Server Virtualization Infrastructure Deployment Guide:

Deploying NComputing L-series and vSpace on Virtual Machines
Due to the added complexity of hypervisors and VM management, every deployment with server virtualization software will be unique. The tips and tricks contained in this document are general in nature, and may not apply to every situation. If you are unfamiliar with server sizing, desktop virtualization, or large-scale deployments, it is strongly suggested that you consult a qualified professional prior to deploying.

Documentation version 1.00.1

©Copyright 2010 NComputing Corporation. All rights reserved.

NComputing, the NComputing Logo are trademarks or registered trademarks of NComputing Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of NComputing Corporation and its licensors, if any.

The documentation is provided “as is” and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. NComputing corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information contained in this documentation is subject to change without notice.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Server Sizing</strong></td>
<td>5</td>
</tr>
<tr>
<td>Processor</td>
<td>5</td>
</tr>
<tr>
<td>Memory</td>
<td>5</td>
</tr>
<tr>
<td>Storage</td>
<td>5</td>
</tr>
<tr>
<td>Network</td>
<td>6</td>
</tr>
<tr>
<td><strong>ESXi Virtual Machine Implementation</strong></td>
<td>8</td>
</tr>
<tr>
<td>Choosing an OS</td>
<td>8</td>
</tr>
<tr>
<td>Enable USB Support</td>
<td>8</td>
</tr>
<tr>
<td>Prevent Accidental Virtual NIC Removal</td>
<td>11</td>
</tr>
<tr>
<td>Disable Auto Connect for CD-ROMs</td>
<td>11</td>
</tr>
<tr>
<td>Disable Transparent Page Sharing (TPS)</td>
<td>12</td>
</tr>
<tr>
<td>VM Templates</td>
<td>13</td>
</tr>
<tr>
<td><strong>Windows VM Optimization</strong></td>
<td>14</td>
</tr>
<tr>
<td>Windows User Profiles</td>
<td>14</td>
</tr>
<tr>
<td>Remote Log-on Policy</td>
<td>14</td>
</tr>
<tr>
<td>Data Execution Prevention</td>
<td>14</td>
</tr>
<tr>
<td>Enable XP Themes</td>
<td>14</td>
</tr>
<tr>
<td>Remove IE Enhanced Security Module</td>
<td>14</td>
</tr>
<tr>
<td>Disable CD-ROM Autoplay</td>
<td>15</td>
</tr>
<tr>
<td>Disable “First Run” Page in Internet Explorer</td>
<td>15</td>
</tr>
<tr>
<td>Disable Winlogon Timeout</td>
<td>15</td>
</tr>
<tr>
<td>Disable Screensaver Password</td>
<td>15</td>
</tr>
<tr>
<td>Windows Performance Options</td>
<td>16</td>
</tr>
<tr>
<td>Disable Excess Processes</td>
<td>16</td>
</tr>
<tr>
<td>Force Off-Screen Compositing</td>
<td>16</td>
</tr>
<tr>
<td>SMB Traffic Optimization</td>
<td>17</td>
</tr>
<tr>
<td>vSpace Registration</td>
<td>17</td>
</tr>
<tr>
<td>L-Series Firmware Updates</td>
<td>17</td>
</tr>
<tr>
<td>L-Series Firmware Password</td>
<td>17</td>
</tr>
<tr>
<td>Server Roll-over Configuration</td>
<td>17</td>
</tr>
<tr>
<td>Assorted Console Settings</td>
<td>18</td>
</tr>
<tr>
<td>Auto Login on the Host</td>
<td>18</td>
</tr>
<tr>
<td>Exclude Programs from Video Acceleration</td>
<td>18</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>19</td>
</tr>
<tr>
<td>External Sources</td>
<td>19</td>
</tr>
<tr>
<td>Glossary</td>
<td>20</td>
</tr>
</tbody>
</table>
Overview

NComputing was founded with the goal of making desktop computing affordable for everyone, and is redefining the economics of desktop computing. NComputing is the fastest growing desktop virtualization company with 2.5 million NComputing virtual desktop solutions deployed in 140 countries. The NComputing solution can be deployed in a variety of ways to best suit the needs of a particular department or organization. Customers can either deploy the NComputing end-to-end solution standalone or in concert with server virtualization infrastructure solutions from popular providers such as Microsoft, VMware and Citrix.

The NComputing’s standard deployment architecture offers the best balance of simplicity, affordability and performance. In this architecture scenario, the NComputing vSpace desktop virtualization software is installed on an operating system that runs directly on a physical host (ranging from PC to server-class hardware). In this configuration, vSpace quickly transforms the host into a multiuser system capable of supporting up to 30 simultaneous users with the NComputing L-series virtual desktop.

For applications requiring additional flexibility, scalability and manageability – NComputing solutions can be deployed with server virtualization infrastructure that leverages virtual machines and hypervisor technology. Under this scenario, NComputing vSpace runs on a host operating system that is running inside a virtual machine. This configuration enables multiple vSpace hosts to run on a single physical server platform resulting in the ability to scale up and host a much larger number of users on a single physical machine (>100). Furthermore, the vSpace virtual machine hosts can be managed using standard management tools giving IT managers additional levels of flexibility and control. This approach is essentially an effective means of server consolidation. While deploying the NComputing solution with server virtualization infrastructure provides a number of benefits over the traditional model, it is also inherently more complex to deploy and greater care must be taken to design and deploy an effective solution.

This guide is intended to serve as a primer for those preparing to deploy NComputing vSpace and L-series products within hypervisor environments. Specific deployment guidelines are provided for VMware’s ESXi hypervisor. Other hypervisors such as Microsoft’s Hyper-V and Citrix’s XenServer may be used in conjunction with NComputing systems, however, ESXi is the leading hypervisor used for server consolidation in the market today, and as such it is the focus of this guide. However, many of the deployment guidelines in this paper also apply to other hypervisors.

This document provides an overview of key technical considerations for successful virtual machine deployment of NComputing products and includes a selection of specific guidelines to help you optimize the overall performance of the VM host and user sessions. Before you begin, you should familiarize yourself with the L-Series User Guide, which can be found on the Documentation page of the Support section of www.ncomputing.com website.

Important Note:

Due to the added complexity of hypervisors and VM management, every deployment with server virtualization software will be unique. The tips and tricks contained in this document are general in nature, and may not apply to every situation. If you are unfamiliar with server sizing, desktop virtualization, or large-scale deployments, it is strongly suggested that you consult a qualified professional prior to deploying.
Host Server Sizing

When choosing hardware for a virtual machine host, it is critical to first understand the expected use case. An environment to support a greater number of users inherently requires more resources than an environment with fewer users. The same is also true of environments where the users’ needs are more complex or demanding. The following sections discuss typical provisioning for different hardware components within a virtual machine host. These recommendations are estimates, and the needs of an actual deployment WILL vary. Note that it is suggested never to exceed 80% utilization of your server’s resources; this means provisioning for roughly 25% more users than are actually expected.

Processor

Today, a typical mid-range PC comes with a dual-core processor in the 2.4-2.6 GHz range. The average user only needs a fraction of this processing power, except for occasional bursts during intensive tasks. For most basic use cases, 600-800 MHz per user of processing power is sufficient provisioning. For more intensive use cases, such as multimedia playback or image manipulation, this number should be raised to 1.0 or 1.2 GHz. Multiply this value by the number of users you are serving to obtain a rough estimate of your deployment's processing needs. In some cases, these needs can be met with a single physical server, but many situations require a cluster of two or more physical systems to support the desired number of users.

When calculating the abilities of a given processor, multiply the processor’s speed (in GHz) by the number of physical cores. If the processor utilizes hyper-threading, include a 25% increase in processing power. The following calculation demonstrates the capabilities of a hyper-threaded quad-core 3.0 GHz processor:

\[
3.0 \text{GHz} \times 4 \text{cores} \times 1.25 (\text{hyper-threading}) = 15.0 \text{GHz} = 12-25 \text{users (depending on use-case)}
\]

Memory

NComputing greatly increases the efficiency of memory usage over typical one-user-per-OS-instance environments. As such, it is typically adequate to provision 2-3GB of memory per 10 users. Obviously, this value will vary depending on the types of applications used. Memory-intensive programs such as photo- or video-editing suites require special consideration.

Storage

Disk storage issues are often overlooked in standard desktop deployments, but they quickly become a serious bottleneck for virtual machines. Rather than measuring just disk Gigabyte sizes or platter speeds, virtual machine servers necessitate the consideration of IOPS (“Input/Output Operations Per Second”). A typical SATA desktop hard drive can deliver between 80 and 100 IOPS, and the average user will draw between 5-10 IOPS. Based on this, you can immediately see how storage access will become a major limiter to user experience as soon as you connect 15 or 20 users to the server. The solution is typically to implement a RAID storage environment. Below are some points to consider when deciding what sort of RAID to use, but it is ultimately up to you to choose a storage solution that is best for your environment and specific needs:

- **Read/Write IOPS** – In a virtualized environment environment, there is rarely an even balance between read IOPS and write IOPS. In fact, usually around 80% of the hard drive activity is for write operations, and that is an important consideration when calculating your RAID requirements.
**IOPS Penalty** – The type of RAID used can cause significant IOPS penalties, which result in diminishing returns as you add more drives. The table below lists these RAID trade-offs:

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Reads Used</th>
<th>Writes Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>RAID 1 (or 10)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>RAID 5 (or 50)</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>RAID 6 (or 60)</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

**Calculating RAID IOPS** – To support a user base of 50 (250-500 IOPS), the server should be provisioned with 600 IOPS. To calculate the RAID penalty, we take 80% of the total IOPS needs (480 IOPS), multiply them by the Writes Used value, then add in the remaining Read IOPS (120). The resulting value is the net IOPS required. Under the different RAID standards, this calculation looks like the following:

- RAID 1: (480 x 2) + 120 = 1,080 IOPS 12 SATA Drives
- RAID 5: (480 x 4) + 120 = 2,040 IOPS 23 SATA Drives
- RAID 6: (480 x 6) + 120 = 3,000 IOPS 34 SATA Drives

**Network**

When determining the network needs of your deployment, it is important to realize that there are two different sources of network activity. First is the communication between vSpace (on the server) and the L-series access devices. Depending on the product model and type of use, this network load can range from 100 Kbps up to 10 or 15 Mbps per connected device. Please see the table below for specifics.

<table>
<thead>
<tr>
<th>Typical Bandwidth Use (in Mbps)</th>
<th>L130</th>
<th>L230</th>
<th>L300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Office Apps</td>
<td>0.3</td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>Multimedia*</td>
<td>15</td>
<td>15</td>
<td>4 to 10</td>
</tr>
<tr>
<td>USB Transfers</td>
<td>2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Recommended Provisioning**</td>
<td>15</td>
<td>17</td>
<td>8 to 10</td>
</tr>
</tbody>
</table>

* The L130 & L230 are designed for no or limited multimedia use.
** These values are an estimate; please test your environment to ensure that network needs are met
The second source of network traffic is between the server and the rest of the network. This traffic can be calculated quite easily, as it will be roughly the same as if your users were on separate desktop PCs (typically no more than 10 Mbps). When planning your network, also take the following into account:

- When subnets are used, make sure all L-series devices and their corresponding hosts are placed on the same VLAN or subnet. This will help to ensure that all UDP-based product features can function normally (for communicating management information between the devices and vSpace on the host VM).

- Use at least one network card with gigabit capabilities on the host computer, AND use gigabit network switches and routers, to connect to the L-series devices. This will help prevent bottlenecking and data loss, and improve connection stability.

  **Note:** L-series access devices are equipped with a 100-megabit port and cannot utilize gigabit network speeds. However, the path to the host should still be gigabit-capable to prevent bottlenecking and subsequent data loss. Using managed switches or auto-detect 10/100/1000 ports can help ensure that the devices are not flooded with gigabit traffic, while the host is still served full gigabit.

- Make sure Jumbo Frames are disabled on your network; this feature can lead to stability problems for L-series client sessions.

- To improve network performance, use a separate NIC card and/or network path to send and receive vSpace L-series virtual desktop data (separate from the network path to the rest of the network/outside network). This will prevent collision and bottlenecking with other types of network traffic, such as internet communication or network file transfers.

- If multiple vSpace hosts are being regularly accessed by each L-series device, make sure each host can communicate with NComputing's registration server. This communication takes place over TCP port 3630, and the server is hosted at register.ncomputing.com.

  **Note:** If “Background Activation” is enabled, this process will be performed silently, with no user input required when new devices are added. See the L-series User Guide for information on enabling this feature.
ESXi Virtual Machine Implementation

Now that you have properly sized the virtual machine host, the next logical step is to decide how to divide your resource pool into distinct virtual machines. With physical vSpace hosts, we would normally try to squeeze as much as possible out of each vSpace instance. When dealing with virtual machines, however, the optimal balance tends to be found with fewer users per VM. For a typical, low-multimedia use case, the following specifications are recommended. As always, you must test your host under full load to ensure that sufficient resources have been allocated.

- 2 Virtual CPUs
- 2-3 GB Memory
- 8-10 Users per Virtual Machine (fewer if using multimedia)

Choosing an OS

NComputing supports a variety of Microsoft Operating Systems, as well as Ubuntu Linux. Please see the vSpace OS Support Matrix by searching for “os support” at ncomputing.com/kb before choosing which OS to deploy. Also fully read the pages at ncomputing.com/mslicensing for information on Microsoft licensing in a multiuser environment.

Enable USB Support

VMware ESXi virtual machines do not have USB controllers associated with them by default; therefore, a standard Windows installation may not include any USB drivers and results in a lack of USB functionality. You can use either of the following methods to enable L-series USB functionality.

Add USB Method1 - Add USB functionality while creating a Virtual Machine:

During the creation process of an ESXi virtual machine, administrators can choose to add a virtual USB hub to the VM. This step takes place near the end of the VM creation process and is demonstrated in the images below:
Add USB Method 2 - Add USB functionality to an existing Virtual Machine:
If you need to add USB functionality to a virtual machine that has already been created, this change can be made from the VMware vSphere console as demonstrated in the images below.
Prevent Accidental Virtual NIC Removal

In some situations, ESXi will place a virtual machine’s virtual NIC in the system tray of the guest OS as part of the “Safely Remove Hardware” wizard.

If the NIC shows up in the Safely Remove Hardware wizard as seen to the right, you can prevent accidental removal by doing the following:

1. Connect a vSphere Client to ESXi or vCenter Server
2. Power off the virtual machine in question
3. Right-click the virtual machine
4. Click “Edit Settings,” then the “Options” tab
5. Click “General,” then “Configuration Parameters,” then “Add Row”
6. Insert a new row with the name “devices.hotplug” and the value “false”
7. Power the virtual machine back on.

Disable Auto Connect for CD-ROMs

Disabling the auto connection feature in a virtual machine that directs it to associate with the host’s CD-ROM can prevent the virtual machine from running a number of processes which in turn, saves on resource overhead. A picture of this setting, with Connection options unchecked, is included to the right:
Disable Transparent Page Sharing (TPS)

Though TPS can offer some gains in memory capacity, it is recommended that it be disabled due to the strain it places on the vmkernel of each running vSpace ESXi virtual machine. You can complete this process from the vSphere editor on your VM host.

First, from your vSphere editor, open the Settings for the VM in question as seen below and left.

Second, select the Options tab and Configure Parameters as seen to the right.

Click “Add Row” as seen below and left and add “sched.mem.pshare.enable” (no quotes) and set the value to FALSE as seen to the right.
VM Templates

Creating streamlined and optimized VM templates is the most important process you will face beyond your initial architecture definition. Leveraging Virtual Center’s template capabilities allows you to create a robust and manageable imaging system. Below are some general best practices for creating and managing VM templates.

To create a VM template, start by installing and configuring a VM with your desired base settings. Any application, setting, or user account created on this VM will be included in the template, and thus appear in any VMs subsequently created from the template. To avoid issues related to product registration, it is recommended that you NOT include vSpace in your VM Template. vSpace should be installed, registered, and tested on each VM as it is created. When you are ready to create a VM template, shut down the VM.

With the virtual machine turned off, right-click it and select Template > Convert to template. Follow on-screen prompts as needed. When the process completes, your template is ready to go, and you may begin deploying VMs from the created template immediately.

To create a VM, right-click the template and select “Deploy VM from this Template.” Once the virtual machine is named and a customization specification is designated, the machine will begin the clone/sysprep process.

When the VM cloning is finished, simply assign a static IP address, verify proper Active Directory membership, and install/register vSpace. After a final reboot, you are ready to connect your L-series access devices.
Windows VM Optimization

The following procedures are designed to optimize vSpace and the Windows operating system itself. They are considered “best practices” and are recommended to deliver the best system stability and to enhance the user experience. (The following are specific for the Windows Server 2003 OS to enable a Windows XP user experience, but similar procedures can be used for the Windows Server 2008 OS to enable a Vista user experience, and/or for the Windows Server 2008 R2 OS to enable a Windows 7 user experience.)

Windows User Profiles

Both local and domain user accounts can be accessed through an NComputing access device, as is the case with a standalone PC. These are standard Windows accounts and are created and managed through Windows in the same way you would any other user account. User accounts accessed through an NComputing device will retain their folder access settings, drive mapping, and group policies. It should be noted, however, that users on NComputing devices are treated as Remote Users for the purpose of some settings and policies.

Remote Logon Policy

By default, Windows only allows Terminal Services (TS) or Remote Desktop Services (RDS) logins for Administrators and Remote Desktop Users. To allow access for other users or user groups, please open the Group Policy Editor (Run > “gpedit.msc”) and navigate to [Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment]. Under this category, double-click the policy object named “Allow log on through Terminal Services” or “Allow log on through Remote Desktop Services”, and add the desired user or user group. To enable all users with local logon rights, add “Everyone” to this policy.

Data Execution Prevention

To help ensure NComputing’s services are able to run properly, Data Execution Prevention (DEP) should be set to “Essential Windows programs and services only”. To make this configuration, right-click My Computer and go to Properties > Advanced (tab) > Performance Settings > Data Execution Prevention (tab).

Enable XP Themes

1. Go to Start > Run > “services.msc” > OK. Change the “Themes” service to “Automatic” and click “Start”
2. Go to Start > Run > “gpedit.msc” > OK. Expand [User Configuration > Administrative Templates > Control Panel > Display > Desktop Themes]. Change “Load a specific visual style file or force Windows Classic” to “Enabled” and point it toward “%windir%\Resources\Themes\Luna\luna.msstyles”.
3. Click Apply

Remove IE Enhanced Security Module

1. Start > control panel > add remove programs
2. Select “Add/Remove Windows Components”
3. Uncheck “Internet Explorer enhanced security configuration”
4. Continue and complete the uninstallation.
Disable CD-ROM Autoplay (At the Administrator’s discretion)

Setting the following registry value will prevent the CD-ROM auto-play prompt from appearing on all terminals.

1. Start>Run>Regedit>HKLM>System>CurrentControlSet>Services>CdRom
2. Set Autorun DWORD value to 0

Disable “First Run” Page in Internet Explorer

To prevent all users from needing to go through the process of Internet Explorer’s custom set up you can instead set the following registry values:

1. Launch the Group Policy Editor (Start > Run > “gpedit.msc”)
2. Navigate to [Computer Configuration > Administrative Templates > Windows Components > Internet Explorer]
3. Double-click “Prevent performance of First Run Customize Settings”
4. Set the value to “Enabled”
5. Once enabled, you must make one of two choices from the available drop-down menu:
   - Skip Customize Settings, and go directly to the user’s home page.
   - Skip Customize Settings, and go directly to the “Welcome to Internet Explorer” Web page.
6. A restart may be necessary for this configuration to take effect.

   Note: If you disable or do not configure this policy setting, each user will go through the regular “First Run” process when launching Internet Explorer.

Disable Winlogon Timeout (At the Administrator’s discretion)

By default, an access device that is connected to a host but not logged in will disconnect after a certain period of time. This is to prevent too many idle sessions from sitting at the Windows login screen for extended periods of time, using up available sessions. However, in certain configurations (such as when a terminal has been configured to “auto-connect” to a host or hosts) this can be detrimental. To disable this function, make the following registry change.

Start>Run>regedit>HKU>.Default>Control Panel>Desktop>ScreenSaveTimeOut – change value to 100

Disable Screensaver Password (At the Administrator’s discretion)

By default in most Active Directory environments, a user’s session would be “locked” after going to a screensaver. This can be disabled in a system’s local policy if desired.

1. Click Start > Run
2. Type in gpedit.msc and Click OK.
3. Expand User Configuration > Administrative Templates > Control Panel.
4. Click the Display container.
5. In the Details pan, double click Password protect the screen saver.
6. Click Disabled.

7. Click OK.

Windows Performance Options

Optimize the speed and responsiveness of your vSpace host from within Windows. Disabling certain visual effects will remove graphical overhead, and by configuring the operating system to favor application processes over services, applications become more visually responsive, improving the overall user experience. To make these configurations, right-click My Computer and go to Properties > Advanced (tab) > Performance Settings. From here:

- **Visual Effects** – To reduce graphical overhead, uncheck any unneeded visual effects in this list. To remove all effects, simply click “Adjust for best performance.” It is important to note that this will also disable the Windows Themes, and return to a Windows Classic appearance.

- **Processor Scheduling** – Located under the “Advanced” tab, improve user experience by setting this to “Programs”

- **Virtual Memory** – System performance can be greatly affected by the size and management of virtual memory, called the “Paging File.” This should be set to “System Managed” except by advanced users.

Disable Excess Processes

To further streamline your host computer, it may be desirable to disable certain start-up programs and background services, which will use up system resources. Go to Start > Run > “msconfig” > OK to launch the System Configuration tool. Under the Services and Startup tabs, uncheck any service or program that is not needed during start-up.

Force Off-Screen Compositing

Certain elements of Internet Explorer’s rendering behavior are inefficient in a multi-user environment, and can be set to improve performance and prevent potential screen flickering issues. The following steps will properly configure one such element, called “Off-Screen Compositing”:

1. Open Notepad and copy-paste the following into a new text file:

   ```plaintext
   CLASS USER
   CATEGORY !!AdditionalSettings
   CATEGORY !!InternetExplorer
   POLICY !!ForceOffscreenComposition
   KEYNAME “Software\Microsoft\Internet Explorer\Main”
   PART !!ForceOffscreenComposition_Help TEXT END PART
   VALUENAME “Force Offscreen Composition”
   VALUEON NUMERIC 1
   VALUEOFF NUMERIC 0
   END POLICY ; !!ForceOffscreenComposition
   END CATEGORY ; !!InternetExplorer
   END CATEGORY ; !!AdditionalSettings
   [strings]
   AdditionalSettings=Additional Settings
   InternetExplorer=Internet Explorer
   ForceOffscreenComposition=Force Offscreen Composition
   ForceOffscreenComposition_Help=Force Offscreen Composition
   ```
2. Save the text document with an “.adm” extension, and a filename of your choice. (for example, “offscreen.adm”)
3. Start the Group Policy Editor (Start > Run > “gpedit.msc”)
4. Under “User Configuration”, highlight Administrative Templates
5. Go to View > Filtering and uncheck “Only show policy settings that can be fully managed”, then click “OK”
6. Right-click Administrative Templates and click “Add/Remove Templates.” Click “Add” and point to the text file you just created. Click “Close” to apply the Template.
7. Navigate to Administrative Templates > Additional Settings and click “Internet Explorer” to view the new policy, called “Force Offscreen Composition.”
8. Double-click this policy and change the value to “Enabled”.

**Server Message Block (SMB) Traffic Optimization**

To reduce excess SMB traffic and improve overall file server performance, it is recommended that certain changes be made to the registry as part of the general OS configuration process. Microsoft has created a write-up on these recommendations and their associated registry locations:


To save time with these configurations, you can copy the provided registry data into a text editor, save it as “smbtweaks.reg,” and double-click it. This will run all of the registry changes automatically, rather than requiring a time-consuming manual configuration.

**vSpace Registration**

NComputing products must be registered and activated before use. Prior to registration, sessions will stop after one hour and the software can only be used for 30 days after the initial install. Please see the User Guide for more information on this process: www.ncomputing.com/documentation.

**L-Series Firmware Updates**

Firmware updates are recommended for any new L-series products prior to deployment. Please see the User Guide or search our online Knowledgebase for more information: www.ncomputing.com/support.

**L-Series Firmware Password**

The L-series devices can be protected from tampering by setting a firmware password. This setting can be found in L-series device’s Device Setup, under the “Password” tab.

**Server Roll-over Configuration**

To reduce downtime risk from server failure, a single L300 device may have the autoconnect feature defined for multiple vSpace hosts. If the first host is unresponsive, the L300 device will move to the next host in its list and attempt to connect. This process repeats until a functional vSpace host is located. For information on configuring this feature, please see the L300 User Guide at www.ncomputing.com/documentation.
Assorted Console Settings

Within the vSpace Console, there are several settings that can be used to optimize your product experience. These are listed below:

- **Video Compression** – If you’re experiencing performance issues due to the network bandwidth needs of your L300 devices, you may limit multimedia stream quality. To configure this, open the vSpace Console and navigate to Software Settings (local) > Information & Settings > System Settings. The JPEG Compression Ratio is a percentage rating of quality. 95% means maximum video quality, and requires highest bandwidth. 5% is minimum video quality, with a respectively lower bandwidth requirement. It is important to note that by decreasing video quality, the CPU assisted compression can cause an increase in processor usage during video streaming events. In situations where your network is robust enough to handle higher quality video, you may see performance improvements by setting the video quality at maximum. The ideal setting for your environment should be determined through your own benchmarking.

- **Background Activation** – To automate the activation process for new L-series devices, this setting allows the vSpace software to automatically register and activate new devices as they are connected. It can be enabled under System Settings in the vSpace Console.

- **Clean-Up Disconnected Sessions** – vSpace has an automatic feature which will end any “orphaned” sessions after a predetermined interval. The default setting cleans up sessions after five minutes of being disconnected from any L-series device. This interval can be increased or decreased to suit the needs of the environment. Setting it to “0” will disable it, and orphaned sessions will remain logged in until the server is rebooted.

Automatic Login on the Host

To allow plug-n-play remote USB drivers to install and work properly, you will need to have a session with admin privileges logged into the host. Below are the steps to accomplish with this.

1. Open up the vSpace Console.
2. Expand Software Settings > Information & Settings and click on System Settings
3. Double click on the setting “Autologon on Host Station”
4. In the new window that opens Check the Box that says “Enable Autologon Mode on Main Station.”
5. Type in the information for the admin privileged user name and password. If you are using a Domain admin, make sure to use the fully qualified domain user name. Example: testdomain\user
6. Click OK

Exclude Programs From Video Acceleration

If a program displays frequent “blue box” flickering, it may be desirable to disable video streaming for that application. To do so, simply add the application’s executable to the following registry key:

[HKEY Local Machine > System > CurrentControlSet >Control > Multiuser > ExcludeVideoPlayerNameList]

Each program in the list must be separated by a semicolon. For example, “explorer.exe;firefox.exe”

With these applications in the excluded list, video acceleration will not attempt to accelerate graphical elements in the application(s).
Conclusion

This deployment guide is intended to provide the knowledge and confidence needed to successfully deploy the NComputing solution with VMware server virtualization infrastructure. If you have any questions, or encounter a problem not covered in this document, please feel free to contact NComputing technical support at www.ncomputing.com/support.

External Sources

<table>
<thead>
<tr>
<th>External Source</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NComputing Knowledgebase</td>
<td>ncomputing.com/kb</td>
</tr>
<tr>
<td>VMware Support Site</td>
<td>vmware.com/support/</td>
</tr>
<tr>
<td>VMware Compatibility List</td>
<td>vmware.com/resources/compatibility/search.php</td>
</tr>
<tr>
<td>Information on RAID (Wikipedia)</td>
<td>en.wikipedia.org/wiki/RAID</td>
</tr>
</tbody>
</table>
Glossary

- **ESXi Host** - The ESXi Host refers to the root ESXi hypervisor in which Guest Operating Systems – such as Windows – can be run.

- **Virtual Machine** - The Virtual Machine refers to the software wrapper that contains a Guest Operating System. Resources (Virtual CPU, Memory, etc) are assigned to the Guest Operating System through the Virtual Machine's configuration interface.

- **Guest Operating System** - The Guest Operating System is the operating system being virtualized by ESXi through the Virtual Machine. In the case of an L300 deployment on Windows Server 2008, Windows Server 2008 would be the Guest Operating System.

- **vSpace Host** - The vSpace Host refers to the Guest Operating System in which vSpace has been installed and to which the L-series terminal users connect.

- **VCPU** - ESXi allows individual CPU cores to be assigned as desired to Virtual Machines. These are referred to as Virtual CPUs.

- **vCenter** - Virtual Center enables complete centralized management of your virtual infrastructure. This enables console access to all NComputing vSpace VMs from one interface. With vCenter you can modify or deploy new vSpace VMs in seconds, reducing overall management time and increasing device uptime. vCenter also provides the ability to roll back vSpace VMs in the event of a software failure by leveraging snapshots.

- **vMotion** - Allows the migration of virtual machines between physical hosts. vMotion allows you to empty ESXi Hosts during the day so that maintenance can be done during production. This reduces the need for downtime and maintenance windows with outages. It also allows for manual load balancing of your ESXi hosts.

- **DRS** - Dynamic Resource Scheduler provides automated load balancing between physical VMware hosts. DRS makes it possible to provision more L-series terminals using less hardware, and to allocate computing resources where they are needed most. This can help provide a consistent user experience for all deployed terminals. DRS helps alleviate issues stemming from the extremely volatile load generation of virtual desktops.

- **HA** - In the event of a physical VMware host failure, High Availability will restart Virtual Machines on remaining hosts. High Availability prevents any extended downtime due to host hardware failure. vSpace servers will automatically restart and end users will only experience a few minutes of downtime versus hours of downtime due to traditional hardware failure.

- **ThinApp** - ThinApp allows for entire applications to be encapsulated as executables and run inside independent containers with zero operating system interaction. ThinApp can be used to overcome application compatibility issues with some software. It enables legacy application support as well as simplifying application management and deployment across an environment.

- **Fault Tolerance** - Provides continuous availability for applications in the event of ESXi hardware failure. Fault Tolerance guarantees 100% virtual machine uptime for your most critical applications. This is similar to an advanced version of High availability or built in business continuance.