu çözümlerin her ikisi de en iyi sonucu vermekten uzaktır.

- VolSnap (Microsoft snapshot sağlayıcısı) kullanarak alınan artımlı (incremental) yedekler kabul edilemez şekilde yavaş olur. Bunun nedeni VolSnap'in bir snapshot ile diğer arasında olan blok değişikliklerinin haritasını tutmamasıdır. Bu nedenle VolSnap.sys kullanan yedekleme yazılımı her seferinde değişiklikleri algılayabilmek için fark (differential) karşılaştırması yapmak zorunda kalır. Fark karşılaştırma işlemleri önemli derecede zaman ve kaynak israfıdır ve mümkün olduğunca kaçınılmalıdır.

- Sistemi yeniden başlatmadan IRP Dağıtım Tablosu Kancalama yöntemi ile özel bir sürücü enjekte etmek sistemin kararlılığını tehlikeye sokabilir ve bunun sonucunda geri alınamaz veri bozulması, sistem çökmesi gibi sorunlar ortaya çıkar. Sistem kararlılığı ve veri bütünlüğü riski ortaya çıkar. (Daha detaylı bilgi için NT Kernel Geliştiricileri forumunu inceleyebilirsiniz: osronline.com)

Filtreleme

Ajanlı veya ajansız çözümlerin her ikisi de kararlı ve güvenilir yedeklemeler için Windows çekirdeğinde sağlanan sürücü ile volume snapshot yeteneğini kullanmak durumundalar. Üreticiler VolSnap.sys sürücüsüne güvenebilirler veya kendi özel sürücülerini geliştirebilirler. Daha önce de bahsedildiği gibi VolSnap sürücüsünün kullanımı ağır ve fazla kaynak tüketen artımlı yedeklere neden olur. Özel bir sürücü bu durumu bertaraf edebilir fakat bu sürücüyü yüklerken kullanılan yöntem sorun olabilir. Snapshot sürücüsünün yüklenebilmesi için Windows sistemin mutlaka yeniden başlatılması gerekir.

Windows çekirdeğinde yer alan sürücüler seviyeler halinde çalışarak aşağıdaki sıralama ile (yüksekten düşük seviyeye) bir depo sürücü yığını oluştururlar:

- Dosya Sistemi Sürücüleri
- Mantıksal Birim Sürücüleri
- Disk Sürücüleri
- Port/Miniport Sürücüleri
- Host Bus Adaptörü (veya depolama kontrolcüsü)

Kernel sürücülerini port/miniport sürücüleri dışında herhangi bir seviyeye eklemek mümkündür. Bu özel sürücüler mevcut depolama sürücü yığınının karşılayamadığı özellikleri sağlar. Örneğin Microsoft kendi snapshot sürücüsünü Dosya Sistemi ve Mantıksal Birim Sürücüleri arasındaki seviyeye yükler.

IRP Dağıtım Tablosu Kancalama – Daha yakından bakalım

'IRP Dağıtım Tablosu Kancalama' bazı yazılım üreticilerinin mevcut işletim sistemi sürücü yığını içerisine sürücü enjekte etmek için kullandıkları bir yöntem. Yedekleme ve Kurtarma penceresinden bakarsak üreticinin ihtiyaç olduğunda yükleyerek ve sonra kaldırarak "ajansız" çözüm sağladığını iddia etmesine yarıyor. Ne yazık ki bu yöntem sıklıkla sistem kararlılığına zarar veriyor ve Microsoft tarafından tavsiye edilmiyor.

IRP Dağıtım Tablosu Kancalama Nasıl Çalışıyor?

Windows Kernel-modu sürücüsünü yükler ve DiverEntry başlatma rutinine bir defalık çağrı yaparak sürücüyü başlatır. Sistem temel fonksiyon dağıtım tablosunu DriverEntry'ye geçirir.

Bir kanca sürücü, başka bir sürücünün dağıtım tablosunu kendisindeki kodu gösteren bellek yolu ile değiştirerek sürücünün I/O su ile etkileşime geçer. Bunun sonucunda işletim sistemi orijinal sürücü yerine kanca sürücüye I/O talebi iletir.

IRP Dağıtım Tablosu İşlem Adımları

Kanca enjekte yöntemi sırasıyla aşağıdaki adımları izler:

1. Windows OS çekirdeği kanca sürücüyü yükler ve kendisi için başlatma rutinini çağırır. (DriverEntry).
2. Kanca atan sürücü kanca atılan sürücüye ait temel fonksiyon dağıtım tablosunu bulur. Bu tablo kanca atılan sürücüdeki I/O taleplerini ele alan rutinleri içeren bellek adreslerini (function pointers) barındırır.
3. Kanca atan sürücü, atılan sürücüye ait temel fonksiyon dağıtım tablosundaki orijinal function pointer değerlerini kendi oluşturduğu başka bir tabloya kopyalar.
4. Kanca atan sürücü, atılan sürücüye ait tablodaki function pointer değerlerini kendisini işaret edecek şekilde değiştirir.
5. Bu durumda işletim sistemi kanca atılmış sürücüye I/O talebi iletirken kanca atan sürücüye ait rutinleri çağırır. Kanca atan sürücü I/O talebi aldığı zaman istediği şeyi yapabilir ve sonrasında daha önce kopyaladığı dağıtım tablosu yardımı ile asıl sürücünün rutinine gönderebilir.