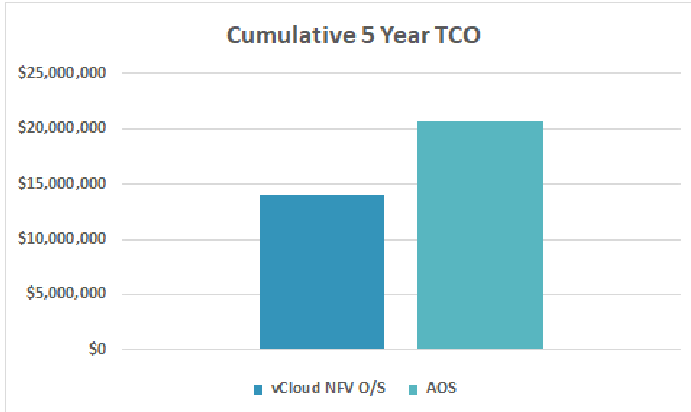
THE TOTAL COST OF OWNERSHIP: ADVANTAGES OF VMWARE vCLOUD NFV OPENSTACK IN THE VIRTUALIZED PACKET CORE OF SERVICE PROVIDERS' MOBILE NETWORKS

AN ECONOMIC ANALYSIS

ACG RESEARCH

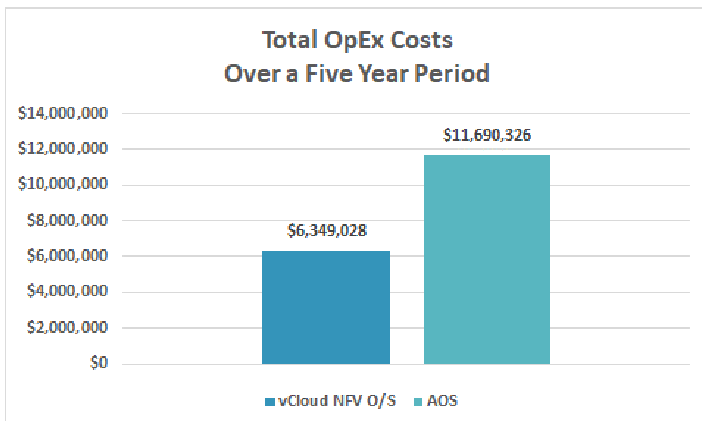
Executive Summary

In a comparison of the total cost of ownership (TCO) of NFV deployments in the evolved packet core of a Tier 1 service provider's mobile network we found the five-year TCO of a deployment based on VMware vCloud NFV OpenStack to be 47% less than the TCO of a deployment based on a comparably configured deployment of an alternative OpenStack solution.



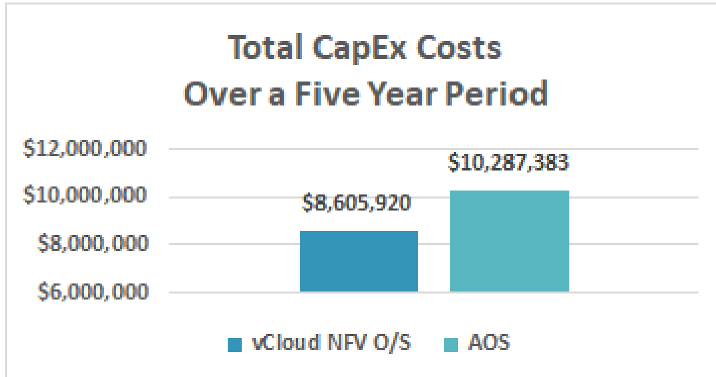
OpEx Savings

Costs were lower in both OpEx and CapEx portions of the TCO. Significant efficiencies in deploying and operating the VMware vCloud OpenStack solution result from its extensive use of automation in provisioning and ongoing life-cycle management, as well as from its integration of a wide range of functionality within the complete solution. Total OpEx for the VMware vCloud NFV OpenStack solution over the five years of the deployment is 54.3% of the total OpEx of the alternative solution.



CapEx Savings

The VMware solution also demonstrated CapEx savings over the alternative. Savings in CapEx were partially based in the use of a smaller number of servers by the vCloud solution than the alternative. The number of servers in five years averages 30% lower in the VMware case. CapEx is also saved by a significant amount of software being integrated into the VMware bundle, which contains licensing costs in its environment compared with the alternative. The total hardware and software CapEx of the VMware solution over five years is 16.4% lower than the total hardware and software CapEx of the alternative.



The total hardware and software CapEx of the VMware solution over five years is 16.4% lower than the total hardware and software CapEx of the alternative.

One interpretation of this substantial overall TCO advantage is that using VMware vCloud NFV OpenStack a service provider can activate approximately three vEPC sites using vCloud NFV O/S for every two sites it could activate using the alternative. In this way the service provider could deploy services for a substantially greater number of subscribers in the same amount of time, using the same amount of money as would be required using the alternative. In an environment in which time to revenue with as many subscribers as possible is a critical success factor for service providers, this is a meaningful and measurable advantage. In this report we describe the environment we analyzed, our conclusions related to it, the substance of the analysis underpinning those conclusions, and the implications of the conclusions for service providers' vEPC deployments.

Table of Contents

Introduction

Comparing the TCO of the VMware vCloud NFV OpenStack and an Alternative OpenStack Solution in the NFV Infrastructure of a Tier 1 Service Provider's Evolved Packet Core

This report outlines our analysis of the total cost of ownership (TCO) of using the VMware vCloud NFV OpenStack in the virtual evolved packet core of a Tier 1 service provider network compared with the TCO of using an alternative OpenStack solution for the same use case. We begin by describing the environment of the networks into which the NFV solutions are being deployed. We proceed to discuss the cost and design considerations involved in using each of the solutions, highlighting both capital and operational expenses for the vEPC. These differences are at the foundation of the economic results service providers are likely to obtain when using either one.

Service Provider Context: Pervasive Embrace of Virtualized, Cloud-Native Design in Highest Priority and Forward-Looking Use Cases

As service providers pursue delivering increased value and innovation to customers in all categories of their businesses they are also focused on using infrastructures that excel at enabling it. In recent years they have begun to use more heavily virtualized, software-driven designs that cloud providers have proven to be so valuable. Although this vision and direction are clear, finding the most efficient and manageable infrastructures to support these deployments remains a challenging task.

Comparing Designs for NFV Deployments

To find the right balance providers need to compare the alternatives that are available and decide which best meets their objectives. They need to consider how they will on-board and deploy the virtual network functions that will give them the functionality they require. At the same time, they need to find the most cost-effective, manageable and scalable infrastructure for their deployment. This typically leads to comparing two types of solutions that are prominent in the market for NFV deployments:

1. One is based on a broadly open source-based combination of components, sourced from one or more open-source communities, and applied to the NFV use case by the operator's staff or by another solution integrator they engage.

2. The other is based on a blend of open-source and independently developed components at various layers of the NFV stack, which allows for flexibility in choosing VNF and at the same time optimizes other attributes of the installation based on innovative designs in other layers of the stack.

As a supplier of virtual system infrastructures for service provider network and IT environments, VMware is keenly aware of the need to strike that balance and compare the characteristics of the alternatives providers have available to them in making plans. VMware has invested in developing vCloud NFV OpenStack, a unique solution for supporting NFV. vCloud NFV OpenStack combines the benefits of participating in an open-source community by integrating OpenStack functions at the virtualized infrastructure management (VIM) layer of the solution. At the same time, it incorporates the functionality of VMware software-defined data centers into its support of the higher OpenStack layers via published APIs and software plug-ins. By doing this it provides a unique combination of openness and optimization that delivers a robust solution for accomplishing the goals of service providers.

To explore the extent to which vCloud NFV OpenStack contributes to achieving these goals, VMware decided to analyze the characteristics of its solution compared with an alternative OpenStack-based solution in important service provider use cases. Deploying NFV into a mobile operator's virtualized packet core is the first of the use cases it analyzed. This report presents the outcomes of that analysis.

Methodology

Focus on Total Cost of Ownership

There are clear architectural similarities, as well as architectural differences, between a solution for the vEPC based on vCloud NFV OpenStack and an implementation based on the alternative OpenStack design. Although our analysis takes those architectural differences into account, the overriding focus of our analysis is on determining the total cost of ownership (or TCO) a service provider can expect to incur when using either one. TCO supplies the most direct way of exploring how a given solution might affect the efficiencies and margins a service provider can obtain when pursuing a given path.

Representative Service Provider Network

To allow our analysis of the two virtual infrastructures to be done on a level playing field, we used the parameters of the same virtual evolved packet core in the deployment of each solution. In this way, an operator would be considering which of the two virtual system infrastructures will generate the outcomes it is interested in for the same networking services. We dimensioned the infrastructure resources (servers, VMs, storage, networking functions) to support a well-known vEPC solution to meet the traffic volumes and transaction counts for the representative network. For the vEPC this included virtualized S-Gateway, P-Gateway, MME, PCRF and operations management functions required for this vEPC. These VNFs are the production workloads being run in the VMs in the deployment.

Table 1 shows several of the attributes of the representative environment that have a direct impact on dimensioning the virtualized packet core.

Attribute	Value in Year 1	Value in Year 5
# of Subscribers in this vEPC	5 million	5.6 million
% Subscribers: 3G	25	23
% Subscribers: 4G	65	75
% 5G Subscribers: 5G	0	1
Average Sustained Rate per GTP Session per Sub Type (4G Example)	25 Kbps	111 Kbps
Total Traffic (in Gbps) through This vEPC	238 Gbps	990 Gbps
Average # of Transactions per Second by Sub Type (4G Example)	54,080	69,847
Total Transactions per Second across All Sub Types for This vEPC	65,225	75,735

Table 1. Network Attributes with Direct Impact on vPC Deployment

Special consideration was given to the following attributes because of the impact they have on the dimensions of the packet core:

- The evolving mix of 3G, 4G, 5G and WiFi based (not shown) subscribers over time. Increasing numbers of 4G, 5G and WiFi attachments in a mobile network will significantly increase the traffic load carried by the operator, causing infrastructure resources to grow along with them.

- And, corresponding increases in the number of connection management transactions per second for each subscriber type over time. This growth adds a second driver for increases in the resources of the packet core (because of the additional processing required to support the larger transaction loads).

Common Physical Elements

In a similar manner, to keep the focus on the software in the two alternative solutions, we used the same physical infrastructure components in each NFVI. This included using the same generation and model of server (on all dimensions: processor type, number of cores, amount + type of memory, on-board storage, and network interface attachments); same storage media; and the same underlying physical network switches in each NFVI and VIM that would be required to deploy either of the solutions. The elements we incorporated are highlighted in Table 2.

Element	Type Employed
Servers	Dell Power Edge R740xd
Storage Arrays[1]	Dell Power Vault MD 3460
Network Switches	Dell S6010-ON

Table 2. Physical Systems Infrastructure Elements Employed in Each NFVI Design

Virtual Infrastructure Elements

The virtual system infrastructures in each solution we analyzed include capabilities needed to run the VNFs in the vEPC use case. These include **virtual compute** (OS/hypervisor and VM/guest processing); **virtual networking** sufficient for the VNF, VIM and network connectivity required in the vEPC; and **virtual storage** suited to the infrastructure, systems management and VNF workload processing requirements of the vEPC. We also included software in each case to support **more complete operational management** of the solutions than is available in the base dashboards and software elements of the VIMs. This includes additional software for monitoring, measuring, and analyzing of the vEPC deployment, as well as software for simplifying configuration management and provisioning (using auto-provisioning based on templates for resource provisioning and upgrades, for example). Service providers are placing increased priority on the manageability of virtualized deployments. Thus, we augmented the content of each solution beyond the core functionality of the NFVI and the VIM to address these needs. The way each implements this set of functions differs, but they each supply it in their own way.

We now describe the two, virtual system infrastructure and virtual infrastructure management solutions supporting the operation of the vEPC. First is VMware vCloud NFV Open Stack (which we will abbreviate as vCloud NFV O/S in the remainder of the report). Second is an alternative OpenStack solution available in the industry today as an option for deploying network services using NFV (which we will abbreviate as AOS in the remainder of the report).

Elements of the vCloud NFV OpenStack Solution

vCloud NFV O/S is an integration of OpenStack community-released software into a virtual infrastructure and systems management solution based on VMware software-defined data center offerings. An illustration of the solution is shown in Figure 1.

[1] In most instances in this analysis we considered server-based storage for the mixture of VM image, logging and other data processing functions required in the solutions. The cases where an external array is involved are in the more fully open-source-based solution where a distributed Ceph-based storage architecture is employed.

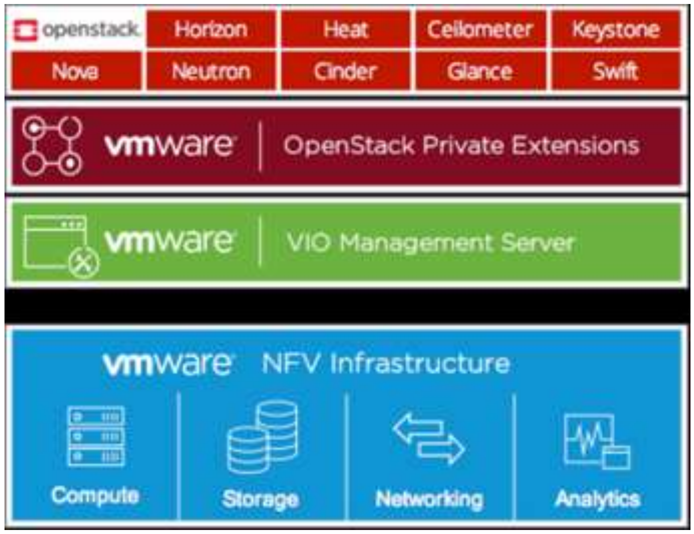


Figure 1. VMware vCloud NFV OpenStack

OpenStack software is integrated via software plug-ins and APIs with VMware SDDC to allow OpenStack services to run in their normal mode while taking advantage of optimizations in the underlying VMware infrastructure. OpenStack compute, storage and virtual machine image management are integrated into corresponding vSphere operations (ESXi and vSAN) via vCenter server. OpenStack networking functions are integrated with VMware NSX to support the networking requirements of the vEPC. The VMware operations management software, designed to simplify operating the SDDC, is included in vCloud NFV O/S (via vRealize Operations Management and vRealize Log Insight).

vCloud NFV O/S is used in this analysis to consider how OpenStack, a widely desired virtual infrastructure management solution in the service provider market, can be deployed in conjunction with an optimized virtual infrastructure design such as VMware SDDC.

Elements of the Alternative OpenStack Solution

The AOS infrastructure is based on the distribution of OpenStack by another supplier combined with additional virtual infrastructure and management applications to construct a vEPC deployment that is as similar as possible to the vCloud NFV O/S functionality. The infrastructure in the AOS includes a current distribution of Linux and kernel-based virtual machine (KVM) for compute; open virtual switch (OVS) software for networking; and Ceph virtualized and software-defined storage for image management, systems management, and VNF operations.

As with vCloud NFV O/S, a distribution of OpenStack is used to manage the resources for the VNFs. All OpenStack services required to support the VNFs are included, from Nova (compute), Cinder (block storage), and Neutron (virtual networking) to Ceilometer (telemetry), Horizon (dashboard monitoring) and Heat (orchestration).

We also included the configuration management and auto-provisioning system, Ansible, to simplify managing the configurations. To support event and trend analysis we included Splunk data collection and analysis software as a part of the AOS.[2]

Analysis of the Two Alternative Virtual Infrastructure Designs

To analyze the TCO of each solution we took a holistic view of the costs in using each for the operators, from conceptual framework and design, to test and validation, to deployment, operation and life-cycle management in the infrastructure over five years. The two cost categories we analyzed are capital and operating expenses (CapEx and OpEx), which combine into the cumulative TCO.

CapEx of the Alternatives

CapEx in each case includes the costs for acquiring the physical (hardware-based) and the virtual (software-based) elements required to deploy.

Hardware CapEx of the Solutions

The hardware elements employed in the vEPC include the servers, storage, network switches, racks, cables and connectors required for each design. To dimension the hardware for each we used a combination of the traffic-handling and workload-processing requirements of the vEPC (driven by variables, including those summarized in Table 1), the hardware required by the VNFs themselves, and the hardware required for the VIM and virtual system infrastructure software of the supplier. Each software element has its own requirements for the number of VMs needed to run it, the number of virtual CPUs (vCPUs) it requires, the amount of memory, storage and other network capacity (based on throughput) it needs to define its configuration. We factored in each of these variables to arrive at the number of servers, amount of storage, and configuration of physical network infrastructure required in each solution to support the vEPC.

As one might expect, there is a different amount of hardware required to support one solution versus the other over the course of such a deployment. In this regard, the factors

[2] In the model we included the option to have Ansible and Splunk active or not, so an analysis of TCO could include cases where either or both would be desirable for an operator to employ is accounted for. The instance of the analysis we are summarizing in this report includes the use of both Ansible and Splunk in the deployment, as this is the most equivalent composition of functionality for comparing with vCloud NFV O/S. It shows a five-year cumulative TCO for vCloud NFV O/S that is 33% lower than the five-year cumulative TCO of the AOS. When Ansible and Splunk are **not** included in the AOS deployment, the five-year cumulative TCO of the VMware solution is 29% lower than the TCO for the AOS, a difference of 4% (a modest but measurable amount). The main point is that the construction of what constitutes the environment the service provider wants to compare will have some effects on the TCO outcomes it will achieve. This is normal. We are pointing out the composition of the environment we investigated for equivalence in our analysis.

determining the amount of hardware each solution needs exist along three dimensions. First is that, because we analyzed the same vEPC software for each design, the amount of hardware required to support the vEPC software is identical in each case. The differences between the hardware requirements for the two solutions, then, comes from differences in two additional areas.

The first is in the management and control portion of the solutions. These include the OpenStack, virtual infrastructure management and operations management software in each. The amount of hardware in the control pool of each solution is not significantly different. The second source of difference is in **the hardware that is needed to run the virtual infrastructure software**: ESXi, vSAN and NSX in the vCloud NFV O/S case; Linux, KVM, OVS and Ceph in the AOS case. There are significant differences between the alternatives in these categories over five years, and they have a meaningful effect, because it is the virtual infrastructure that needs to grow and support the traffic as the network of the service provider evolves.

We show the overall cost of the hardware needed in each of the solutions and elaborate on the sources of these differences in the section Sources of the CapEx Differences.

Figure 2 shows a summary of the number of servers required in the vEPC in each of the two solutions.

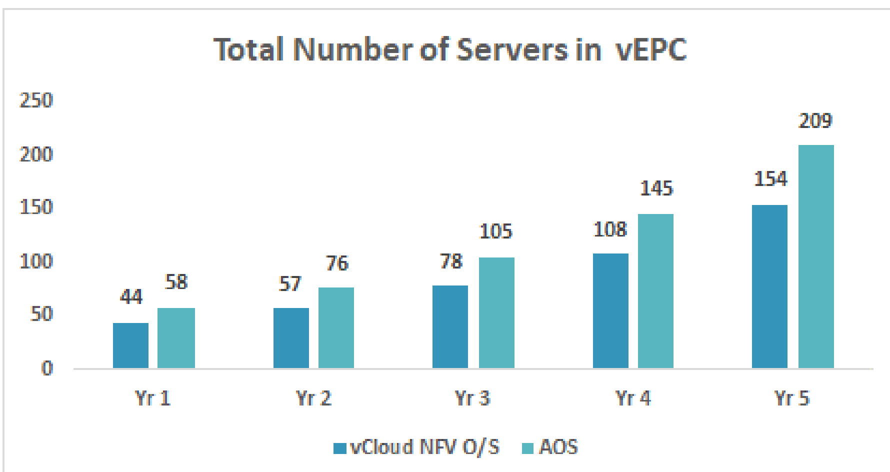


Figure 2. Total Number of Servers Required in Each Solution for Each Year in the Analysis

The vCloud NFV O/S solution requires a smaller number of servers during each year of the deployment, ranging from 31% fewer at the start to 35% fewer in the final year. Proportionally, most of the difference is driven by the increasing number of VNFs required in the virtualized packet core to support the provider's traffic, augmented by the differences in the resources required by the software in the two infrastructure solutions.

The cost implications of this different amount of hardware required by the two alternatives is shown in Figure 3.

The total hardware cost for the vCloud NFV O/S design is 60% of the total hardware cost for the AOS.

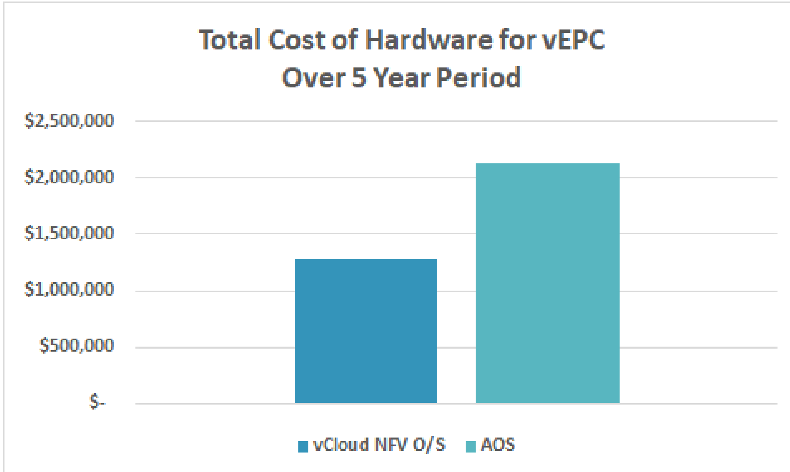


Figure 3. Total Cost of Hardware for the vEPC Deployment over Five Years[3]

Software CapEx of the Solutions

The second major component of CapEx is the costs of the software of the solution. CapEx for software is incurred via licensing and subscription fees for the software of the suppliers. **Each solution uses bundles** for its OpenStack and virtual system infrastructure software offerings. Both bundles include a downstream distribution (from the OpenStack community) of OpenStack and certain virtual systems infrastructure software (such as OS or hypervisor software and related systems- management modules). In vCloud NFV O/S, NSX is licensed separately from the bundle. In AOS, Ceph, Ansible and Splunk (when employed) are licensed separately from the bundle.

Charging practices vary based on the module or the package. Some software is licensed on a per-server-socket (or per-CPU) basis, while other software is licensed on a per-full-physical-server basis (including both sockets or CPUs of a server in the price). Other software is licensed based on the number of nodes in the installation it is supporting. And further, timing and length of the charges varies, some charges being annually based, others having a multi-year structure. In each case we used the licensing model employed by the supplier as applicable to the vEPC deployment case (length of time, number of nodes involved, deployment of each module according to its design).

We did **not** include the cost of the vEPC (VNF) software licenses, as the purpose of the analysis is to focus on the costs of the virtual system infrastructures and the resources they consume to support the vEPC. We **did** account for the physical resources required to support the vEPC VNFs, along with the suppliers' virtual infrastructure software needed to run those resources so we would have a full accounting of the NFVI into which the

[3] Includes the total costs for server, storage, network, rack and cable/connector hardware across the five years of the analysis for each of the solution designs.

VNFs are deployed. The vEPC (VNF) software licenses are the only components of the configuration we excluded (ensuring the comparisons are based on the same assumptions).

Figure 4 shows the total cost of software for each solution across the five years of the deployment.

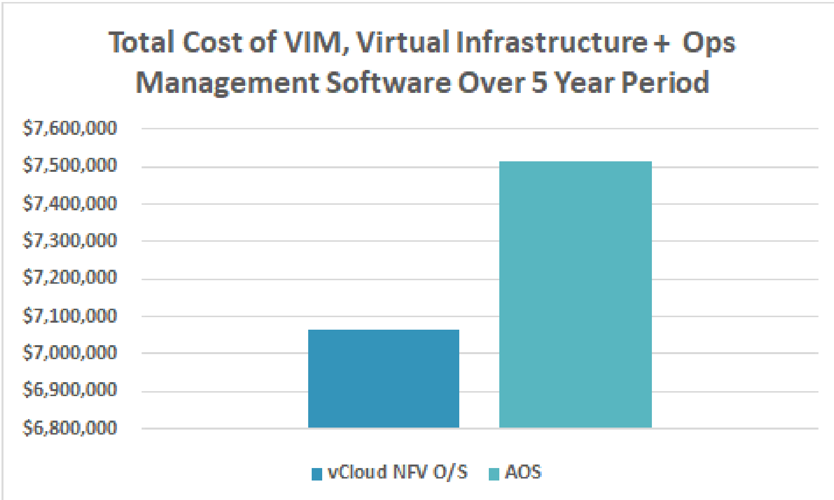


Figure 4. Total Cost of Software in Each Solution across the Five Years of the Deployment

As with the hardware costs, **costs for software reflect the growth in resources in the vEPC over the five years of the analysis**. As we can see the total software CapEx for the vCloud NFV O/S solution is 6.1% less than the software CapEx for the AOS.

Combining the two CapEx elements, cost of hardware and software for the two solution alternatives, we see in Figure 5 that **the capital costs of the vCloud NFV O/S solution in this configuration are 16.4% lower than those for the AOS**.

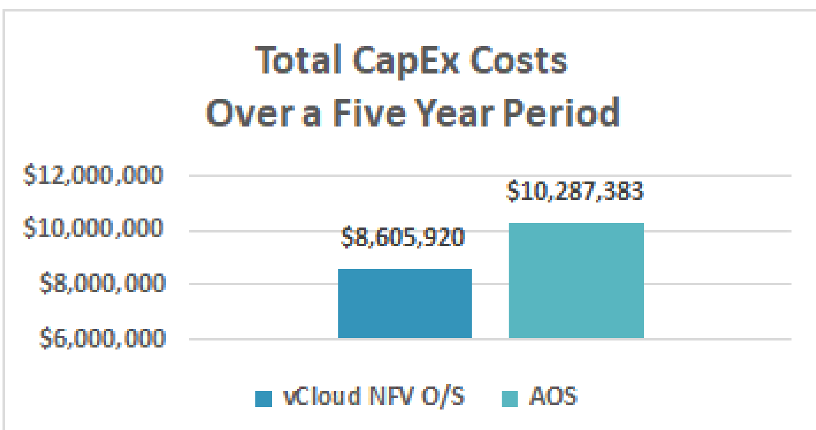


Figure 5. Total CapEx of the Two Solutions over Five Years

Sources of the CapEx Differences

There is a difference in the CapEx of the solutions in both hardware and software. On the hardware side, there are two sources of the lower cost for vCloud NFV O/S.

The first is the relative efficiency with which ESXi (supplying hypervisor and virtual machine support in vCloud NFV O/S) and KVM (supplying virtual machine support in the AOS) manage the processing of their workloads. Tests and deployments of ESXi have shown it provides greater efficiency managing memory needed by VM workloads compared with KVM. The level of efficiency advantage varies based on workload; online transaction processing, for example, has a different mode of operation than I/O-centric virtual networking functions running in a vEPC. Applying those fundamentals, however, in a deployment using, for example, 100 servers running ESXi, one would need a proportionally larger number of servers running KVM to support the same workloads with the exact number based on the gain associated with those workloads. To be conservative in the vEPC case, we used an average of 10% greater processing efficiency in the ESXi servers supporting VNFs, supplying a modest efficiency advantage for vCloud NFV O/S using ESXi compared with the AOS using KVM. This is one source of the lower hardware CapEx for vCloud NFV O/S in this use case.

The second source of lower hardware CapEx for vCloud NFV O/S in the way virtual storage is implemented in the two alternatives. vCloud NFV O/S employs VMware vSAN software-defined storage. vSAN is a hyper-converged implementation, meaning it is tightly coupled with ESXi and uses local server storage and memory for its operations while providing an abstracted, logically distributed operation to support an efficient storage pool for a variety of users and applications. In the vEPC these include OpenStack images using Glance image management, as well as the data base, monitoring and configuration information for the vEPC and its infrastructure. vSAN uses the server-based storage of the servers in the vEPC and does not require the use of additional servers or storage arrays to do its work.

Storage in the AOS is based on a more distributed implementation using Ceph.[4] Ceph's support for OpenStack and the vEPC is based on a distributed architecture using daemon servers, also known as object storage device, servers (OSD). Individual VNFs and the VMs in which they are running access storage as clients of the OSD servers from other servers in the configuration, which handle resource mapping and storage management on behalf of their clients. OSD servers map a set of external storage arrays into the vEPC and its OpenStack services. This implementation is costlier (with respect to server and storage infrastructure required) than the more compact vSAN design in vCloud NFV O/S. This is a second source of lower hardware CapEx in the vCloud NFV O/S case.

There is also a difference in software costs that impacts the CapEx of the solutions. There are several differences in the way the licensing occurs in the vCloud NFV O/S compared with the AOS. In the end it is the degree of integration and the bundling that is employed in the vCloud NFV O/S solution that gives it a modest advantage from the software CapEx

[4] A view of the general case Ceph storage management architecture is available at: https://ceph.com/.

point of view over the AOS. We describe the major differences in software licensing practices between the solutions in the next section and indicate the impact of those differences on the software costs in each case.

The first is whether the cost for the virtual infrastructure software (hypervisor or OS, for example) is based on a per-socket or a per-server basis. In vCloud NFV O/S, licensing is based on a per-socket basis, while AOS is generally based on a per-server model. These differences create a modest per-server software licensing cost advantage for the AOS for the portions that are included in that part of its solution.

The second is based on what software is included in the solution bundle and what is not. In the vCloud NFV O/S, NSX is not included in the bundled offering (separately charged) while in the open source-based offering, OVS is included in the per-server OS software subscription fees. Conversely, in the AOS, analytics and certain management software modules are not included in the baseline bundle. The costs for these incremental software modules increase significantly the overall cost of the AOS software and tend to offset its advantage from the per-socket or per-server practice.

It is the degree of integration and the bundling that is employed in the vCloud NFV O/S solution that gives it a modest advantage from the software CapEx point of view over the AOS.

The way storage is supported in each solution differs. In the vCloud NFV O/S case, although vSAN conserves hardware by not requiring dedicated servers and storage arrays, it also brings a per-socket licensing charge that adds to the total vCloud NFV O/S software cost. By contrast, although Ceph in the open source-based solution introduces greater hardware costs by its distributed configuration, its total software cost does not contribute to the total of that solution in the same manner as the vSAN licensing does for VIO.

Combining these elements into a full view of the software costs of the deployment, the software for the vCloud NFV O/S deployment is 6.1% less costly than the software for the equivalent AOS functionality.

In total, combining both hardware and software costs into an integrated view of the relative CapEx of the solution, we determine the cumulative five-year CapEx of the vCloud NFV O/S solution is 16.4% less than the CapEx of the fully open-sourced design.

OpEx of the Alternative Designs

The second and more proportionally impactful category of TCO we analyzed about the solutions is the set of OpEx involved in deploying them in the use case. OpEx largely determines the efficiency with which the service provider can run the solution and use it to support the services it is offering with it. It has a significant contribution to the margins that can be earned by the operator for its offerings. In the use case we analyzed, the impact of the OpEx of the solutions is approximately twice the impact of their CapEx on their cumulative TCO over five years.

> *The impact of the OpEx of the solutions is approximately twice the impact of their CapEx on their cumulative TCO over five years.*

OpEx is largely composed of the cost of time of people performing the tasks to design, test, deploy, operate, and expand the solution being used. It also includes recurring costs such as electricity for powering and cooling the infrastructure and the cost of real estate or physical space to house the resources that have been deployed.

OpEx Model in Our Analysis

To compare the solutions, we constructed a personnel team representative of ones that service providers are using to do their NFV deployments, including individuals from disciplines with the skills necessary at each stage of implementation.[5] This includes personnel with architecture and design, integration and test, and operations skills, and their management. The teams have members with expertise in server, storage and networking (both virtual and physical), as well as mobile packet core functionality for operating the mobile network.

Based on this composition, we analyzed workflows and levels of effort to do the work to deploy the vEPC in each design. The dimensions of each solution being worked on (number of servers, switches, amount of storage, and amounts of control and operational software required in each case) are based on the same service provider network profile.[6]

During the design phase, the software for management and control and software for infrastructure support (hypervisor, OS, virtual networking, virtual storage) is specified to support the VNFs that will be run. In vCloud NFV O/S this involves the management cluster of the deployment, including Integrated OpenStack Manager, vCenter Server, NSX Manager, vRealize Operations Manager, vRealize Log Insight, and additional modules for control of the infrastructure for the vEPC. Similarly, the needs of the resource cluster (to run the VNFs for the vEPC) and the Edge Services cluster (to supply networking and firewalling services in the deployment) are specified.

[5] A list of the representative personnel categories whose work we analyzed in our analysis is provided in *Sources of OpEx Differences*.

[6] Refer to Table 1 for the key dimensions.

In the AOS deployment, the controller and compute pools for the solution are designed, supporting both the OpenStack and the underlying virtual systems infrastructure. Incremental management functions, including Ansible for auto-provisioning and Splunk for a variety of traffic and application analytics, were factored in.

Using similar granularity in tasking and staff, we analyzed the test and integration, deployment to production, and operations management costs of the solutions across the five years of the deployment. This included considerations for growth in subscriber traffic (and thus growth in the resources required to support it), upgrades based on the release cycles of the OpenStack and other software components, work involved in monitoring and fault repair, and measurements in service level agreement (SLA) monitoring and enforcement. In short, we analyzed the full cycle of costs involved in supporting the operation of the two designs.

OpEx Cost Comparison

Figure 6 shows a comparison of the complete OpEx costs of the two designs over five years. Our analysis illustrates a substantially lower cost of operation for the vCloud NFV O/S infrastructure for the vEPC compared with the cost of operation of the AOS. **As shown in Figure 6, the total OpEx of the vCloud NFV O/S infrastructure is 54.3% of the total OpEx cost of the AOS.**

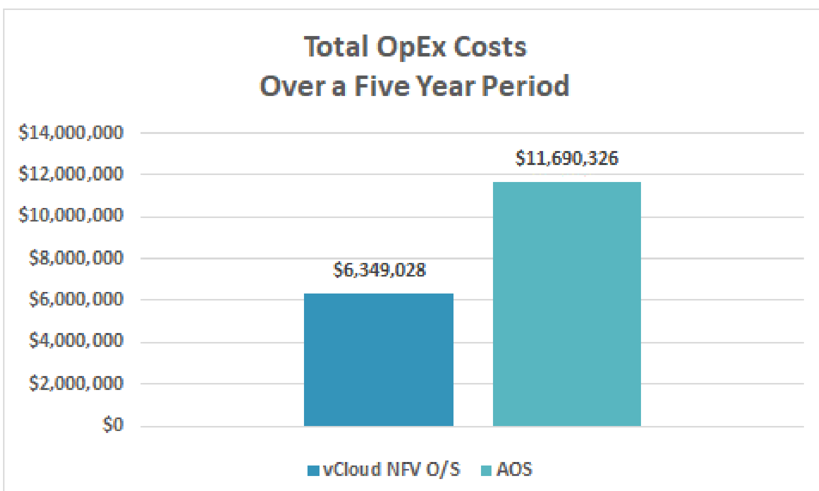


Figure 6. Total OpEx Costs for the Two Solutions over Five Years

Given the magnitude of this difference it is important to identify the sources of the lower costs in the vCloud NFV O/S deployment and the reasons they exist. Figure 7 shows a more granular breakdown of the OpEx of each solution. As one can see in each category, there is a lower amount incurred in the vCloud NFV O/S case versus AOS.

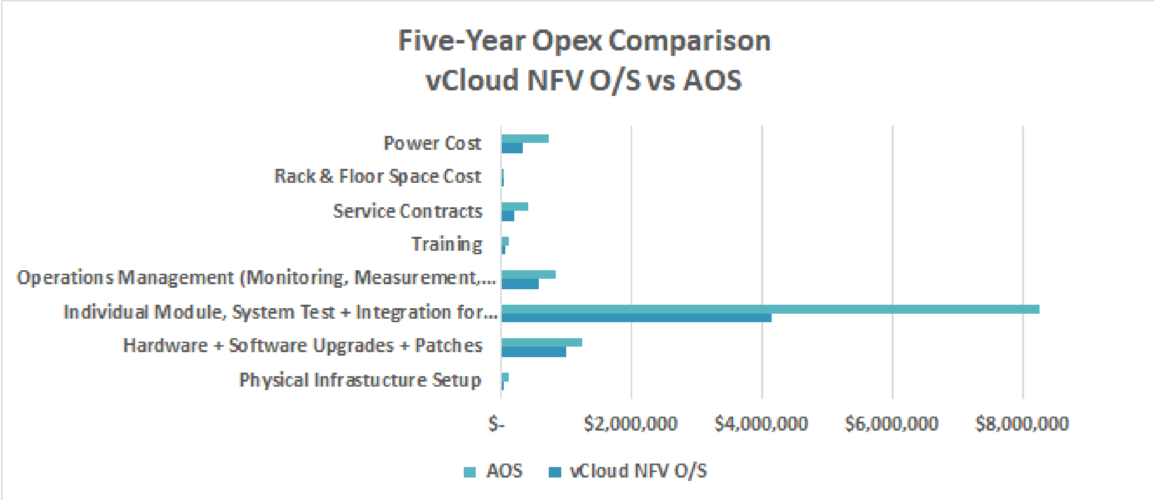


Figure 7. Five-Year OpEx Costs by Principal OpEx Category of the Two Solutions

Certain costs, notably costs of electricity, space, and physical infrastructure setup, are related to the smaller physical infrastructure vCloud NFV O/S requires. It simply takes less time to install and activate a smaller number of servers and other infrastructure elements than it does to install the larger resource set. Those differences are reflected in those components of the costs.

However, three other categories of OpEx present significantly larger differences and are more important when considering the relative efficiency of the solutions.

- Cost of system integration, test, and deployment into production.
- Costs of running the two solutions across a full life cycle of operation:
  - Costs of operations, management (monitoring, measurement, fault diagnosis/resolution).
  - Costs of implementing system upgrades (capacity expansions, software and hardware upgrades, maintenance + patches). Together these categories account for nearly 80% of the OpEx advantage the vCloud NFV O/S solution holds.

In general, the cost of performing these tasks (integration, test, operations and upgrades) are influenced by the degree of automation and streamlining of steps toward a result that either solution has achieved. This is indeed the case when comparing the vCloud NFV O/S with the AOS. Given the importance service providers are placing on the efficiency and manageability of virtual infrastructures they are deploying to support NFV, clarifying the reasons for these differences becomes that much more important.

At a high level, the degree of automation and simplification that has been developed in vCloud NFV O/S to support the workloads in an OpenStack-based deployment of VNFs is the primary reason the efficiency differences exist.

Sources of the OpEx Differences

We identified five principal sources contributing to the lower OpEx of vCloud NFV O/S compared with the AOS. We describe them in the order in which one might encounter them in a deployment with a final, more pervasive source saved until last.

Four sources of difference are technically based. Their effect is to save time for staff doing the work in deployments. Time savings on the tasks produces lower cost of operation and creates the opportunity to do more work with the money saved, generating additional benefits.

The four attributes of vCloud NFV O/S we identified as having the greatest contribution to time savings are:

- Installer automation
- Plug-in integration of VMware SDDC with OpenStack
- Hyper-converged infrastructure
- Mature and functionally rich virtual infrastructure management software

The fifth source is from the broadly available, proportionally less costly pool of VMware architects and admins present in the market, based on VMware engagements and penetration into virtual IT in service provider and other industry segments. Using a common platform, such as VMware SDDC for virtual application **and** virtual networking services, creates efficiencies by applying well-understood techniques to neighboring workloads in a broadly deployed infrastructure. This is an area in which the increasing use of virtual IT solutions as the foundation for the adoption of NFV by the telecommunications industry can yield dividends. This is true across every category of personnel involved in a deployment such as the use cases analyzed, allowing them to work on adapting to the new workload types that NFV presents more efficiently.

The degree of automation and simplification that has been developed in vCloud NFV O/S to support the workloads in an OpenStack-based deployment of VNFs is the primary reason the efficiency differences exist.

By contrast when a service provider decides to use a more completely open-source-based virtual system infrastructure the provider is not able to benefit from as widely developed a pool of expertise as is the case for a VMware-based solution. The upshot is that a smaller number of equivalently talented architects and engineers is available to meet the level of interest in the markets for their services, tending to drive up the cost of their time. Based on this market condition, at the baseline in our OpEx calculations we apply an average of 30% higher cost for personnel whose skills specifically apply to the deployment of the AOS based virtual systems infrastructure. Although not the sole determinant of lower OpEx for vCloud NFV O/S, it is a significant one.[7]

We now describe the technically-based sources of the difference in OpEx in the order we introduced them. We describe the source of the difference first and then illustrate the effect of those differences on the workflows involved in the deployments and their impact on OpEx.

Installer simplification and automation. Based on learnings from inputs from customers in its virtualized data center business, as well as on its own engineering insights, VMware has developed an appreciation for reducing the complexity of tasks in deploying virtualized system infrastructures. By streamlining workflows to select the shortest paths to ready and combining variables into simplified selection steps, vCloud NFV O/S selects the crucial elements of the OpenStack services needed to support a set of workloads (such as VNFs included in a vEPC) and activates them in a streamlined, prompted manner that minimizes CLI keystroking and maximizes application of engineers' insights into the configuration. This is done by embedding process and configuration intelligence into the vCloud NFV O/S OpenStack Installer that in combination with vSphere, vSAN and NSX produce a highly efficient deployment process. The impact is experienced in test and integration, as well as in production and life-cycle management (upgrades, capacity expansions, and activation of new service features).

Operational simplifications from plug-ins. An additional area of simplification is integrations between components of OpenStack, such as Nova (compute), Cinder (block storage), and Neutron (networking), with corresponding components of the VMware software-defined data center in the vCloud NFV O/S solution: vSphere, vSAN and NSX. Via software plug-ins, these SDDC elements interpret OpenStack commands and implement them using VMware-optimized procedures within the SDDC. The significance of this is in reducing the steps to perform a configuration or resource management function using OpenStack native terminology at the dashboard/user interface level and having them executed automatically under the covers by the VMware components supporting the workloads in the infrastructure. Time savings from these integrations, again, contribute to efficiencies in test, integration (with VNFs, networks and OSS/BSS), upgrades, and operations.

[7] In parallel, to gauge the effect of having personnel costs be exactly equal (in order to observe what the OpEx of the two solutions would be in a situation where the personnel costs for an operator would be the same), we calculated that the reduction in OpEx for the alternative solution would be 8.3% of its total OpEx, and in that situation the OpEx for VMware vCloud NFV O/S is 59% of the OpEx for the AOS, a modest 5% lower advantage than the case when the difference in personnel costs is at the higher percentage difference, yet still very substantial.

Simplifications based on hyper-converged system architecture. Another source of efficiencies in vCloud NFV O/S is its leverage of hyper-converged functionality in vSAN, ESXi, and (increasingly as time progresses) NSX. Hyper-converged in this case means integration of functionality for virtual infrastructure support into hypervisor modules, making them accessible to VM workloads using local host-based operations versus implementing them via a more distributed and (in many cases) more complex solution. Managing both compute and storage, for example, under a common control point such as vCenter Server, as is the case for vSphere and vSAN in vCloud NFV O/S, creates incremental efficiencies over the life cycle of the deployment of the solution. When managing the deployment of VNFs in a service provider's production mobile network, having these simplifications designed in to the infrastructure being used is a valuable attribute.

Mature and functionally rich virtual infrastructure management software. In parallel with the automations cited previously, vCloud NFV O/S benefits from functionality in vRealize Operations Management and vRealize Log Insight software. vRealize OM and vRealize LI bring important monitoring, performance measurement, capacity management, security analysis and SLA measurement functions to vCloud NFV O/S that bolster the toolkit available to test and operations teams. Because these tools have been designed for close integration into vSphere and the VMware SDDC and have been extended to provide support specifically oriented to management of an OpenStack environment supported in the SDDC, they supply a valuable set of functions to help optimize the performance and the efficiency of the workloads being run in the NFVI. It is this close integration that allows them to contribute substantially to efficiency and streamlining of tasks.

The sources of these efficiencies are in the automation, platform integration and management application capabilities of the vCloud NFV O/S implementation. Together they produce the time efficiencies identified.

By comparison in the AOS, it is possible to assemble a collection of tools from a combination of suppliers (for example, log analysis for subscriber and service analytics using Splunk in addition to the OpenStack and NFVI software in the deployment). However, doing so adds costs in both CapEx (licensing) and OpEx (integration, test, operations and life cycle management) that are not present in the VIO environment, where the equivalent functions are built in to the solution and simplify operations based on the integration.

This combination of functions contributes to efficiencies across the OpEx life cycle (alongside the personnel costs mentioned). As an indication of their contributions to the efficiency of operations at different points in the life cycle, the greatest impacts are in the initial installation and testing of the VIM (OpenStack) and virtual infrastructure, where the work to install and test the vCloud NFV O/S combination is 36% of the work required in the AOS; and in the integration of the VNFs into the NFVI and VIM and end-to-end testing of the complete solution, where the time required for integration and test of the solution in vCloud NFV O/S case is 34% of the work required in the alternative.

The sources of these efficiencies are in the automation, platform integration and management application capabilities of the vCloud NFV O/S implementation. Together they produce the time efficiencies identified.

Cumulative Five-Year TCO of the Two Alternatives

Combining the two sources of cost in each solution (CapEx and OpEx) our analysis shows the cumulative total cost of operation of vCloud NFV O/S solution in the virtualized EPC use case is 47% less than the cumulative TCO of the AOS.[8]

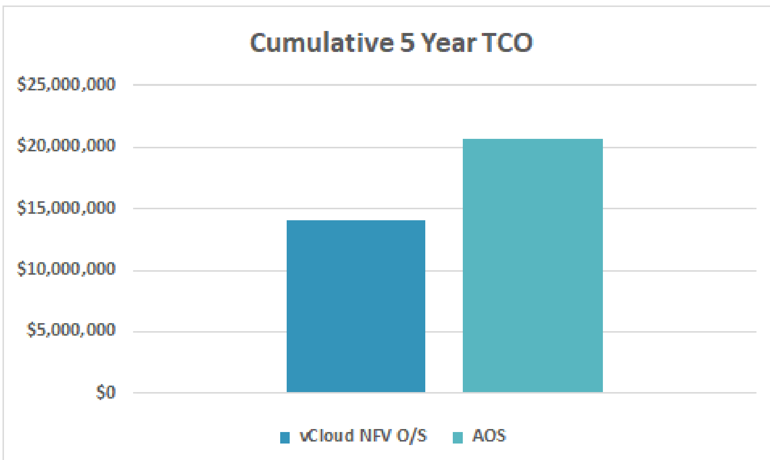


Figure 8. Cumulative Five-Year Total Cost of Ownership of the Two Alternative Designs

One way to appreciate the value of this difference is to consider that a proportionally larger amount of work can be performed by a service provider's staff when working with a solution based on this design compared with its alternative. For example, for every two vEPC sites that could be deployed using the AOS, approximately three vEPC sites of the same size could be deployed using vCloud NFV O/S. Looked at from an additional lens, the provider could support a substantially greater number of subscribers at the same cost using vCloud NFV O/S, or could support the same number of subscribers for a lower cost using vCloud NFV O/S instead of the alternative. In either case, it is the efficiency of the underlying solution that would make the results achievable.

[8] This is derived by taking the difference between the cumulative TCO of the vCloud NFV O/S solution and the cumulative TCO of the AOS and dividing that difference into the cumulative TCO of the vCloud NFV O/S solution. This yields the percentage of the investment in the vCloud NFV O/S solution that is represented by what the operator saves in not pursuing the AOS.

Implications for Service Providers Deciding on Their Direction for Virtual System Infrastructures in their NFV Deployments

Service providers globally are clearly looking for ways they can increase the flexibility and efficiency with which they bring new services and applications to market. Using open, virtualized and cloud-native designs for their applications is the dominant mode in which they are pursuing this goal. Supporting the virtualization of their network functions using an open workload management system, such as OpenStack, is a leading candidate for how many new services and functions are being enabled. The unique deployment model of the VMware vCloud NFV O/S solution allows service providers to benefit from the openness of VNF and orchestration that OpenStack provides, while at the same time benefiting from the production tested and evolved virtual systems infrastructure provided by VMware software-defined data center infrastructure and its operations management applications. Especially in environments where VMware virtual infrastructures have been employed in service providers' IT operations to date, the benefits of carrying those efficiencies and procedures into NFV deployments can be substantial.

> *These are economics that should not be ignored. They indicate that vCloud NFV O/S solution merits significant consideration for use in service providers' vEPC deployments.*

The results in our analysis clearly demonstrate that exploring this path is an option that service providers should consider in creating the plans for their virtualized network services. Our analysis shows that a vEPC deployment based on vCloud NFV O/S:

- Uses an average of 30% fewer servers in its deployments than an alternative OpenStack solution
- Requires 16.4% less CapEx than the alternative design
- Consumes 54.3% of the OpEx of the alternative in running its deployment
- Exhibits a 47% lower **cumulative** TCO over five years of operation

These are economics that should not be ignored. They indicate that vCloud NFV O/S solution merits significant consideration for use in service providers' vEPC deployments.