Reference Architecture: QxVDI VMware Edition-HC with NSX®

Release Date:1. Dec 2017

Version 1.1

CONTENTS

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH QUANTA CLOUD TECHNOLOGY (QCT) PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN QCT'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, QCT ASSUMES NO LIABILITY WHATSOEVER AND QCT DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF QCT PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY QCT, THE QCT PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE QCT PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Quanta Cloud Technology (QCT) may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." QCT reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Contact your local QCT sales office or your distributor to obtain the latest specifications and before placing your product order.

1. Introduction

The Software-Defined Data Center (SDDC) is characterized by server virtualization, storage virtualization, and network virtualization. Server virtualization has already proved the value of SDDC architectures in reducing cost and complexity of the compute infrastructure. VMware NSX® network virtualization provides the third critical pillar of the SDDC. It extends the same benefits to the data center network to accelerate network service provisioning, simplify network operations, and improve network economics.

Virtual desktop infrastructure provides end users to access virtual desktops, applications, and online services through a single digital workspace. VDI with NSX® provides flexible control, delivery, and protection on datacenter environment. The built-in security policies can be dynamically applied to the workload units and the virtual networks on demand can simplify and dynamically protect data center infrastructure and workloads by separating each unit.

1.1 Purpose

The purpose of this document is to showcase the design, configuration, validation, and scenarios of QxVDI VMware Edition-HC with VMware NSX® solution on QCT server T41S-2U with existing VMware Horizon® infrastructure. To verify the optimized solution, the resource consumption of VMware NSX® on the QxVDI VMware Edition-HC is demonstrated by using Login VSI tool.

1.2 Scope

The topics and objects in the document are to:

- Design the architecture of the solution.
- Demonstrate the primary scenario of the solution.
- Illustrate the test results by using Login VSI.
- Provide a reference to scale the network virtualization in data center.

1.3 Audience

This reference architecture provides a guidance for customers, IT architects, administrators, and consultants involved in the phases of choosing, planning, and designing a network secured and virtualized Horizon® VDI. It is recommended that the reader should have:

- A solid understanding of VMware vSphere®.
- A solid understanding of VMware Horizon®.
- A solid understanding of network knowledge.
- A solid understanding of VMware NSX®.

2. Solution Overview

2.1 QxVDI VMware Edition-HC with VMware NSX®

Quanta Cloud Technology (QCT) QxVDI VMware Edition-HC is a pre-validated hyper-converged appliance powered by VMware Horizon® software. This solution uses a 2U 4-node server to create an easy-to-deploy building block for Software-Defined Data Center (SDDC). QxVDI VMware Edition-HC natively integrates compute and storage resources into a hyper-converged infrastructure, offering an exceptional Virtual Desktop Infrastructure (VDI) user experience with ease of management. QCT QxVDI VMware Edition-HC with NSX® is intended to:

- Virtualize and isolate network in data center.
- Centralize security policy controls.
- Minimize the demand of third party security software.
- Integrate the existing workloads with new VDI seamlessly.

The detailed scenario and validation of this solution will be described in the following sections. For more solution information, please visit: http://www.qct.io/solution/index/Desktop-Virtualization/QxVDI-VMware-Edition-HC

3. Solution Architecture

3.1 Architecture Topology

The QCT QxVDI VMware Edition-HC with NSX® utilizes vSphere® as the cloud infrastructure platform. Horizon® and NSX®, which respectively represent desktop virtualization and network virtualization software are installed with vSphere® on QCT T41S-2U server. vSphere® provides the functions of software defined data center such as clusters, hosts, VMs, distributed switches, and data store. Horizon® provides virtual desktops and applications for end users, and also achieves the centralization of desktop management and server-based resource pooling. NSX® provides centralized and logical networks to secure data center objects. It brings some benefits such as the abstraction from underlying IP network, centralized network management, etc.

The QxVDI VMware Edition auto-deployment tool is designed to provide an automatic deployment of virtual desktop infrastructure. This tool simplifies the configurations, provides a user-friendly interface, minimizes human errors, and reduces the overall deployment time. In the solution topology, vSphere® is installed on the QCT T41S-2U four-node server with configured vCenter server®, vSAN™, and distributed switch, as shown in Fig. 1. Horizon® services including connection server, composer™ server, and active directory DNS server are established to provide a desktop pool service for end users. Simultaneously, the NSX® components, Manager™, Edge™ service gateway, distributed logical router, logical switches, and distributed firewalls are created to isolate and secure the virtual desktop infrastructure.

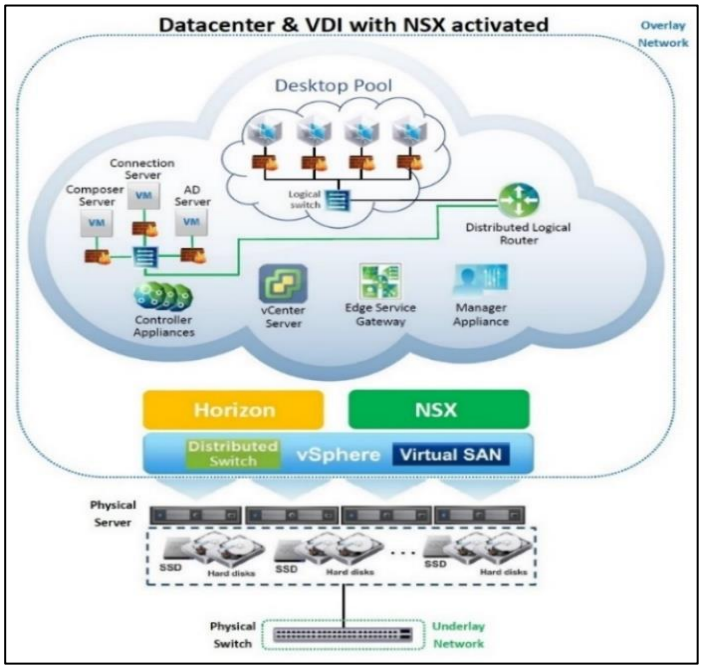

Figure 1. Solution Architecture Topology.

3.2 Hardware Configurations

QCT QxVDI VMware Edition-HC adopts the server – QuantaPlex T41S-2U as a foundation (see Fig. 2). The features of T41S-2U are:

- Ultra-dense design equipped with four independent nodes.
- Hight flexibility to set up different workloads independently in one 2U-shared infrastructure, providing optimal data center performance.
- Operation with Intel® E5-2620 v4 and DDR4 2133 RAM technology.
- Economical total cost of ownership (TCO) due to the shared infrastructure such as cooling and power supply.
- Modularized design. For example, the network mezzanine cards can fit into every QCT server system to reduce the complexity of the system availability options.
- High serviceability to reduce service time and cost.

The hardware specification is carefully chosen to fit all the requirements of the software platform, as shown in Table 1.

Table 1. QxVDI VMware Edition-HC Hardware Configuration.

Server Model Name		QuantaPlex T41S-2U
Server Nodes		4 Nodes
Server Physical Resource	CPU	(8) Intel® Xeon® processor E5-2620 v4
	SSD	(4) Intel S3710 SATA 400GB 2.5”
	HDD	(20) HGST SAS 1.2TB 2.5”
	RAM	(64) 16GB DDR4 RDIMM
	NIC	(4) Intel® 82599 dual-port 10G mezz card
	SATADOM	(4) 32G SATADOM

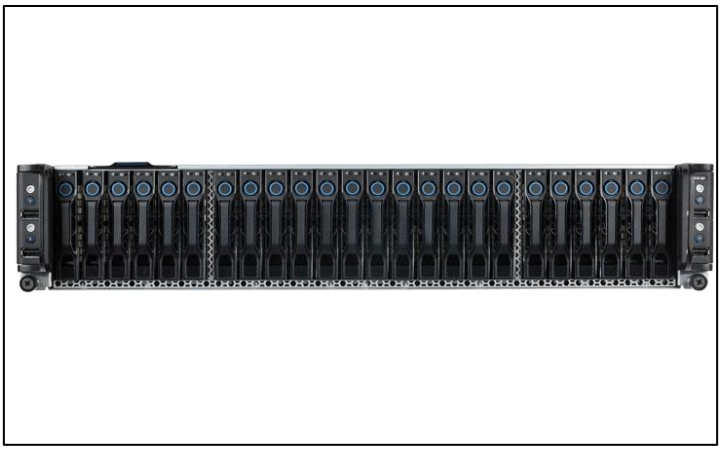

Figure 2. QxVDI -VMware Edition HC

3.3 Software Configurations

3.3.1 VMware Horizon®

The VMware Horizon® is the virtual desktop platform in QxVDI VMware Edition-HC solution with NSX®. The Horizon® is a centralized and fast-deploy virtual desktop, and an app platform. It delivers highly-personalized configurations for terminal users across sessions and devices, enables high availability of overall desktop services, and reduces the total cost of desktop ownership. With VMware Horizon®, traditional hardware requirement can be minimized. End users can increase productivity from more devices and locations. IT administrators can be more efficient in policy control.

VMware Horizon® version 7 enterprise edition is adopted in this QxVDI VMware Edition-HC solution with NSX®. VMware Horizon® consists of several major components, as shown in Table 2.

Table 2. Horizon Software Components.

Name	Description
Horizon® Composer™	This software service manages VMs. Horizon® Composer™ can create a pool of linked clones from a specified parent VM. This strategy reduces storage cost up to 90 percent. Each linked clone acts like an independent desktop with a unique host name and IP address, yet the linked clone requires significantly less storage because it shares a base image with the parent. ITs can quickly deploy, updates, and patches VM pools by updating only the parent virtual machine since the linked-clone desktop pools share a base image. A Composer™ is activated in the solution to enable the linked-clone function.
Horizon® Connection	The Connection server acts as a bridge for client connections. View Connection Server authenticates users through Microsoft Active Directory and directs the request to the appropriate VM, physical or blade PC, or Windows Terminal Services server. View Connection server provides management capabilities such as enabling SSO, authenticating client users, entitling client users to specific desktops or pools, and creating links between users and desktops, etc. A connection server is activated in the solution as well.
Horizon® Client	This client software which accesses remote desktops and applications can run on a tablet, a phone, a Windows, Linux, notebook, etc. After logging in, users select a list of remote desktops and apps that they are authorized to use. Permission may require Active Directory credentials, a UPN, a smart card PIN, an RSA SecureID, or an authentication token. In the solution, the View Clients are installed and used to log in to the virtual desktop services.
Active Directory	The Active Directory is developed from Microsoft for the Windows system domain networks. The Horizon® needs Active Directory infrastructure to perform the user validation and management. One Active Directory server is used in the solution to manage the VDI topology.
Horizon Agent	Acting as a bridge between Horizon and VMs' guest OS, the Agent installed on the source parent VMs is used for the communication between client and virtual machines.

3.3.2 VMware NSX®

VMware NSX® is a software-defined network that delivers scalable and flexible network architecture. The NSX® virtual network components reproduce Layer2 to Layer7 network model in the software, allowing complex multi-tier network topologies to be programmatically created and simplified within a short period. NSX® consists of several main components, as shown in Table 3. VMware NSX® version 6.3 enterprise edition is adopted in this QxVDI VMware Edition-HC with NSX® solution.

Table 3. NSX® Software Components.

Name	Description
NSX® Manager™	NSX® Manager™ is the management plane and centralized network management component of NSX®, installed as a virtual appliance in the vCenter Server®. It determines the core configuration of the whole system. A Manager™ is activated in the validation of solution.
NSX® Controller™	NSX® Controller™ is the control plane that controls virtual networks and overlay tunnels' information such as logical switches and logical routers. NSX® Controller™ is a central control point for all logical switches. It processes the information of all virtual machines, hosts, and logical switches (VXLANs). The Controller™ supports two control plane modes, namely, Unicast and Hybrid. These modes make NSX® decouple from the physical network. The Controller™ exists in virtual appliance format and the three Controllers™ are activated for solution validation.
NSX® Distributed Logical Router	NSX® logical router enables east-west distributed routing with tenant IP address space and data path isolation between switches. The router can also be deployed as Edge™ Service Gateway (ESG). The ESG provides north-south traffic for the data center. VMs or workloads that reside on the same host with different subnets can communicate with each other without having to traverse a traditional routing interface; thus, the traffic is optimized. There is an ESG router deployed in the test environment.
NSX® Distributed Logical Router	NSX® logical router enables east-west distributed routing with tenant IP address space and data path isolation between switches. The router can also be deployed as Edge™ Service Gateway (ESG). The ESG provides north-south traffic for the data center. VMs or workloads that reside on the same host with different subnets can communicate with each other without having to traverse a traditional routing interface; thus, the traffic is optimized. There is an ESG router deployed in the test environment.
NSX® L2 Bridge	The L2 bridge function can be used to connect logical switches and physical switch VLANs, allowing the extension of virtual logical network to access physical networks by bridging the logical VXLAN with the physical VLAN. This function is only available on the distributed logical router and is enabled in the validation of solution.
NSX® Distributed Firewall	NSX® Distributed Firewall (DFW) is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. L2 to L4 access control policies can be created based on VMware vCenter® objects such as data centers, clusters, virtual machine names and tags, and network construction such as IP/VLAN/VXLAN addresses as well as user group identity

	from the Microsoft Active Directory. The nature of this firewall can automatically extend firewall capacity when additional hosts are added to the data center. DFW is enabled to secure VMs and isolate different groups and services.
Logical Switch	The logical switches use VXLAN as the kernel service which can solve traditional VLAN challenges such as sprawl. This kernel-based VXLAN also leverages IT automation within the data center.

3.4 QxVDI VMware Edition-auto deployment tool

QCT designed a powerful automatic tool to deploy VMware vSphere® and Horizon® platform. The auto-deployment tool is a block system, mainly used to centrally deploy VMware infrastructure. The block system is pre-loaded in the HDD of the QxVDI VMware Edition-HC solution. Once the block system is installed, the IPs can be automatically allocated via web browser for vSphere infrastructure server pool (i.e., VMs, vCenter®, AD server, and DHCP server).

Administrators should firstly design the LAN and the topology of the target servers, and install ESXi™ hypervisor on each node. The tool OVA and VMware studio OVA are deployed to one of the target nodes. Subsequently, administrators need to provide the information including network domain, VMs, vCenter server®, DHCP, and IPs for each server node, Connection server, and Composter server in the portal, as shown in Fig. 3. The auto-deployment process can be completed within one hour.

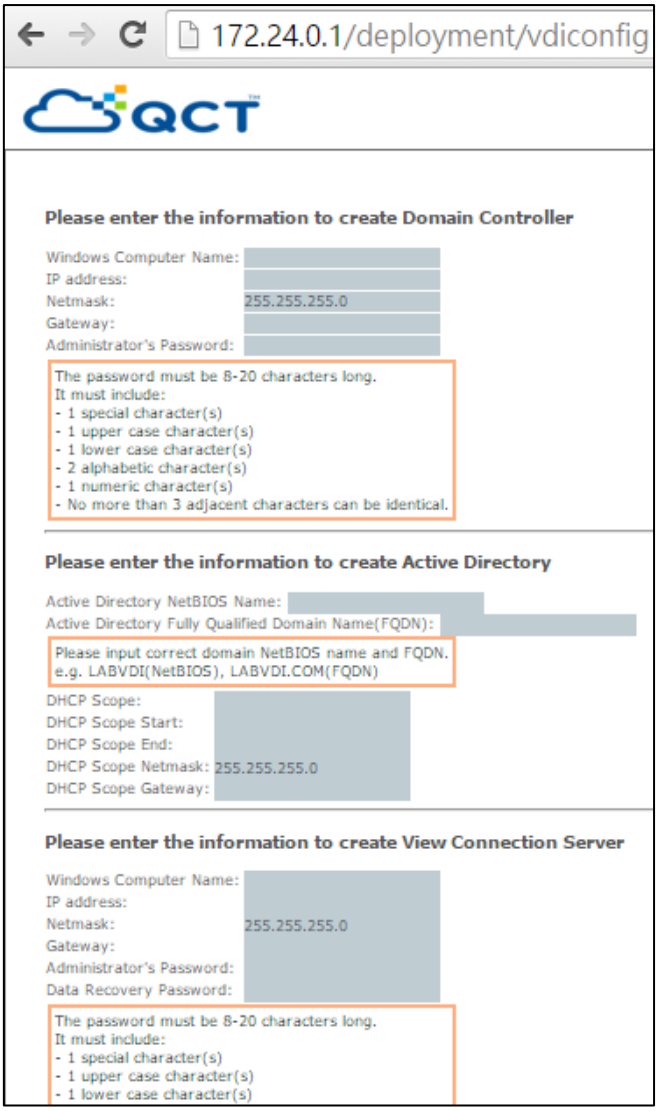

Figure 3. Auto-Deployment Console.

With the simplified infrastructure design and user-friendly web interface, QCT auto-deployment tool can highly simplify the operations of building vSphere® and Horizon® infrastructure, increase work efficiency, and eliminate human intervention errors.

4. Solution Scenario

4.1 Use Case 1: Layer 2 bridging with existing physical services

While using the QxVDI VMware Edition-HC with NSX®, enterprises might have difficulty in integrating existing physical services with NSX® VXLAN environment. Traditionally, in the QxVDI VMware Edition-HC environment, the VLAN tag has to be set the same as the external services' VLAN tag; if multiple VLAN subnets are needed, the multiple VLAN tags also need to be set. After the VLAN tag is configured, the VM workloads in data center can seamlessly communicate with the external VLAN subnet, as shown in Fig. 4.

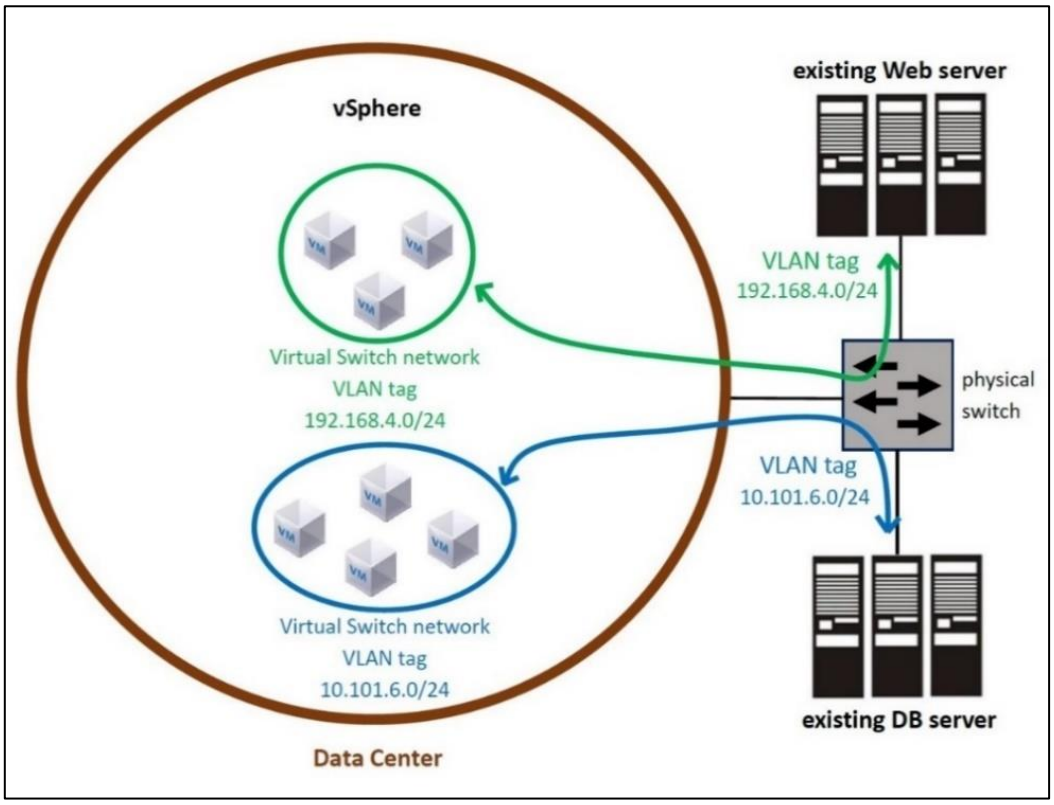

Figure 4. Typical Network Topology of QxVDI VMware Edition-HC.

After adopting the QxVDI VMware Edition-HC solution with NSX®, the data center environment will turn into a world filled with VXLAN logical switches. The distributed logical router provides a Lyer2 bridging function to seamlessly bridge the physical workloads (VLAN) and the internal VM workloads (VXLAN) by encapsulating and decapsulating the network packet. The VXLAN workloads can be connected to the external existing physical services even the IP subnet is not changed, as shown in Fig. 5.

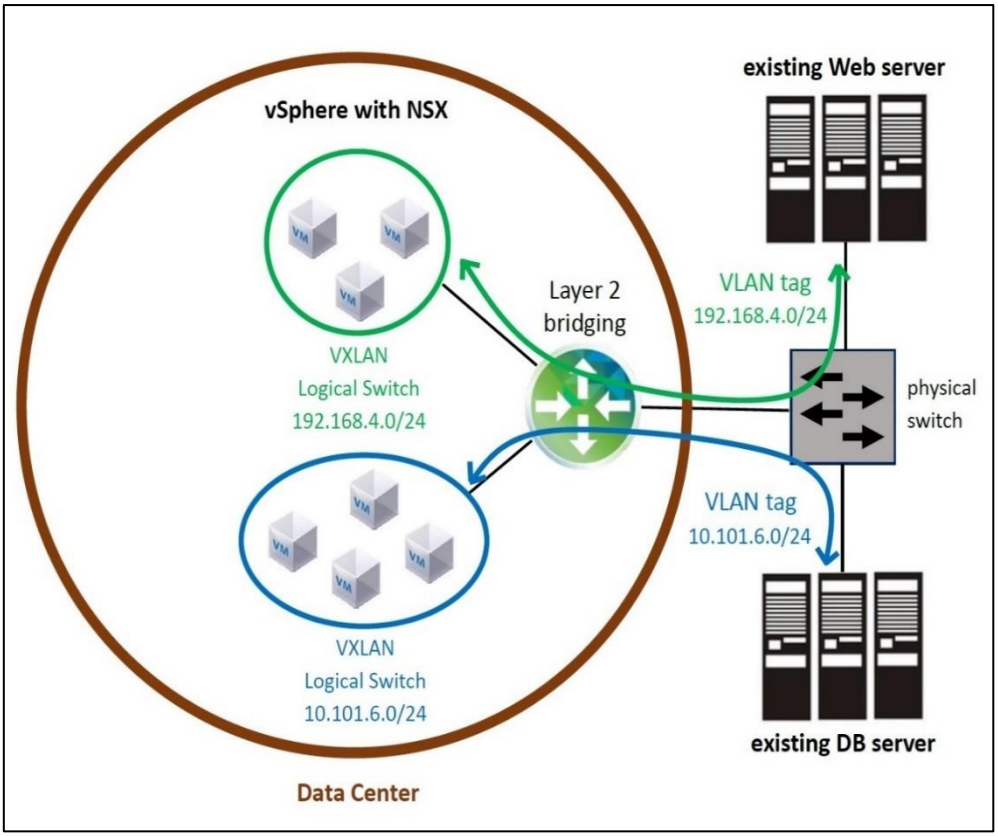

Figure 5. QxVDI VMware Edition-HC with NSX® with Integration of Physical Workloads.

To summarize, this use case brings the following benefits to enterprises:

- Integrating the software-defined network environment with existing physical workloads without any risky IP subnet changes.
- Providing enterprises a stable way to migrate workloads from physical environment to virtual environment during the transition.

4.2 Use Case 2: Micro-segmentation on VDI

Typical VDI without NSX® functions could be attacked by malicious behaviors from the data center inside. Even the physical perimeter firewall is powerful for the infrastructure, it posts no help of controlling the abnormal traffics inside the VDI. There is no network segment separation for the desktop groups and no security management for the virtual desktops. If one of the VMs compromises a virus, all the other VMs will be in great danger, as shown in Fig. 6. Hence, many third-party security solutions are designed to make up the insufficient security. Several security issues can be improved in typical VDI environment:

- To separate and optimize networks for groups and departments.
- To simplify the complexity of security controls for the groups and departments.
- To prevent malicious behavior such as worms and hackers from the compromised VMs.
- To integrate VDI with third-party security solutions efficiently.

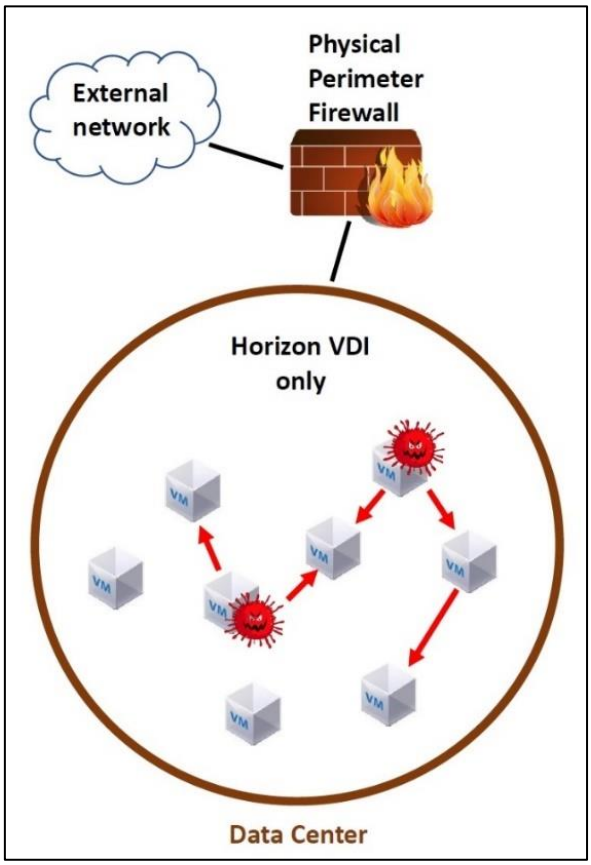

Figure 6. Typical VDI without Security.

4.2.1 Enablement of distributed logical firewall

After adopting the QxVDI VMware Edition-HC with NSX®, the kernel-based distributed logical firewall can be configured on the objects such as a VM, OS, IP sets, VM name or even large groups such as logical switches, hosts, resource pools, clusters, etc, as shown in Figure 7. Thus, the dependency is highly reduced on the physical firewall.

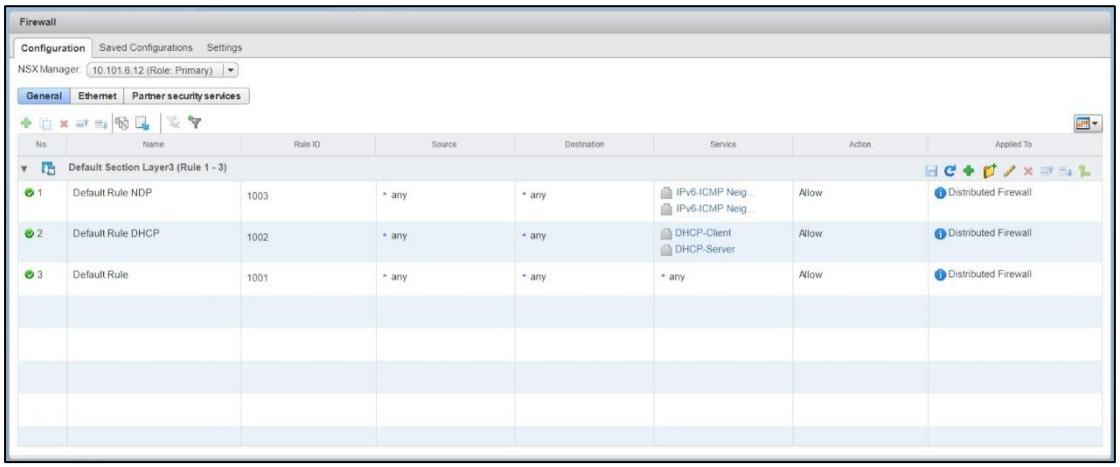

Figure 7. Management Interface of Distributed Logical Firewall.

4.2.2 Enablement of VXLAN logical switch

The VXLAN logical switches can easily separate networks for each group. According to IETF organization RFC 7348 record, VXLAN extends over 16 million IDs which can solve the space limit of traditional VLAN with only 4096 usable IDs. Moreover, the administrators can programmatically create the VXLAN logical switches, execute network automation in data center, and reduce the need of manual configurations. The manual platform of VXLAN is as shown in Fig. 8.

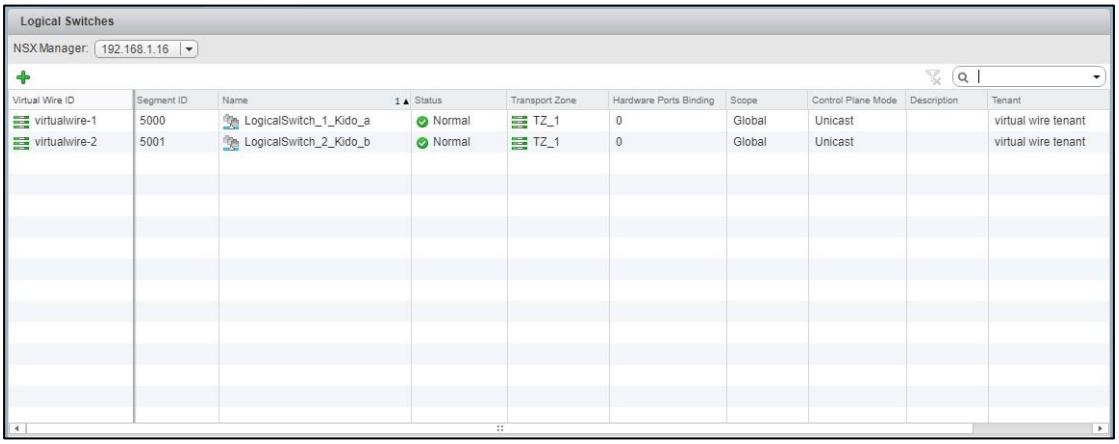

Figure 8. Management Interface of VXLAN Logical Switches.

The purpose of using VXLAN and distributed firewall is to accomplish the security control of the VDI in data center. The security management spans from a single VM to the large objects such as hosts and clusters, reaching the zero-trust model to defense malicious traffic from anywhere, as shown in Figure 9.

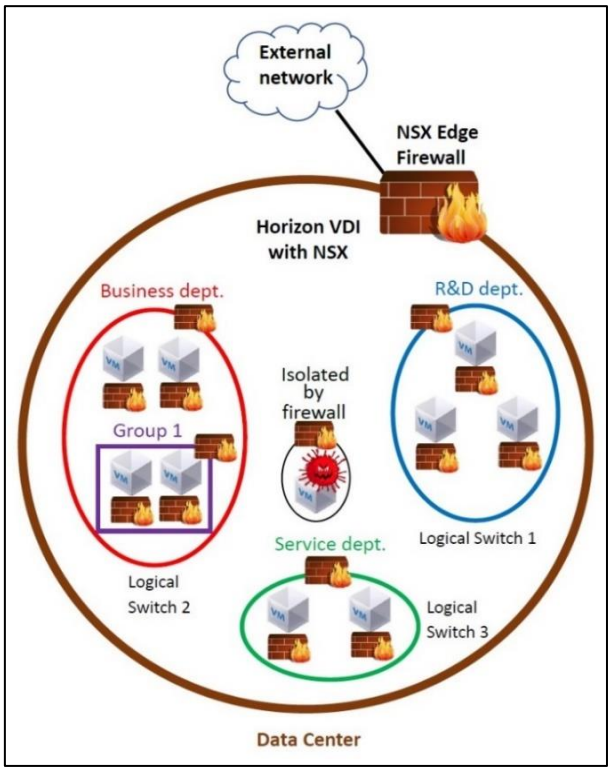

Figure 9. A Network Virtualized and Secured VDI.

To summarize, this use case brings the following benefits to enterprises:

- A network-secured VDI with isolated groups and depts.
- Simplified network topology by software controls.
- Centralized security controls such as distributed firewall in data center.
- Infrastructure independency from the underlying IP network.

4.3 Use Case 3: Optimized network traffic and simplified network hardware requirement

Without NSX® in the data center, the typical QxVDI VMware Edition-HC needs to be configured settings on network devices such as physical firewall, load balance, and switch. The settings include the design of network topology and the configuration of VLAN tags to make logical groups for the data center. The network traffic has to pass through several physical devices. As shown in Fig. 10, the red line refers to the north-south traffic between data center and external network while the green line refers to the east-west traffic in the data center.

The traffic from VM to external environment have to pass the load balancer and firewall. In this example, the traffic between different VLANs' VMs in the data center have to pass the firewall before reaching the target. This typical topology needs additional network devices to establish the security and balance the workloads. These requirements indicate the cost of network devices and a complicated network topology.

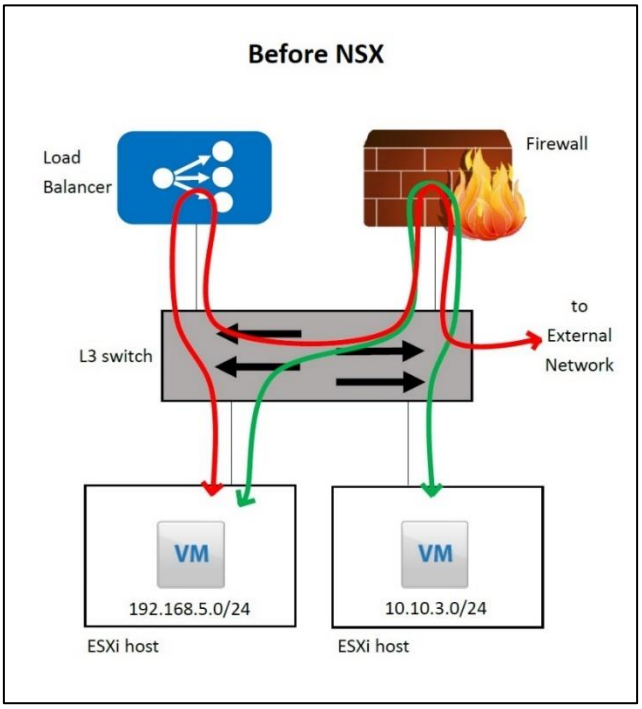

Figure 10. East-West and North-South Traffics Before Using NSX®.

After adopting the QxVDI VMware Edition-HC with NSX®, the built-in VXLAN logical switch, the distributed router, and the distributed firewall can be created in the data center on demand. The distributed firewalls can be applied to any workload or VMs to establish the built-in network security. The VXLAN logical switches can isolate

workloads into different networks. The distributed routers can execute the routing between different VXLAN networks in the kernel while the NSX® Edge appliance can provide perimeter firewall and load balancer.

The physical network devices such as physical load balancer and firewall can be eliminated because the traffic doesn't need to pass through. As shown in Figure 11, the red line and the green line respectively represent the north-south and the east-west traffics. The red line is only processed by NSX® Edge and the physical switch while the green line is processed by the physical switch, and the kernel-based distributed router, firewall, and VXLAN. The traffic paths are reduced compared to the typical QxVDI without NSX®.

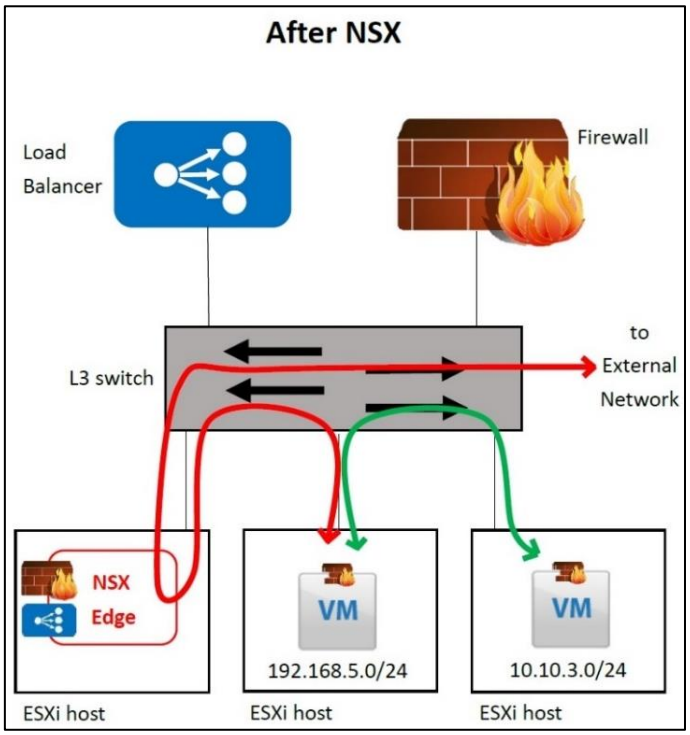

Figure 11. East-West and North-South Traffics after Using NSX®.

In this use case, the QxVDI VMware Edition-HC with NSX® brings the following benefits to enterprises:

- Simplified network management.
- Eliminated underlying physical hardware.
- Abstracted configuration from the underlying physical hardware.
- Enabled logical networks in hypervisor level.

5. Solution Validation

5.1 Login VSI test

5.1.1 Testing Purpose

The goal of this test is to showcase the performance of QuantaPlex T41S-2U running on VMware NSX® and Horizon® platform, and also shows the use of NSX® function – Layer 2 bridging. The theoretical maximum virtual desktops can be launched in specific configurations. Power Worker VDI VM workload is tested to simulate the real-world customer environment using Login VSI as a performance benchmark tool.

5.1.2 Benchmark Tool & Measured Value

Login VSI is an industry-standard load testing solution for centralizing virtualized desktop environment. Login VSI is designed to perform benchmarks for SBC or VDI workloads through system saturation. Login VSI loads the system with simulated user workloads using well-known desktop applications like Microsoft Office, Internet Explorer, and Adobe PDF reader. By gradually increasing the number of simulated users, the system will eventually be saturated. Once the system is saturated, the response time of the applications will increase significantly. This latency in application response time clearly indicates whether the system is close to be overloaded. As a result, by overloading a system, it is possible to find out what its true maximum user capacity is. Used for benchmarking, the software measures total response time of several specific user operations within a desktop workload in a scripted loop. Several Login VSI values and terms are noted below:

- **VSImax v4.1** shows that the number of sessions can be activated on a system before the system is saturated. This number indicates the scalability of the environment. It is noted that the higher the VSImax v4 is, the more the sessions can be launched on a system.
- **VSImax v4.1 base** refers to the best performance of a system during a test within the shortest response time. This number is used to determine what the performance threshold will be. VSImax v4.1 base indicates the base performance of the environment. It is noted that the lower the VSImax v4.1base is, the better the performance of a system is.
- **VSImax v4.1 threshold** is VSImax v4.1 base plus 1000ms. It is used to mark saturation point for a tested system. When the VSImax v4.1 curve reaches to VSImax v4.1 threshold, the system reaches the saturation point.
- **VSImax v4.1 average** represents the average response time found in the

environment after completing the test. This value should normally fit the criterion VSImax v4.1 base < VSImax v4.1 average < VSImax v4.1 threshold.

- **VSI Index Average** indicates the average value calculated by VSI. The VSI Index Average differs from Average Response since Average Response is a pure average. VSI Index Average applies certain statistical rules to avoid spikes from highly influencing the average.

Other values measured to correlate the system state during the test are:

- **CPU utilization rate**: Cluster CPU utilization rate is obtained from VMware vCenter® when Login VSI test starts.
- **Memory utilization rate**: Cluster memory utilization rate is obtained from VMware vCenter® when Login VSI test starts.

5.1.3 Workload Resource Usage

The Login VSI provides four primary workloads, namely, “Task Worker”, “Office Worker”, “Knowledge Worker” and “Power Worker.” The differences between the workloads are the amount of applications and media launched in VMs including MS office, Internet Explorer, etc. The workloads are graded from “Task Worker” to “Power Worker” to simulate different user environments, as shown in Table 4. The Power worker workload is mainly used as the baseline in this test to simulate the realistic environment since the heaviest workload covers all workload types and is suitable to scale the VDI’s maximum capability.

Table 4. Workload Resource Usage.

Type	VSI Version	Apps Launch	CPU Usage	Disk Reads /Writes	IOPS	vCPU	vRAM
Light	4.0	2	66%	52%/ 65%	5,2	1	1 GB
Medium	4.0	5 - 7	99%	93%/ 97%	7,4	2	1 GB
Heavy	4.0	8 - 10	124%	89%/ 94%	7	2	1 GB
Task Worker	4.1	2 - 7	70%	79%/ 77%	6	1	1 GB
Office Worker	4.1	5 - 8	82%	90%/ 101%	8,1	1	1.5GB
Knowledge Worker	4.1	5 - 9	100%	100%/100%	8,5	2	1.5GB
Power Worker	4.1	8 - 12	133%	133%/123%	10,8	2+	2 GB

Fig. 12 below shows the VM profiles suggested by Login VSI according to different workloads. It is noted that the Power Worker workload vRAM is increased to 4GB in our test case to simulate the realistic user environment.

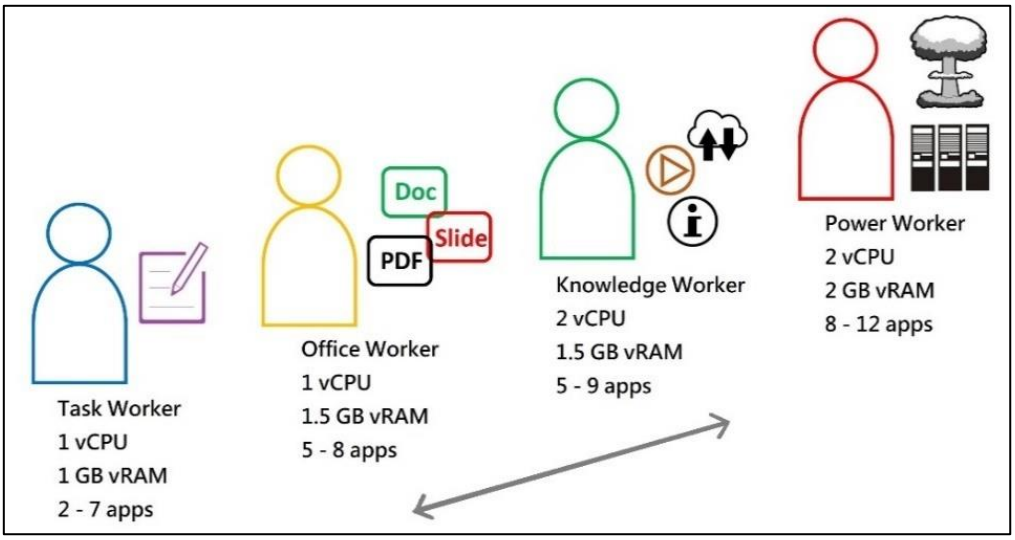

Figure 12. Workload Profile of Login VSI.

5.1.4 Hardware Configuration

QuantaPlex T41S-2U is the hardware platform of the solution. The specification configured for the test is listed in Table 5.

Table 5. Specification of the Test Platform.

Server Model Name		QuantaPlex T41S-2U
Server Nodes		4 Nodes
Per Node Configuration	CPU	(2) Intel® Xeon® processor E5-2620 v4
	SSD	(1) Intel S3710 SATA 400GB 2.5”
	HDD	(5) HGST SAS 1.2TB 2.5”
	RAM	(16) 16GB DDR4 RDIMM
	NIC	(1) Intel® 82599 dual-port 10G mezz card
	SATADOM	(1) 32G SATADOM

The overall test environment is separated into two parts: the test platform with VDI and the Login VSI server platform with the Login VSI services. The Login VSI server platform specification is listed in Table 6. The Login VSI server platform does not affect test environment’s resource consumption due to the separation of the two environments.

Table 6. Hardware Specification of Login VSI Platform.

Server Model Name		QuantaMicro X10E-9N
Server Nodes		9 Nodes
Per Node Configuration	CPU	(1) Intel® Xeon® processor E3-1270 v5
	SSD	(1) Intel S3710 SATA 200GB 2.5”
	HDD	(3) HGST SATA 1TB 2.5”
	RAM	(4) 16GB DDR4 RDIMM
	NIC	(1) QCT Intel® i350 mezz card
	SATADOM	(1) 32G SATADOM

5.1.5 Software Configurations

The software configurations include the vCenter®, Horizon® and NSX® appliances, as shown in Table 7. The vSphere® functions vSAN™ and high availability are respectively activated to create a storage pool and provide host failure redundancy. The resource consumption of the virtual machines including vSphere®, Horizon®, and NSX® in the test environment is referenced from VMware official data.

Table 7. Software Configuration in Test Environment.

Software Item	Software Version
VMware vSphere® Enterprise Plus Edition™	VMware ESXi™ 6.5 build 4887370
	vCenter Server® Appliance 6.5.0.5200 * 1 (vCenter Server® Standard™)
	vSAN™ 6.5 enabled
	High Availability enabled
VMware Horizon®7 related VMs	AD & DHCP Server (Windows Server 2008) * 1
	Composer™ Server (Windows Server 2008) * 1
	Connection Server (Windows Server 2008) * 1
VMware NSX® Appliances	Manager™ * 1
	Controller™ * 3
	Edge™ Service Gateway * 1

The total resources consumed by these services in the test environment are 26 vCPU, 62.5 GB vRAM and 373 GB disk space, as shown in Table 8. In the Login VSI server platform, the total resource consumption of the VMs are 18 vCPU, 36 vRAM and 120GB disk space, as shown in Table 9.

Table 8. Profile of Each VM Server in Test Environment.

Virtual Appliances	vCPU	vRAM	Disk Space
vCenter Server®	4	16GB	12GB
AD & DHCP Server	1	2GB	40GB
Connection Server	2	8GB	100GB
Composer™ Server	2	8GB	100GB
Manager™	4	16 GB	60 GB
Controller™ Nodes * 3	4 * 3	4 GB * 3	20 GB * 3
Edge™ Service Gateway	1	512 MB	1 GB
Total	**26**	**62.5 GB**	**373 GB**

Table 9. Profile of Each VM Server in QuantaMicro X10E-9N.

Virtual Appliances	vCPU	vRAM	Disk Space
Login VSI Share Server *1	2	4	60 GB
Login VSI Launcher Server * 8	2 * 8	4 * 8	60 GB
Total	**18**	**36**	**120 GB**

5.1.6 Test Methodology

Login VSI is used to simulate application workloads and the response time is measured to validate utilization and user experience. Cluster and host resource utilization rates can also be recorded for analysis. Power Worker workload with 180 users is the target in this test. The vRAM is increased to 4GB, which is different from the default Power worker workload in Login VSI (2GB vRAM). The specification of the Power Worker workload is shown in Table 10.

Table 10. VM Profile of Target User.

VM Profile	180 Power Worker
vCPU	2
Memory	4GB
VMDK	24GB thin provision
OS	Windows 7 SP1 64bit
MS Office version	2007
Login VSI workload	Power Worker

5.1.7 Test Topology & Success Criteria

The environment is separated into two parts, test platform target environment and Login VSI launcher environment, to avoid the resource effects from the login VSI tool itself and also to validate the availability of Layer 2 bridging function, as shown in Fig. 13. The communication between the target and launcher environments are all through the red line, the Layer 2 bridging. In order to simulate the integration of existing IP subnet with new VDI, the target environment is configured with the same IP subnet in the launcher environment.

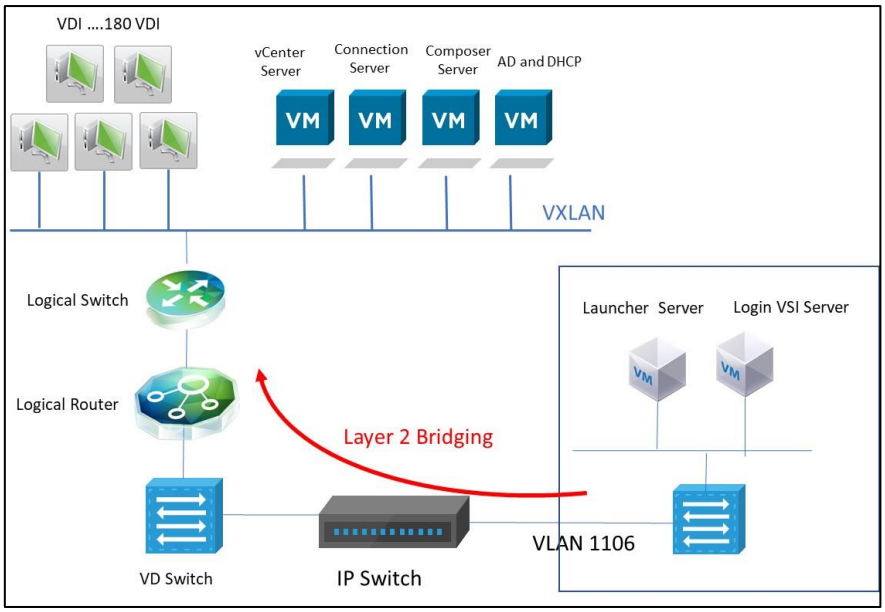

Figure 13. Network Topology of Testing Environment.

The success criteria of this test are listed below:

1. Cluster CPU and memory utilization in the cluster must remain 20% to deal with potential hardware failures for HA function. Memory consumption of ESXi™ host must show no memory ballooning or swapping for our target VDI user.
2. The test with minimal variability must be consecutively executed until the consistent performance appears under the scenario of the specified VDI deployment size.
3. Login VSI provides score value of baseline performance, as shown in Table 11. The testing results of VSI Baseline and Average score must fall within the "Good Performance" category in order to confirm both good end-user experience and adequate environment performance throughout the entire simulation. Moreover, the Average Index score must be lower than the VSImax threshold during the entire simulation.
4. The vSAN™ backend should be capable of satisfying I/O needs of target VDI users and the latency should be under 2 milliseconds throughout the simulation test.

Table 11. Login VSI Rating of Test Results.

VSIbase (ms)	Performance
0 – 1500	Good
1501 - 3000	Average
3001 - 4500	Below Average
4501 - 9999	Poor

5.1.8 Test Results and Explanation

The test result shows the “Good” baseline performance with 180 sessions and index average score 920 lower than the threshold, as shown in Fig. 14.

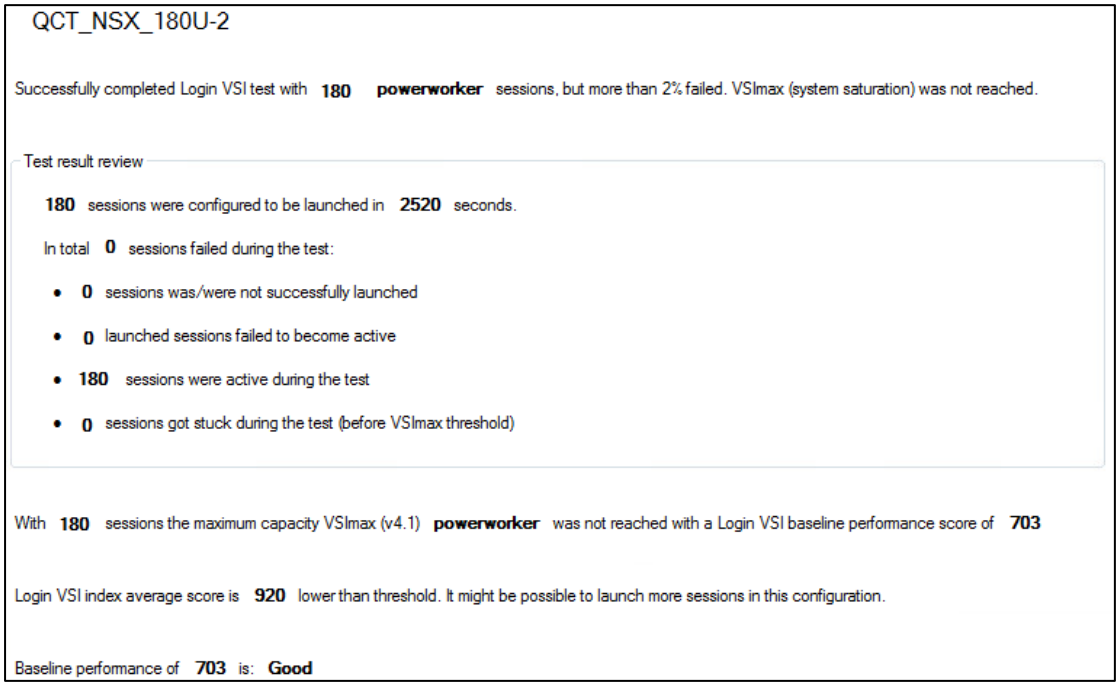

Figure 14. Summary of Login VSI Testing Report.

Login VSI test sessions with 180 Power workers (4GB RAM) is successfully completed, as shown in Table 12. According to the VSIbase rating (see Table 11), the baseline 703 ms is under the “Good” performance rating, indicating the baseline form a good user experience. It is possible to launch more sessions by adopting this configuration since VSI index average score is lower than the thresholds. However, to deal with potential hardware failures for HA function, Cluster CPU and memory utilization should be kept down below 80%. The value marked in red indicates that the cluster memory usage over 80% is not suggested. QuantaPlex T41S-2U has four nodes in one chassis. If one node fails, the other three nodes can still sustain the failed node so as to minimize the impact and fulfill the HA.

Table 12. Server Utilization and Login VSI Test Results.

Test Case	Target User	VM Profile	Login VSI Workload	Max CPU Usage	Max Memory Usage	VSIbase	Login VSI Index Average Score	VSImax v4.1 Average
TC1	180	2vCPU /4GB RAM	Power Worker	44.89%	82.63%	703	1703	920

By taking the average of the 13 lowest indexes in the overall test, the result of VSIbase score 703 shows “Good” performance (see Fig. 11). By adding 1000ms to the VSIbase, the threshold is 1703. The average response time of VSImax v4.1 average is 793 ms, which is under the threshold. The response time does not exceed the threshold which indicates that the system saturation is not reached and the server can sufficiently sustain the 180 Power workers, as shown in Fig. 15.

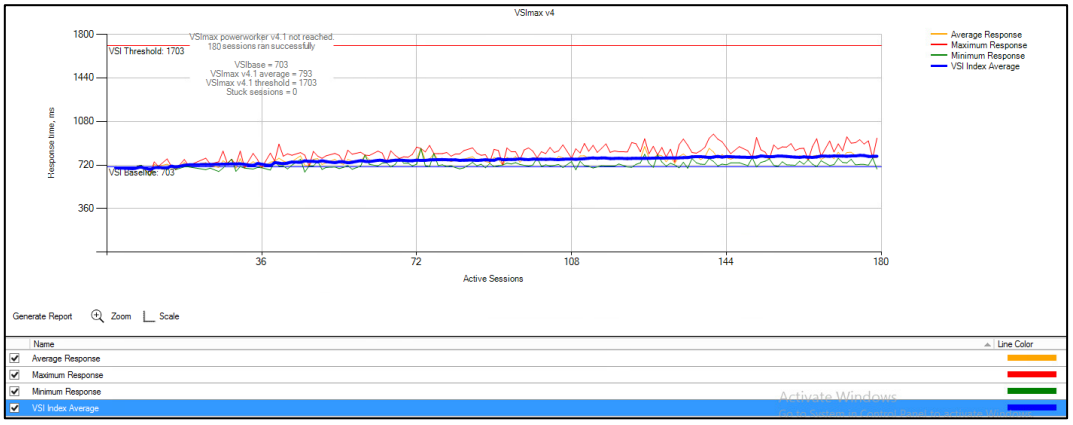

Figure 15. Test Result of VSImax v4.1.

The CPU maximum utilization reaches to approximately 45% while the average is approximately 28%, as shown in Fig. 16. This indicates that CPU resource is still sufficient to execute more tasks.

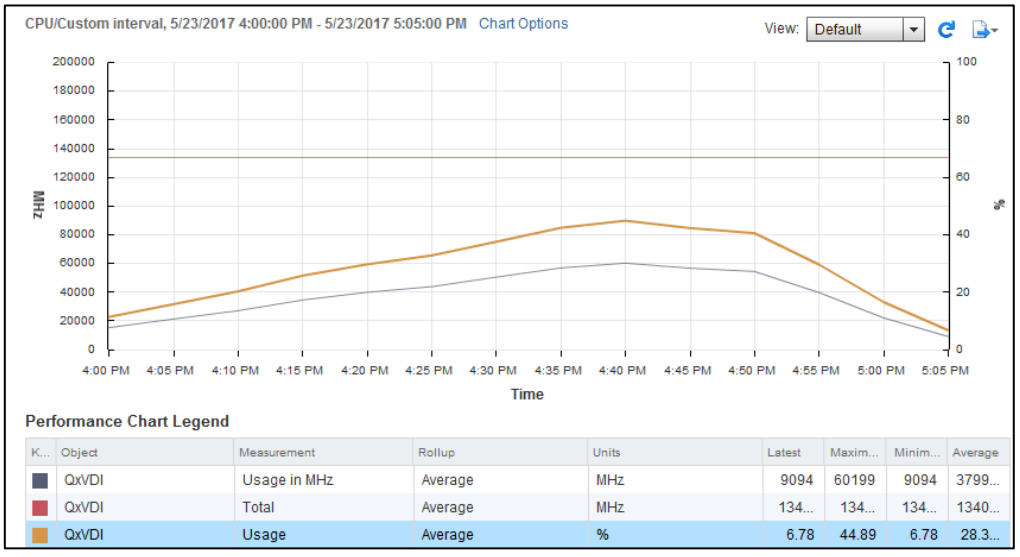

Figure 16. Cluster CPU Utilization.

The memory preservation around 20% is recommended to prevent possible host failure. The theoretical memory limit is thus set to 80%. In Fig. 17, although the average

memory consumption is close to 83%, the memory ballooning does not appear in the test; hence, the memory resource is still sufficient to deal with the workloads.

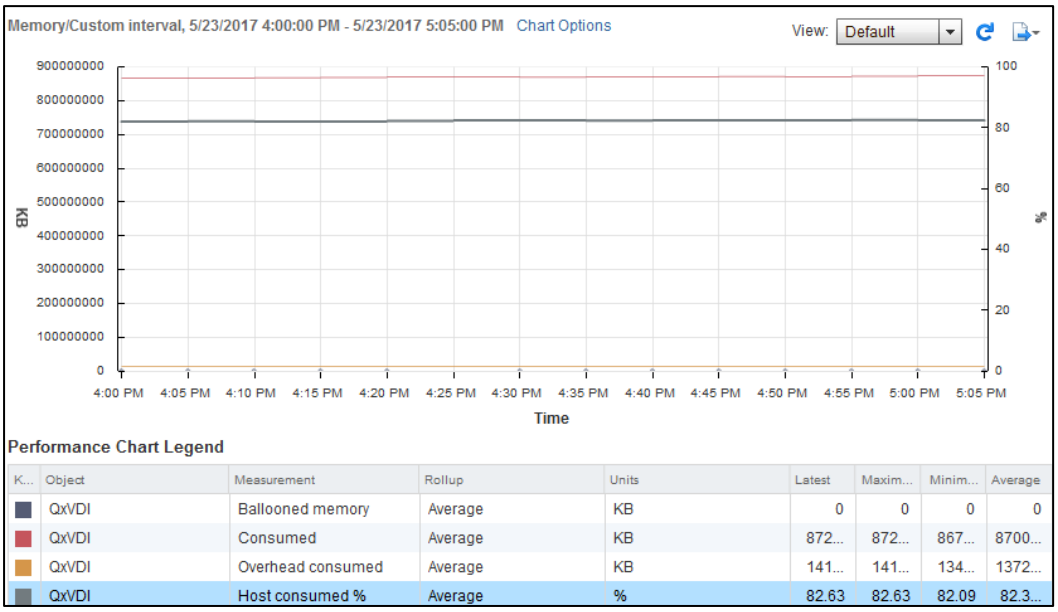

Figure 17. Cluster Memory Utilization without Memory Ballooning.

6. Conclusion

The test result of Login VSI reveals that QxVDI VMware Edition-HC with NSX® is capable of supporting up to 180 virtual desktop users when the NSX® virtual appliances are enabled and some resources are consumed. The test results of Login VSI also show good and acceptable response time even when all virtual desktop users log in. With straight and predictable end user performance, QxVDI VMware Edition-HC with NSX® solution is a considerably stable and trust-worthy model. Some strong benefits in terms of QxVDI VMware Edition-HC with NSX® are summarized below:

- Eliminating the deployment time of the VDI.
- Reducing human intervention errors and increasing administrators' work efficiency.
- Simplifying the infrastructure design by automating tool.
- Securing all the services through the distributed firewall and extendable networks.
- Centralizing and simplifying network management.
- Eliminating the requirement of networking hardware such as firewall.
- Seamlessly integrating existing services with network secured new VDI.

7. Reference

【1】 QxVDI VMware Edition-HC
http://qct.io/solution/index/Desktop-Virtualization/QxVDI-VMware-Edition-HC

【2】 VMware Horizon® 7
https://www.vmware.com/products/horizon.html

【3】 VMware NSX®
https://www.vmware.com/products/nsx.html

【4】 VMware Horizon® 7 Documentation
https://docs.vmware.com/en/VMware--7/index.html

【5】 VMware NSX® Documentation
https://docs.vmware.com/en/VMware-NSX-for-vSphHorizonere/index.html

【6】 Login VSI
https://www.loginvsi.com/products/login-vsi

8. Document history

Version 1.0	1. September 2017	First version
Version 1.1	1. December 2017	Second version

About QCT

QCT (Quanta Cloud Technology) is a global datacenter solution provider extending the power of hyperscale datacenter design in standard and open SKUs to all datacenter customers.

Product lines include servers, storage, network switches, integrated rack systems and cloud solutions, all delivering hyperscale efficiency, scalability, reliability, manageability, serviceability and optimized performance for each workload.

QCT offers a full spectrum of datacenter products and services from engineering, integration and optimization to global supply chain support, all under one roof.

The parent of QCT is Quanta Computer Inc., a Fortune Global 500 technology engineering and manufacturing company.

http://www.QCT.io

United States

QCT LLC., Silicon Valley office
1010 Rincon Circle, San Jose, CA 95131
TOLL-FREE: 1-855-QCT-MUST
TEL: +1-510-270-6111
FAX: +1-510-270-6161
Support: +1-510-270-6216

QCT LLC., Seattle office
13810 SE Eastgate Way, Suite 190, Building 1,
Bellevue, WA 98005
TEL: +1-425-633-1620
FAX: +1-425-633-1621

China

云达科技，北京办公室（Quanta Cloud Technology）
北京市朝阳区东三环中路 1 号，环球金融中心东楼 1508 室
Room 1508, East Tower 15F, World Financial Center
No.1, East 3rd Ring Zhong Rd., Chaoyang District, Beijing, China
TEL: +86-10-5920-7600
FAX: +86-10-5981-7958

云达科技，杭州办公室（Quanta Cloud Technology）
浙江省杭州市西湖区古墩路浙商财富中心 4 号楼 303 室
Room 303，Building No.4，ZheShang Wealth Center
No. 83 GuDun Road, Xihu District, Hangzhou, Zhejiang , China
TEL: +86-571-2819-8660

Japan

Quanta Cloud Technology Japan 株式会社
日本国東京都港区芝大門二丁目五番八号
牧田ビル３階
Makita Building 3F, 2-5-8, Shibadaimon ,
Minato-ku, Tokyo 105-0012, Japan
TEL: +81-3-5777-0818
FAX: +81-3-5777-0819

Taiwan

雲達科技（Quanta Cloud Technology）
桃園市龜山區文化二路 211 號 1 樓
1F, No. 211 Wenhua 2nd Rd., Guishan Dist.,
Taoyuan City 33377, Taiwan
TEL: +886-3-286-0707
FAX: +886-3-327-0001

Germany

Quanta Cloud Technology Germany GmbH
Hamborner Str. 55, 40472 Düsseldorf ,
Germany
TEL: + 492405-4083-1300

Other regions

Quanta Cloud Technology
No. 211 Wenhua 2nd Rd., Guishan Dist.,
Taoyuan City 33377, Taiwan
TEL: +886-3-327-2345
FAX: +886-3-397-4770