XenDesktop Planning Guide

Integration with VMware vSphere
Contents

Introduction ........................................................................................................................................... 3
Guidelines ............................................................................................................................................ 3
  VMware vCenter Server .................................................................................................................... 5
  Hardware Specification ...................................................................................................................... 7
  Networking ....................................................................................................................................... 11
  Storage ........................................................................................................................................... 13
  Implementation Considerations for XenDesktop on vSphere ......................................................... 19
Appendix ............................................................................................................................................... 20
  vSphere Product Features .................................................................................................................. 20
  VMware vSphere Document Reference .......................................................................................... 20
Introduction

This document provides design guidance for Citrix XenDesktop 5.5 deployments that leverage VMware vSphere versions 4 and 5. It should not be considered as a replacement for other XenDesktop design guidance, but rather an addendum that will assist in design decisions specifically related to using VMware vSphere as the hypervisor. For further planning guides, please refer to the XenDesktop Design Handbook.

Guidelines

Clusters and High Availability

In vSphere, a cluster is a construct that consists of multiple VMware ESXi hosts bound together to form a single entity for the purpose of management and high-availability. Hosts, within a cluster, usually share common resources so that virtual machines can be started on, or migrated between (vMotion) any host within the cluster where sufficient resources exist. Resource pools, which can be created within a cluster, allow administrators to subdivide a cluster configuration to create shared logical pools of CPU and memory resources and in some cases guarantee resource levels for certain groups. Based on the vSphere 5 Configuration Maximums, VMware supports up to 32 hosts and/or 3000 virtual machines in a single cluster and up to 1600 resource pools can be created per cluster.

The number of clusters required to support an implementation of XenDesktop depends on various factors, including:

- Number of Hosts and Virtual Desktops – Citrix Consulting has observed optimal virtual desktop density in vSphere 4 configurations with a maximum of 8 hosts per cluster or approximately 1000 virtual machines per cluster. Increased scalability in vSphere 5 allows for up to 10,000 running virtual machines per vCenter configuration, and a maximum cluster configuration of 32 ESXi hosts or 3000 virtual machines per cluster. Multiple cluster configurations are permitted per vCenter configuration, but VMware does not publish a maximum number. Although the maximum cluster configurations are higher for vSphere 5, there are still additional items that need to be considered when evaluating the different FlexCast models. For Machine Creation Services (MCS), it is recommended that cluster size should not exceed 8 hosts given that the MCS virtual desktops reference a master image and all the reads from that single image are processed by the hypervisor. For Provisioning Services (PVS), it may be possible to increase the number of virtual desktops per cluster as the master vDisk image is accessed for reads either from local cache or through network access. In general, Citrix Consulting recommends that customers perform scalability testing of individual configurations to validate performance, particularly beyond the best practices configuration of 8 hosts per cluster and/or 1000 virtual desktops per cluster configuration.
• Performance – Most businesses will have desktops groups that require guaranteed performance levels. To address this requirement in a small environment, consider the implementation of dedicated ESXi hosts within an existing cluster, and the use of vSphere resource pools to subdivide the cluster. For larger environments, it is sometimes necessary to create dedicated clusters to meet the service level agreements associated with these desktops.

• High Availability – There may be a requirement for desktop groups to offer varying levels of redundancy. For example, a desktop group used by financial traders could require N+100% redundancy while a desktop group accessed by human resources may only require N+10%. In order to accommodate increased levels of redundancy, sufficient capacity must exist within the cluster to handle the required number of host failures. In such situations, it may be pertinent to isolate desktop groups into their own clusters based on the level of redundancy required.

• Infrastructure Nodes – When designing a clustered solution, consider separating the XenDesktop infrastructure nodes (host server components such as AD, SQL and XenDesktop controllers) from the virtual desktop nodes by placing them on different vSphere clusters. This will allow vSphere features such as Distributed Resource Scheduler (DRS), Storage DRS and High Availability to be tailored for the specific requirements for either desktops or servers.

• Application Set – It may be beneficial to dedicate clusters for large desktop groups as they share a common, predictable resource footprint and application behavior. Alternatively, grouping desktop groups together based on differing resource footprints could help to improve desktop density per host. For example, splitting processor intensive desktops across several clusters will help to distribute the impact from processor saturation. If XenApp is used within the XenDesktop configuration to provide virtualized application access, it is advisable to separate the XenApp configuration into a separate cluster to balance resource utilization.

• Physical Network – Some environments may have complex network configurations which require multiple clusters to be deployed. For example, some desktop groups may need to be isolated onto specific subnets for reasons of security, whilst others may have requirements for network connectivity which can only be satisfied within specific data centers or network locations.

• Virtual Network – Depending on the environment, it may be overly complex to trunk every VLAN to every cluster. As such, it may be necessary to define clusters based on the VLANs to which they are connected.
Security Restrictions – Some vSphere clusters may provide a platform for desktops which are sensitive in nature or which must be isolated in order to meet regulatory compliance. A separate cluster may be mandatory under these circumstances to ensure the required segregation and administrative separation.

Dedicated Hardware – Certain desktop groups may require more expensive hardware than others, including faster network cards, Host Bus Adapters (HBAs), extra memory and additional redundant components. If so, consider separating out these hosts into separate clusters so that they can be dedicated to the relevant desktop groups.

In many cases, virtual workloads will fall into multiple categories, for example high priority users will require a high level of both performance and high availability. By capturing all of the requirements, it should be possible to understand the most appropriate cluster design for the environment and to allocate resources accordingly. In some situations, it may become necessary to configure multiple clusters within a single desktop group.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Options</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of clusters</td>
<td>1+</td>
<td>2-3+: one for server infrastructure, one or more for virtual desktops. If XenApp is used in the configuration, add another cluster for XenApp servers.</td>
</tr>
<tr>
<td>ESXi hosts per cluster</td>
<td>1-32</td>
<td>Citrix Consulting has observed optimal virtual desktop density at 8 hosts per cluster (with vSphere 4 and MCS on vSphere 5). Theoretically, it may be possible to increase the cluster size to 10 hosts for PVS with vSphere 5, but scalability for vSphere 5 has not been evaluated by Citrix Consulting, and should be thoroughly tested beyond the 8 hosts per cluster recommendation.</td>
</tr>
<tr>
<td>Clusters per Desktop Group</td>
<td>1+</td>
<td>For simplicity, try to maintain one cluster per desktop group.</td>
</tr>
<tr>
<td>High Availability in Clusters</td>
<td>N+</td>
<td>At least, N+1 so that the cluster can continue to operate in the event of a single host failure.</td>
</tr>
</tbody>
</table>

Table 1: Cluster Recommendations

VMware vCenter Server

VMware vCenter is a dedicated server used to manage VMware vSphere environments and is a critical component in a XenDesktop environment due to its central role of managing all communication between XenDesktop and vSphere. Since each VMware vSphere server cluster relies on vCenter to perform cluster management and other hosting infrastructure tasks, the delivery of desktops may be hindered should the vCenter Server encounter high stress conditions and become slow or unresponsive, such as in a large XenDesktop environment with many
morning logons or rapid shift changes. The following section provides vCenter Server best practices for a XenDesktop implementation.

VMware vCenter server 5.0 requires a 64 bit operating system and can be deployed on the 64 bit versions of Windows Server 2003, 2008 and 2008 R2. VMware best practices for installing Virtual Center 5.0 can be found in the Knowledge Base article 2003790.

VMware fully supports and recommends deploying the vCenter Server as a virtual machine which allows the vCenter Server to utilize benefits provided by virtualization such as high availability. Achieving high availability for the VMware vCenter Server is recommended for XenDesktop deployments and can be implemented using the following recommended practices:

- **VMware High Availability (HA):** Citrix Consulting recommends that the vCenter Server be highly available for all production XenDesktop and vSphere deployments. While the loss of a vCenter server will not affect current XenDesktop connections, administrators will lose the ability to make changes to and manage the vSphere cluster configurations. High availability for vCenter can be achieved by placing the vSphere host running the vCenter Server in a VMware HA cluster. If the host supporting the vCenter Server fails, the vCenter Server will be restarted on another host in the cluster. It is recommended that the startup priority for the vCenter Server is changed from a default value of ‘medium’ to ‘high’. Also ensure that other services that the vCenter Server depends on, such as Active Directory, DNS and the SQL hosting the vCenter data store, are also configured with a ‘high’ startup priority.

- **vCenter Server Heartbeat:** The vCenter Heartbeat offers a comprehensive level of protection which is highly recommended for physical instances of vCenter Server. It uses a primary and secondary vCenter Servers with identical names and IP addresses to provide continuous availability of the vCenter Server through a hardware failure scenario or operating system crash. As previously mentioned, VMware HA is the preferred choice for virtual vCenter instances; whereas, vCenter Heartbeat is preferred for physical instances. Please refer to the [VMware vCenter Server Heartbeat Reference Guide](#) for more information.

- **Distributed Resource Scheduling (DRS):** If VMware DRS is implemented on the service cluster that hosts vCenter Server (sometimes referenced as the ‘infrastructure cluster’), be aware that the host on which the vCenter virtual machine runs might change from time to time as the load is rebalanced. This might not be an issue for small size service clusters as a limited manual search will be required to locate the vCenter instance. Alternatively, DRS can be disabled on the vCenter virtual machine, by setting the Automation Level to “Disabled”. This will allow DRS to be implemented for other virtual machines on the service cluster and also allow the location of the vCenter Server to be explicitly known at all times. With DRS disabled for the vCenter Server, high availability will still be ensured by VMware HA services.
• vCenter Server and XenDesktop Desktop Delivery Controller (DDC) Communication: In order to facilitate setup and communication between the DDC and the vCenter server, a third party or self-signed certificate must be installed on the vCenter server and the DDCs in the environment. Although a self-signed certificate may be used in non-production environments, Citrix Consulting recommends the use of a certificate provided by a third-party certification authority or an internal enterprise CA for production use. The pool management service on the DDC communicates with the vCenter Server by sending virtual desktop power on/off commands. By default, these requests are throttled at 10% of the total cluster. For example, if there are 1,000 VMs in the desktop group, then 100 VM power operation requests will be sent at a time. As the number of desktops increase, it becomes important to change this default throttling value to avoid having the vCenter Server become overloaded. Citrix recommends that each organization properly test the configuration before determining the optimal balance between the number of concurrent commands that can be serviced and the performance/responsiveness of the hosting infrastructure when sending power commands from the DDC. This value should be lower if DRS is enabled for the ‘general cluster’ hosting virtual desktops, as DRS needs additional time to determine guest placement before powering it on. Citrix Consulting conducted testing using a value of 20 concurrent commands with DRS enabled and 40 without DRS which can be referenced as a baseline and then increased based on performance testing.

Hardware Specification

The hardware selected for the VMware ESXi hosts has a direct impact on the performance, scalability and resilience of the XenDesktop solution. As such, it is critical that the following key areas are considered during the hardware selection process:

• ESX vs. ESXi – With vSphere 4, there is support for both VMware ESX and ESXi hypervisor architectures. However with the release of vSphere 5, only the ESXi architecture is supported. To support future upgrades, it is recommended that vSphere 4 solutions be constructed on the ESXi architecture.

• Compatibility – All server hardware should be listed on the current vSphere Hardware Compatibility Guide. VMware ESXi 5.0 supports 160 logical processors, 2 TB of RAM and up to 32 NICs per ESXi host. Minimum system requirements for ESXi can be found in VMware Knowledge Base article 1003661.

• Scale Up/Out – The decision to scale up (add more resources to a single host) or scale out (add additional hosts) should be based on the amount of space available, cooling/power capacity and maintenance/hardware or hosting costs. Currently, smaller two-socket servers generally scale better than four-socket servers in terms of the aggregate of number of VM’s per socket/core. With due consideration for specific requirements, Citrix recommends to scale out rather than up in most situations.
• Processor – Intel VT or AMD-V is required for 64 bit virtual machines. All servers in a cluster must be configured with processors capable of executing a common instruction set. If an environment consists of Intel and AMD processors, they must be configured in separate clusters. VMware ESXi 5.0 requires 64-bit Intel or AMD processors with LAHF/SAHF support and a minimum of two cores, as referenced in the System Requirements.

• As a rough rule of thumb, the following calculation can be used to determine how many virtual desktops can be supported per ESXi host, where processor is the primary bottleneck:

\[
\text{Virtual Desktops per Server} = \text{Virtual Desktops per Core} \times (\text{Server Cores} - 1)
\]

<table>
<thead>
<tr>
<th>User Group</th>
<th>Virtual Desktops Per Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>Light</td>
<td>8-10</td>
</tr>
<tr>
<td>Normal</td>
<td>6-8</td>
</tr>
<tr>
<td>Power</td>
<td>4-6</td>
</tr>
<tr>
<td>Heavy</td>
<td>2-4</td>
</tr>
</tbody>
</table>

Table 2: Virtual Desktops per Core

Note: Each implementation will have different resource requirements. Scalability testing should be completed to provide more accurate figures.

Note: For additional information on virtual machine based resource allocation, please refer to CTX127277.

• Disk – At a minimum, ESXi requires a 1GB boot partition. When booting from a local disk, or SCSI/iSCSI LUN, 5.2GB of storage is required to create the VMFS volume and a 4GB scratch partition. Sufficient storage will be required for VM hosting, depending upon the Citrix FlexCast model used.

• Memory – Sufficient RAM should be specified for ESXi operations as well as the anticipated number of virtual machines. ESXi requires a minimum of 2GB of RAM. For information on virtual machine based resource allocation, please refer to CTX127277.

vSphere uses multiple methods to manage and optimize memory, such as transparent page sharing, memory ballooning, and host swapping. More details on memory management within vSphere can be found in the VMware Technical Paper Understanding Memory Management in vSphere 5.

  – Transparent Page Sharing (TPS) – When multiple virtual machines are using identical pages of memory, TPS reclaims the redundant copies in memory and allows a single copy to be shared across multiple virtual machines.
- Ballooning – Uses a balloon driver within a virtual machine to artificially increase memory pressure within the guest operating system, causing the operating system to page memory to disk, and free up memory at the hypervisor level. Ballooning uses a target balloon size from the hypervisor which determines how much to inflate or deflate the memory balloon. While this can ease memory pressure on the hypervisor if memory is overcommitted, it can potentially cause performance issues for the virtual desktop due to swapping.

- Memory Compression/Swapping – When TPS or Ballooning fails to reclaim memory, ESXi will swap at the hypervisor level. With vSphere 5, an option for memory compression has been added which allows for a compression cache in memory where compressible pages can be stored rather than swapping to disk. Swapping to disk has a very high performance penalty on the hypervisor operations.

In general, Citrix recommends that the aforementioned features be enabled; but that memory is allocated such that the XenDesktop environment is not dependent on memory overcommit. If the ESXi host does not run into memory contention issues, then Ballooning or Memory Compression/Swapping will not occur. Citrix recommends that memory overcommit be used only for non-critical environments and that baseline performance testing should begin with a 10-15% range of overcommit.

- Component Redundancy – The hardware selected for the ESXi hosts should have sufficient redundancy to meet the requirements of the proposed XenDesktop solution, for example disk, power, cooling, storage connections and network. Depending on requirements, it may be necessary to offer different levels of redundancy per cluster.

The use of blade servers introduces specific redundancy requirements not associated with traditional server deployments. For scenarios where a high level of redundancy is required, consider the following recommendations:

- Network Switches – Within each enclosure, each blade should be logically attached to diverse blade enclosure switches. The blade enclosure should provide redundant network uplinks to the backbone network.

- Redundant FC-SAN Switches – Within each enclosure, each blade should be logically attached to diverse SAN switches. Each blade enclosure should provide redundant connectivity to the SAN fabric(s).

- Redundant Chassis Power – Each chassis should be configured with redundant power supplies.

- Redundant Chassis Cooling - Each chassis should be configured with redundant cooling fans.

- Redundant Admin Connectivity – Where out-of-band management interfaces are provided, these too should ideally be redundant.
• Network Interface Cards (NIC) – There are a number of factors which must be considered when determining the number of NICs required in each ESXi host, please refer to the networking section of this document for further information:

  ∙ At a maximum, ESXi 5.0 supports 32 network cards.

  ∙ VMware ESXi allows for NIC teaming and link aggregation to enable network redundancy, load balancing and fail-over. Specific details on requirements for link aggregation can be found in VMware Knowledge Base article 1001938.

  ∙ If sufficient infrastructure exists, performance may be improved by separating different types of network traffic across multiple physical NICs, for example management, virtual machine, provisioning, backup and storage (iSCSI and NFS) traffic can all be isolated from each other.

Sharing network cards between virtual desktops can lead to a network bottleneck. The use of fast network adapters/switches (1 GBps or greater) will help prevent the network from becoming a bottleneck.

• Storage Controllers – High performance solutions include Fiber Channel SAN and hardware iSCSI, while lower throughput can be achieved using standard network adapters and configuring software iSCSI or NFS.
Scaling Options | Recommendation
---|---
Scaling | Up Out | Scaling out typically offers better density and minimizes risk.
Processor | Intel VT AMD-V | Intel and AMD processors cannot be mixed in a vSphere cluster. Intel VT or AMD-V are required for 64-bit virtual machines (e.g. XenDesktop Controllers)
Memory | 2GB Minimum | VMware ESXi requires a minimum of 2GB of RAM. Memory should be sized for virtual desktop requirements. For planning guidance, see CTX127277.
vSphere Memory Management | Enabled | Enabled, but no dependencies. RAM should typically be allocated based on peak utilization to ensure that enough physical RAM is available without Ballooning/Compression/Swap.
Disk | 5.2GB minimum | The vSphere hypervisor needs a minimum of 5.2GB of storage (inclusive of ESXi, a VMFS volume and a 4GB scratch partition). For virtual desktop disk requirements, determine sizing based on FlexCast model storage recommendations.
Network Cards | 1 to 32 | 4-8 x NICs –
• NIC (preferably bonded) for virtual machine
• NIC (preferably bonded) for management/HA
• NIC (preferably bonded) for storage and backup
• NIC (preferably bonded) for provisioning (if used)

Table 3: Hardware Recommendations

Networking

When integrating vSphere with XenDesktop it is important to consider the following key networking topics:

- Compatibility – Network adapters should be selected from the vSphere Hardware Compatibility Guide.
- NIC Configuration – The host’s networking resources are shared by the virtual desktops it supports. If insufficient bandwidth exists, users will experience a degraded level of performance. As such, Citrix recommend the use of fast network cards and switches (1Gbps or greater) to help address this concern.

If sufficient infrastructure exists, performance may be improved by separating different types of network traffic across multiple physical NICs, for example management, virtual machine,
storage, provisioning and backup traffic can all be isolated from each other. For details on how to setup a multi-homed virtual desktop, please refer to CTX120955.

- NIC Teaming – The implementation of NIC teaming allows for increased resiliency by allowing a pair of network cards to function as a single entity. Both load balancing and failover configurations can be configured depending upon the desired configuration requirements. Ideally, NICs within each bond should be diversely routed so that a single switch failure does not bring down the bond.

- Provisioning Services – Provisioning Services is a network intensive application that could negatively impact the performance of other network traffic. For example, Provisioning Services typically streams 200MB of data across the network during the boot process of a single Windows 7 x86 desktop. Depending on the impact Provisioning Services will have on the underlying network, it may be necessary to implement link aggregation or to create a separate physical network dedicated to Provisioning Services traffic. Given that vSphere supports 802.3ad and LACP in static modes, link aggregation can be utilized to address the increased network requirements for Provisioning Services without upgrading the network.

For details on how to create a separate Provisioning Services network with XenDesktop, please refer to CTX120955. For details on the average data transfers during boot-up by operating system, please refer to CTX125744.

- Addressing – IP addresses need to be assigned to the management interfaces and individual virtual machines. As such, the design must consider the IP addressing requirements for these components and have sufficient IP’s available for all the necessary VM’s that are to be started.

- Resiliency – Many servers today are supplied with NICs offering two or more ports. As such, it is important that any NIC teams created consist of connections from two separate physical NICs so that a single card failure does not bring down the bond. Redundancy should also encompass the external network. Teamed NICs should be diversely connected to external switches to help reduce the risk from a single switch failure.

- VLANs – Many network environments take advantage of VLAN technologies to reduce broadcast traffic and enable complex virtual network configurations which would otherwise not be possible. Requirements may exist for separate VLANs per resource pool or even desktop group. VMware vSphere supports the configuration and use of 802.1Q tagged VLANs. Each ESXi host in a cluster will need to have its physical NICs connected to specific VLAN trunk ports to allow for the correct routing of VLAN tagged traffic. For additional information on VLANs, please refer to “VLAN configuration” in the Advanced Networking section of the vSphere 5 Product Documentation.
Security – High security environments may require firewalls to be placed between various Citrix components within the data center. When integrating vSphere with XenDesktop it is essential to ensure that either port 80 or 443 is open (depending on encryption requirements) between the XenDesktop Controllers and the ESXi hosts to facilitate machine state queries and power management operations. For more information on the ports required by XenDesktop and other Citrix technologies, please refer to CTX101810.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Options</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC Hardware</td>
<td>HCL</td>
<td>Selecting components from the vSphere Hardware Compatibility Guide ensures they are certified and supported.</td>
</tr>
</tbody>
</table>
| NICs per host  | 1 to 32 | 4-8 x NICs –
|                |         |   • NIC (preferably bonded) for virtual machine
|                |         |   • NIC (preferably bonded) for management/HA
|                |         |   • NIC (preferably bonded) for storage and backup
|                |         |   • NIC (preferably bonded) for provisioning (if used)                          |
| NIC Configuration | Consistent across cluster | Same across all hosts within the cluster. When using multiple port NICs, bonds should be created using ports from disparate physical NICs for additional redundancy. |
| NIC Teaming - HA | Enabled | Enable bonding to improve redundancy provided sufficient NICs, switches and ports are available. Bonds should be diversely routed to help reduce the risk from a single switch failure. |
| LAN / VLANs    | 2+      | For reasons of security and performance, the XenDesktop infrastructure should be hosted on a separate LAN/VLAN to the virtual desktops. |

Table 4: Network Recommendations

Storage

For an introduction to storage, please refer to CTX118397, and the XenDesktop storage best practices guide CTX130632. Storage has a major impact on the performance, scalability and availability of the XenDesktop implementation. As such, storage requirements must be considered for each key component:

1. ESXi hosts – At a minimum, VMware ESXi requires 5GB of storage for the base install. Windows Server VM or physical machine is required for vCenter server, with a minimum of 3GB of disk space beyond that required for the Windows OS install. Additional space may be required if the vCenter database is local on the server.

2. Virtual Machines – Those virtual machines which do not utilize Provisioning Services or Machine Creation Services will require dedicated storage to host their virtual disk image(s).
3. **Provisioning Services** – Sufficient storage must exist for the Provisioning Services store to support the estimated number of vDisks required, including backups and future updates.

   Each target provisioned from a shared vDisk must have sufficient storage available to host its write-cache, which can either be hosted on the target itself (RAM/local storage/shared storage) or a Provisioning Services Server (local storage/shared storage). In most situations, consider using either local or shared storage on the target device due to the following concerns:

   a. **Device-RAM** – Provides fastest level of access, but is an expensive use of memory.

   b. **Provisioning Services-Storage** – Adds additional latency as requests to/from the cache must cross the network.

4. **Application Streaming** – The Application Hub is a file share or web server used to host streaming profiles. For details on sample profile sizes, please refer to CTX114838.

5. **Database Storage** – Storage must be allocated at a minimum for the vCenter database and a Citrix XenDesktop site database. Other databases may be needed based on current and future requirements:

   - XenDesktop Site
   - XenApp Power and Capacity Management
   - Command Center
   - XenApp Farm
   - vCenter Database
   - Provisioning Services farm
   - XenApp Configuration Logging
   - EdgeSight for NetScaler
   - EdgeSight for XenApp / Endpoints
   - vSphere Update Manager

6. **User Profiles / Data** – Central storage is required to share profiles and data between multiple Desktops / XenApp Servers.

7. **Machine Creation Services (MCS)** – Storage must be allocated for the Master, ID and Difference Disks. Where possible, MCS will use thin provisioning to optimize the disk space used in the creation of the target virtual machines. Machine Creation Services can be used with local disks, NFS and block storage.

   The XenDesktop storage design should focus on the following key areas so that the most appropriate storage solution is selected:

   - **Local/Shared Storage** – Virtual deployments typically utilize shared storage in preference to local storage. This can be an expensive strategy, especially for SMB, where there may not be an existing enterprise storage solution to leverage. As an alternative, it may be possible to achieve the required level of performance and redundancy through the use of local storage. Although using local storage may require additional disks and array controllers to be purchased per server the overall cost is likely to be less than that of an enterprise storage solution, especially if a storage system is not already in place.
A disadvantage of local storage is a reduced level of scalability due to the hardware limit on the number of disks supported, particularly for blade systems. As the number of virtual desktops per host increases, additional disks may be required to accommodate the number of IOPS generated. For example, 15K SAS disk drives, which provide approximately 150 IOPS, can support around 10-15 Virtual Desktops per available drive. Another limitation is that shared storage is required to support vMotion, DRS and High Availability. Although these features are less critical when supporting virtual desktops, they are still very important for server workloads.

- **Tiered Storage** – A one-size-fits-all storage solution is unlikely to meet the requirements of most virtual desktop implementations. The use of tiered storage, where different storage technologies such as Solid State Drives, network attached and fibre channel attached storage systems, as well as different drive access technologies such as SAS, SATA, etc. are grouped together into storage tiers, provides an effective mechanism for offering a range of different storage options differentiated by performance, scalability, redundancy and cost. In this way, different virtual workloads with similar storage requirements can be grouped together and a similar cost model applied.

- **Performance** – The performance requirements for each desktop group must be considered during the design of the datastores:
  - **Storage Architectures** – If Network Attached Storage (NAS) is to be used, consider isolating this traffic onto a separate physical network to help prevent congestion.
  - **Storage Controllers** – High performance solutions include Fiber Channel SAN and hardware iSCSI, while lower throughput can be achieved using standard network adapters and configuring software iSCSI or NFS. The performance of Fiber Channel and iSCSI can be improved by implementing multiple storage adapters and configuring them for multipathing, where supported. Also, when used with compatible storage arrays, VMware Storage APIs for Array Integration (VAAI) can improve performance by offloading some of the storage operations from the ESXi hosts directly to the hardware, allowing for increased density of Virtual Machines per Storage LUN.
  - **SSD/HDD** – As the cost of Solid State Drives (SSD) falls, more and more organizations are benefiting from the performance of these drives. However, SSD is still significantly more expensive than the traditional Hard Disk Drive option (HDD), and consideration must be taken for both the write and read performance on specific SSD Devices as some lower cost devices may not provide the desired performance.
Disk I/O Interface – ESXi provides built-in support for local SATA, SCSI and SAS interfaces as well as support for iSCSI, NFS, and Fibre Channel RAID. In RAID configurations, RAID-5 will incur higher write penalties; 4-6 IOPS per write depending upon the number of physical disks and parity stripes, versus RAID-0, 1 and 10 as shown in Table 5. As virtual desktops delivered through Provisioning Services are typically write-intensive (80% write / 20% read), RAID-1 or RAID-10 should be considered for the Provisioning Services write-cache in preference to RAID-5 due to the associated write penalties. MCS virtual machines have a more balanced read/write profile (50% write / 50% read) but will also benefit from increased performance of RAID 1 or RAID 10 configurations:

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Write Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID-0</td>
<td>1</td>
</tr>
<tr>
<td>RAID-1 &amp; RAID-10</td>
<td>2</td>
</tr>
<tr>
<td>RAID-5 (3 data &amp; 1 parity)</td>
<td>4</td>
</tr>
<tr>
<td>RAID-5 (4 data &amp; 1 parity</td>
<td>3 data &amp; 2 parity)</td>
</tr>
<tr>
<td>RAID-5 (5 data &amp; 1 parity</td>
<td>4 data &amp; 2 parity)</td>
</tr>
</tbody>
</table>

Table 5: IOPS Write Penalty for RAID Configurations

The disk activity for the Provisioning Services vDisk Store will primarily consist of reads, provided that it is not used for private vDisks or server side caching. In this scenario, RAID-5 offers an acceptable solution at a reduced cost to protect the vDisk store from a drive failure. It should also be mentioned that when evaluating RAID controllers, that battery-backed cache on the controllers is recommended to help preserve data integrity and increase performance.

IOPS – The number of IOPS generated will vary based on application set, user behavior, time of day and operating system used. Scalability testing should be performed to determine the IOPS required during boot-up, logon, working and log-off phases. Guessing the number of IOPS required is likely to lead to performance issues or an over-priced storage solution.

The boot process typically generates the highest level of disk I/O activity. As such, virtual desktops should be started in batches prior to the beginning of the business day to help reduce the load on the storage subsystem. In addition, disabling the automatic restart of virtual desktops following logoff will also help to reduce storage load.

The Windows XP setup and diskpart utilities create misaligned boot partitions resulting in additional disk I/O activity. The diskpart utility included with Windows Server 2003 SP1 and Windows 7 addresses this issue. However, misaligned offsets may still occur depending on the size of the partition. The recommended approach is to always manually create the partition offset with diskpart on all virtual hard disks prior to formatting. For more information on
calculating the correct offset, please refer to the following article from Microsoft – KB929491.

The number of IOPS generated by the virtual desktops can be further reduced through operating system optimizations. For more information, please refer to the Windows XP –CTX124239 and Windows 7 –CTX127050 optimization guides for XenDesktop.

Current and future requirements for multiple staggered shifts must be considered, as there is likely to be a significant impact on performance due to the increased logon and logoff activity.

The number of virtual disk images assigned to each datastore will have a direct impact on performance. A balance must be found between performance, cost and management.

- **Load Balancing** – vSphere 5 introduces the concept of Storage Clusters and Storage DRS (Distributed Resource Scheduler) to provide load balancing and automated data placement. A storage cluster groups similar vSphere datastores together as a single managed entity, and Storage vMotion and Storage DRS can control the placement of virtual machine disk files manually or in an automated fashion based on datastore capacity and/or I/O load within the cluster. Storage DRS can be used for XenDesktop infrastructure components or streamed and static virtual machines, but is not currently supported for use with Machine Creation Services.

- **Redundancy** – vSphere datastores must be designed to meet the redundancy requirements of the components which they support. This includes RAID levels, storage adapters and the back end storage configuration. The best practice for shared storage is to configure two NICs or HBAs in a bonded or multipath setup.

- **Provisioning Services** – The vDisk store should be configured so that Provisioning Services can leverage the Windows System Cache. This can either be accomplished by hosting the vDisk store on a block-level storage device with the default Provisioning Services configurations or on CIFS storage through modifications to the Provisioning Services registry as referenced here. For more information on memory considerations for Provisioning Services, please refer to CTX125126.
Thin Provisioning – Thin provisioning can be used to present more storage space to the virtual machines than is actually available on the datastore. The VMware File System (VMFS) allows for thin provisioning at the virtual disk (VMDK) level, allowing Virtual Machines to take advantage of thin provisioning across a wide range of storage devices, including block level storage.

**Warning:** If using thin provisioning in production environments, take appropriate measures to ensure that sufficient storage exists. If available disk space is exhausted, virtual machines will fail to write to disk, and in some cases may fail to read from disk, possibly rendering the virtual machine unusable.

<table>
<thead>
<tr>
<th>Decision</th>
<th>Options</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Location</td>
<td>Local</td>
<td>Use Tiered storage to optimize the location of virtual desktops and other virtual machines based on their specific performance and availability requirements.</td>
</tr>
<tr>
<td></td>
<td>Shared</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tiered</td>
<td></td>
</tr>
<tr>
<td>RAID for Provisioning Services Write Cache or Machine Creation Services</td>
<td>All RAID levels</td>
<td>RAID-1 or RAID-10 to optimize the read/write performance.</td>
</tr>
<tr>
<td>RAID for Provisioning Services vDisk Store</td>
<td>All RAID levels</td>
<td>RAID configuration is recommended to protect the vDisk store from drive failure. RAID 5 is a good option to balance cost and protection as write performance is generally not an issue.</td>
</tr>
<tr>
<td>vDisk Store Storage</td>
<td>Block Level</td>
<td>Ensure that Provisioning Services is able to leverage the Windows System Cache for the vDisk Store.</td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>MCS Storage</td>
<td>Local</td>
<td>MCS should reside on thin provisioned storage. If High Availability of virtual desktops is desired, local storage should be avoided as it does not support vMotion/HA/DRS.</td>
</tr>
<tr>
<td></td>
<td>NFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Block</td>
<td></td>
</tr>
<tr>
<td>Thin Provisioning</td>
<td>Enabled</td>
<td>Enabled, but the amount of free storage space available should be actively monitored.</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: Storage Recommendations
# Implementation Considerations for XenDesktop on vSphere

The table below outlines general considerations for implementing XenDesktop 5.5 on vSphere. For specific implementation steps, refer to the [XenDesktop Deployment Guide with vSphere](#).

<table>
<thead>
<tr>
<th>Area</th>
<th>Implementation Considerations</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere 5 vCenter</td>
<td>HTTPS communications are required between vSphere and XenDesktop Controllers. Install a certificate from a trusted third party Certificate Authority (CA) or enterprise CA on the vCenter server and all DDCs to enable setup of the VMware host using https://&lt;virtualcenterserver&gt;/sdk.</td>
<td>XD5.5, 5 vSphere 4,5</td>
</tr>
<tr>
<td>Storage Clusters</td>
<td>If storage clusters are used in vSphere configuration, XD host configuration cannot call the cluster by name. The individual datastores configured within the cluster must be configured manually in the host configuration in Desktop Studio.</td>
<td>XD 5.5, 5 vSphere 5</td>
</tr>
<tr>
<td>Storage DRS</td>
<td>Storage DRS should only be implemented for infrastructure servers or for virtual machines delivered as streamed or existing desktops. Storage vMotion, and therefore Storage DRS, is not supported for MCS created desktops.</td>
<td>XD 5.5, 5 vSphere 5</td>
</tr>
<tr>
<td>Citrix Provisioning Services (PVS) and vCenter</td>
<td>When creating a Provisioning Services target, create the target vDisk before installing the XD 5.5 Virtual Desktop Agent (VDA). Citrix WDDM drivers will conflict with the vCenter console during the creation of the target vDisk. The XD5.5 VDA can be installed once the imaging is completed and before the vDisk is placed in Standard mode.</td>
<td>XD 5.5 PVS 5.6, 6 vSphere 4,5</td>
</tr>
<tr>
<td>PXE Boot VMs</td>
<td>When creating a template VM for use with PVS, administrators need to set the network boot option in the VM BIOS settings, which must be done on a VM, not a template. Before creating the VM template, configure the VM to boot into BIOS (vSphere VM Settings) and then boot into BIOS and set the boot order for network boot first. Once this is saved, the VM can be converted into a template for use with PVS.</td>
<td>XD 5.5, 5 PVS 5.6, 6 vSphere 4,5</td>
</tr>
<tr>
<td>VMXNET3 NIC</td>
<td>When using VMXNET3 NIC configurations, install the Microsoft hotfix referenced in <a href="#">CTX125361</a>. For streamed images, this prevents an issue where VMs fail to boot. For pooled MCS images, this fix prevents VMs from showing a “Reboot Now” message on every restart.</td>
<td>XD 5.5, 5 PVS 5.6, 6 vSphere 5</td>
</tr>
<tr>
<td>ISO CD Storage</td>
<td>When creating streamed or pooled desktops, ensure that all ISO CD mount points have been removed from the master VMs before creating the catalogs. Note that having a mounted CD-ROM device within the virtual image can prevent vMotion for working successfully.</td>
<td>XD 5.5, 5 PVS 5.6, 6 vSphere 4,5</td>
</tr>
<tr>
<td>DRS Configuration</td>
<td>Use DRS Groups to group infrastructure services and virtual desktops to specific groups of hosts within a vSphere cluster. This is effective if there are multiple hosts within a cluster and separation between desktop delivery infrastructure and the virtual desktops is desired.</td>
<td>XD 5.5, 5 vSphere 4.1, 5</td>
</tr>
</tbody>
</table>

| Table 7: Implementation Considerations |
Appendix

vSphere Product Features

The following table outlines some of the VMware vSphere features referenced in this document and the vSphere product edition required to use them. For more information, refer VMware’s vSphere 5.0 editions comparison.

<table>
<thead>
<tr>
<th>Feature</th>
<th>vSphere Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Ballooning</td>
<td>Standard</td>
</tr>
<tr>
<td>Transparent Page Sharing</td>
<td>Standard</td>
</tr>
<tr>
<td>Thin Provisioning</td>
<td>Standard</td>
</tr>
<tr>
<td>High Availability</td>
<td>Standard</td>
</tr>
<tr>
<td>vMotion</td>
<td>Standard</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Distributed Resource Scheduler (DRS)</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Storage vMotion</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Storage Multipathing</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Storage DRS</td>
<td>Enterprise Plus</td>
</tr>
<tr>
<td>Distributed Switch</td>
<td>Enterprise Plus</td>
</tr>
</tbody>
</table>

*In addition to the features discussed, the vSphere Edition will dictate the entitlement to the amount of vRAM (32, 64, 96MB) and vCPU (8, 32 vCPU) available. This should also be considered in the selection of the appropriate vSphere Edition.

VMware vSphere Document Reference

A number of VMware articles and whitepapers were used in the development of this guide. While many are referenced in-line in this document, refer to the following list for more information and reference to VMware best practices:

- vSphere Documentation Center: http://pubs.vmware.com/vsphere-50/index.jsp
- Understanding Memory Management in vSphere 5: http://www.vmware.com/resources/techresources/10206
- Minimum System Requirements for ESX/ESXi:

- Installing vCenter Server 5.0 Best Practices:

- ESXi Installable and vCenter Setup Guide:
Acknowledgments

Citrix Consulting Solutions would like to thank all of the individuals that offered guidance and technical assistance during the course of this project including Rich Meesters, Nicholas Rintalan, Dimitrios Samorgiannidis, Andy Baker, Ray De Varona, and Carisa Stringer who were extremely helpful answering questions, providing technical guidance and reviewing documentation throughout the project. Additionally, thanks go to Peter Smeryage and Rafael Gomez who helped with the configuration and build out of the testing environment.

Product Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenDesktop</td>
<td>5.5</td>
</tr>
<tr>
<td>VMware vSphere</td>
<td>4.0, 5.0</td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Change Description</th>
<th>Updated By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Document Release for vSphere and XenDesktop 5.5</td>
<td>Rich Meesters</td>
<td>January 11, 2012</td>
</tr>
<tr>
<td>1.1</td>
<td>Technical Quality Assurance</td>
<td>Nick Rintalan &amp; Dimitrios Samorgiannidis</td>
<td>January 24, 2012</td>
</tr>
</tbody>
</table>

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2010 was $1.87 billion.

©2012 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.