Consolidating network appliances with virtualization

By Dan Joe Barry, Napatech

Virtualization has transformed the economics of running data centers. Indeed one could say that without virtualization, data centers would have faced a serious power consumption dilemma. With virtualization, it is now possible to make more efficient use of physical resources and thereby space and power consumption, which lead to cost savings.

Cost, space and power will continue to dominate the agenda as Internet data traffic continues to grow between 50% and 60% per year. Indeed, for data centers, traffic could grow even quicker as cloud computing centralizes more computing resources and more devices are used to exchange data, such as mobile phones, tablets, TVs, etc.

As more computing resources are centralized, monitoring, analyzing and securing these resources becomes more important than ever. Yet, network appliances today are typically single server implementations with few implementations providing more than one application. It is not uncommon to find several network appliances accessing a single monitoring location. For example, a typical scenario could be three appliances monitoring the same connection with one monitoring specific flows, another providing performance analysis and a third providing intrusion detection functionality.

Since cost, space and power are major issues for data centers, reducing the footprint of network appliances also becomes a major consideration. Many network appliances require all the processing power they can get and thus cannot share processing resources with other applications. Examples are 10 GbE Intrusion Prevention Systems or Application Performance Monitoring systems.

But, there are also a large number of monitoring, analysis and security appliances that run at lower speeds or do not require as much processing resources. Here, there are opportunities to consolidate these appliances into a single server solution.

If all appliances are based on the same operating system, it is possible to consolidate them using intelligent network adapters that can distribute data and share data between multiple applications. Such solutions exist today.

However, if the appliances are based on different operating systems or environments or expect to have full control over available hardware resources, then an alternative solution is required. Virtualization can be used in such instances to consolidate these very different applications. A number of different solutions are possible depending on data sharing and distribution needs. The following describes various solutions based on VMware that can be used to consolidate multiple network appliances onto a single physical platform.

Using VMware Direct Path

VMware Direct Path allows a virtual machine to control a physical network adapter. This allows existing network appliance applications to be transferred to a virtual environment:

Typical Network Appliance Implementation — **Virtual Network Appliance Implementation**
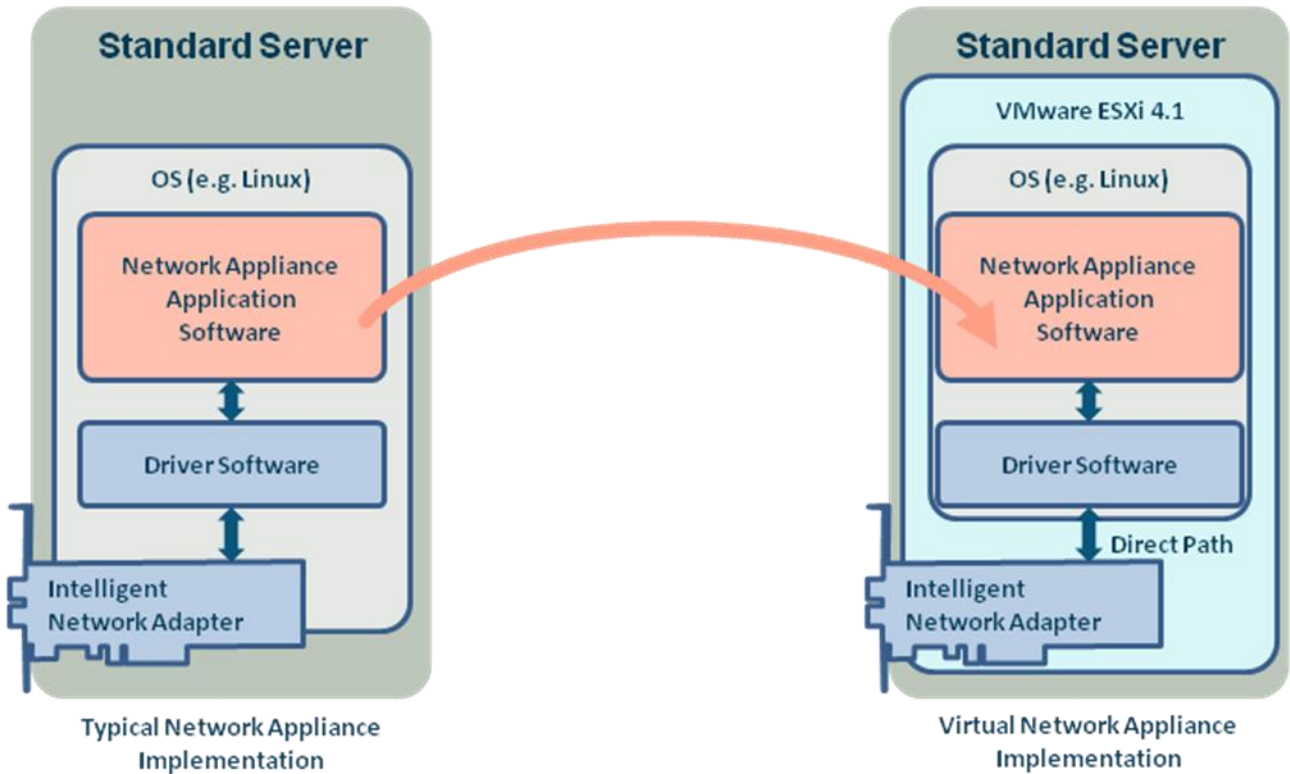
This is the first step in consolidation. To the network appliance application software, it still appears as if it is running on its own server with full control of the intelligent network adapter. The driver software has been updated to support VMware Direct Path, but otherwise, no changes need to be made.

With this solution, a consolidation can be performed for multiple network appliances:
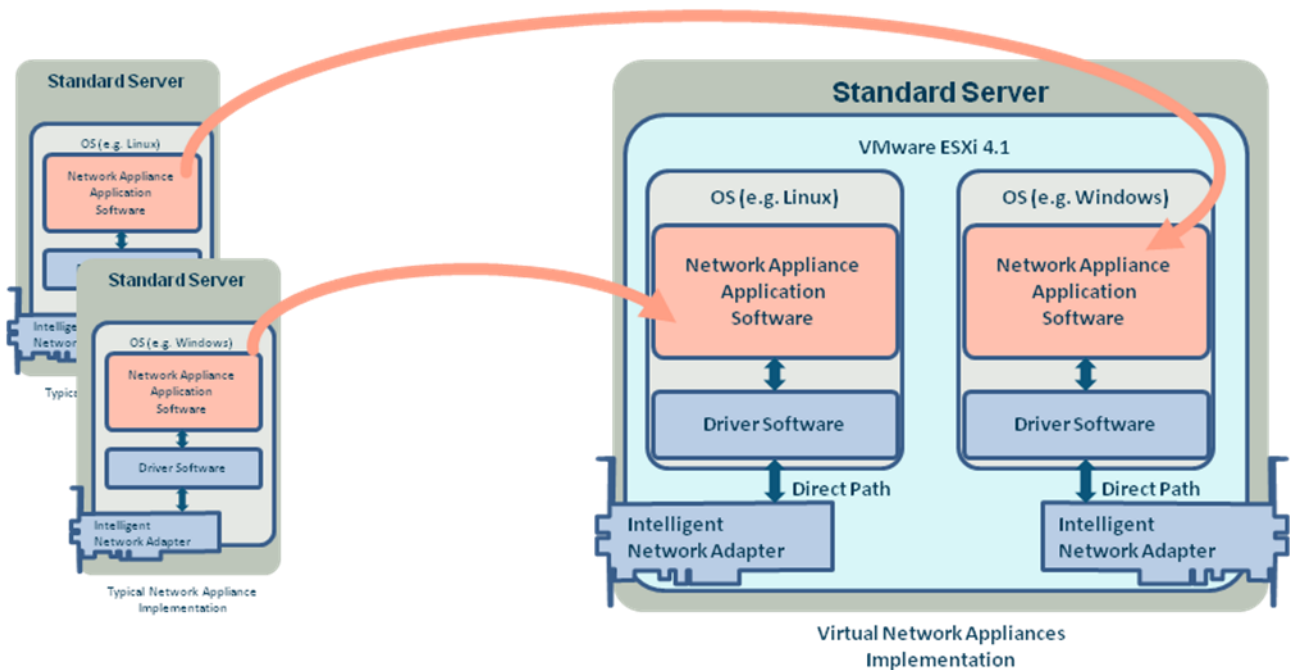
As can be seen, each network appliance can be based on a different operating system and execution environment, but still be supported on the same physical server. The only restriction is that each virtual machine needs its own network adapter as only one virtual machine can control a given network adapter at one time.

Sharing network adapters

While the above implementation works, it still requires that a network adapter is dedicated to each virtual client. This limits the number of applications to the number of slots in the server. If all the virtual clients need to access the same point in the network, a separate load balancer would be required to distribute the data between the network adapters.
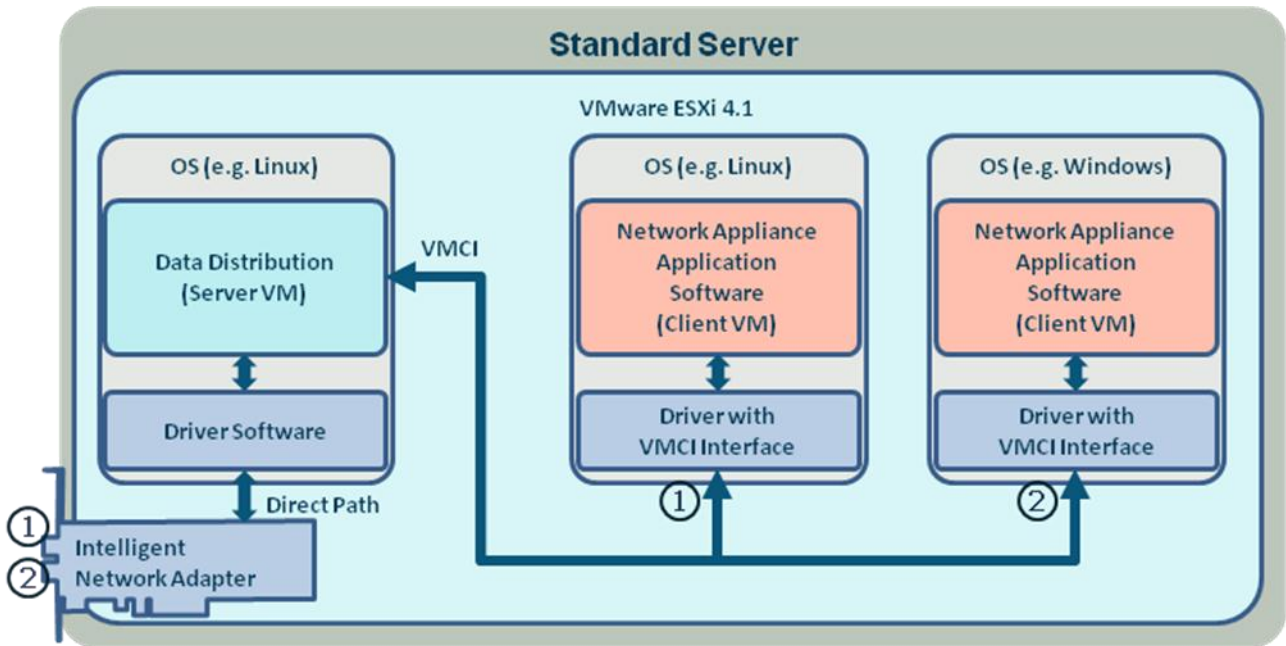
By distributing data within VMware, we can eliminate the load balancer and reduce the number of network adapters required.
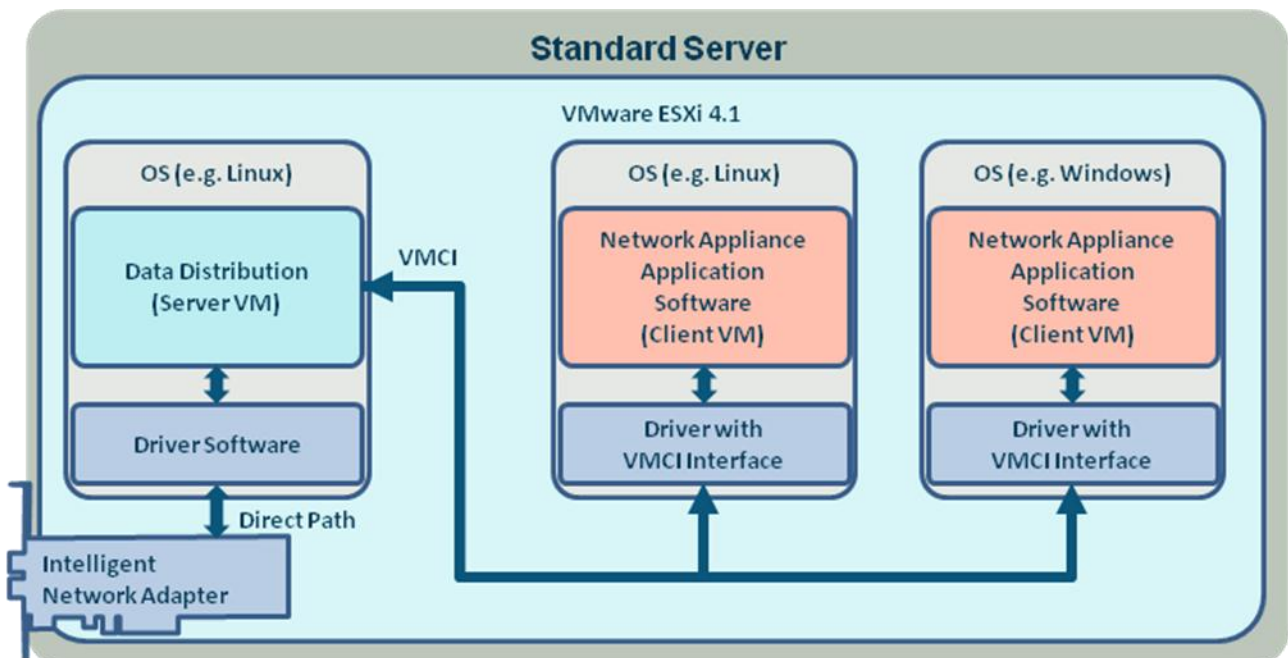
By using a data distribution virtual machine as a server virtual machine based on VMware's VMCI (Virtual Machine Communication Interface), it is possible to distribute and replicate data to multiple virtual machine clients. The data distribution virtual machine can thus distribute or replicate data captured by a single intelligent network adapter to multiple client virtual machines each supporting a separate network appliance.

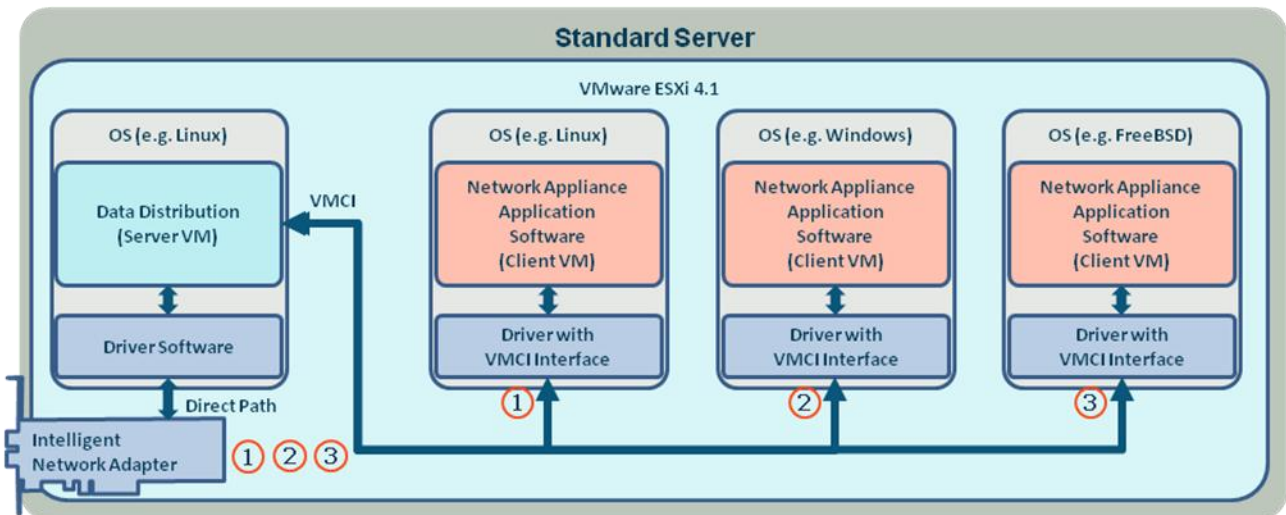**Distributing data on a per physical or virtual port basis**

One method of distributing data to multiple client virtual machines is by physical port:

Standard Server

VMware ESXi 4.1

OS (e.g. Linux) — Data Distribution (Server VM) — Driver Software

VMCI

OS (e.g. Linux) — Network Appliance Application Software (Client VM) — Driver with VMCI Interface ①

OS (e.g. Windows) — Network Appliance Application Software (Client VM) — Driver with VMCI Interface ②

Direct Path

① ② Intelligent Network Adapter

① Physical port

In the example above, data on each port of the network adapter is mapped to a separate client virtual machine. However, this limits the solution by the number of physical ports on the network adapter.

A more interesting solution is to use logical ports:

Standard Server

VMware ESXi 4.1

OS (e.g. Linux) — Data Distribution (Server VM) — Driver Software

VMCI

OS (e.g. Linux) — Network Appliance Application Software (Client VM) — Driver with VMCI Interface ①

OS (e.g. Windows) — Network Appliance Application Software (Client VM) — Driver with VMCI Interface ②

OS (e.g. FreeBSD) — Network Appliance Application Software (Client VM) — Driver with VMCI Interface ③

Direct Path

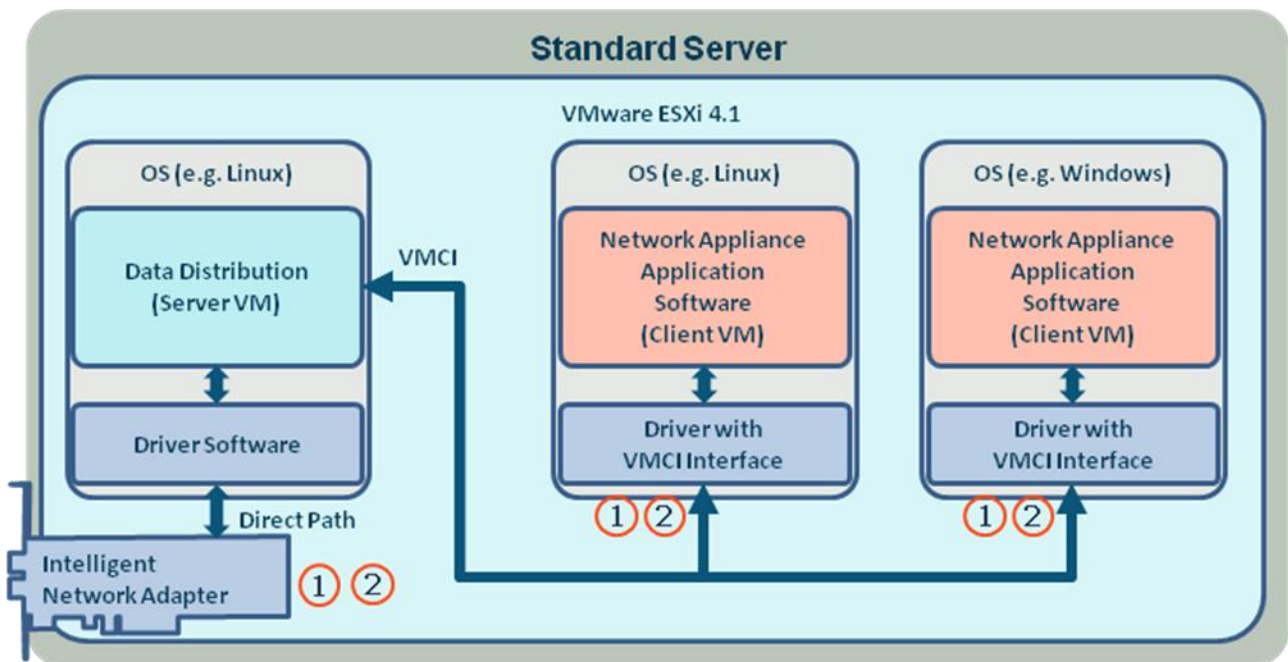Intelligent Network Adapter ① ② ③

① Logical port = VMCI port

Some intelligent network adapters are capable of identifying flows and thus defining logical ports providing specific flow data. These logical ports can be mapped to VMCI ports allowing specific data to be distributed to dedicated network appliances running on client virtual machines. The number of virtual ports that can be supported is limited by the implementation on the network adapter, but can be up to 32.

Sharing data between multiple virtual machine clients

As mentioned earlier, it is not uncommon for multiple network appliances to need to access the same data at the same point in the network at the same time. The captured data needs to be shared and replicated to multiple network appliances.

The data distribution virtual machine can be used to replicate the data captured by the intelligent network adapter to each virtual machine that requires that data. The only limitation is the bandwidth of the VMCI interface itself, which is dependent on the processing power of the supported CPU chipset.

Performance expectations

Implementations of the solutions described above have been made providing a benchmark for expected performance. Napatech has successfully demonstrated that the VMCI interface can support up to 30 Gbps of data replication and distribution to multiple virtual machines. This allows any combination of port speeds and number of virtual clients to be implemented as long as the total consumed VMCI bandwidth does not exceed 30 Gbps.

Benefits of network appliance virtualization

As stated previously, not all network appliances can be virtualized, especially high-speed, high-performance appliances that require all the processing resources available. However, for less processing intensive appliance applications, there is an opportunity for consolidation that is compelling.

One of the advantages of using virtualization for consolidation is that each network appliance can be re-used to a large extent with the same operating system and environment. This also means that it is possible to upgrade the physical hardware without needing to upgrade the supported network appliance virtual machines. As physical servers continue to increase in power and performance, even more appliances can be consolidated onto a single physical server.

As network interface speeds change, it is possible to upgrade the intelligent network adapter to support a higher speed interface without having to change the support network appliance virtual machines. This possibility can also be used to upgrade existing network appliances to support higher speed interfaces in a fast and effective way.

For example, a 10 Gbps network appliance can be upgraded to support 40 Gbps by porting four instances of the network appliance software to four virtual machines running on a single server supported by a single 40 Gbps intelligent network adapter. Four logical ports are created to distribute the data between the four virtual machines making sure that none of the virtual machines receive more than the expected 10 Gbps of data. Thus, a 10 Gbps network appliance becomes a 40 Gbps network appliance without having to re-haul the network appliance application software.

This approach can also be used to upgrade older network appliances supporting legacy operating systems or where resources to update the network appliance application software no longer are available.

Virtualization enables consolidation of network appliances

Consolidation of network appliances is the last frontier of virtualization in the data center. Cost, space and power demands require that network appliances are as effectively and efficiently utilized as their application server counterparts. While many high-speed, high-performance network appliances already make optimal use of the server resources available to them, there are a number of opportunities for network appliance consolidation that can be exploited, especially as we move to higher network speeds and ever more powerful physical servers.

For more information visit us at: www.napatech.com

PR Contact

Regine Hartmann, Eskenzi PR

+44 207 183 2834

Regine@eskenzipr.com