MULTIMEDIA REDIRECTION: EFFECT ON SERVER CAPACITY FOR MICROSOFT RDS VIRTUAL DESKTOPS

Ran 17.7% more virtual desktops
with multimedia redirection enabled*
*versus the same Intel® Xeon® Processor X5570-powered server
running virtual desktops with multimedia redirection disabled

OUR FINDINGS

Organizations considering deploying virtual desktops as part of a Virtual Desktop Infrastructure (VDI) benefit by best utilizing the server and client resources that are available for deployment. VDI deployments are often associated with higher datacenter build-out costs due to the infrastructure required to deliver virtual desktops to the targeted user population. An IT department can save money by reducing the number of servers required to support these users. Multimedia redirection (MMR) technology can increase the number of virtual desktops a server can support by offloading the execution of multimedia content to a capable client. Principled Technologies put this methodology to the test. In our tests, a server running Microsoft® Windows Server ® 2008 R2 with Remote Desktop Services supported 17.7 percent more virtual desktops with MMR turned on. Thus, enabling MMR is an effective method for reducing server load.

OUR PROCESS

To determine how enabling MMR affected our server's virtual desktop capacity, we used the Login Consultants Virtual Session Indexer (Login VSI) Beta3 benchmark. Login VSI consists of several workloads that perform a range of tasks to simulate a typical office user. The results show the maximum number of virtual desktops a server can support for a maximum response time of a particular task. In addition to the performance scores from the Login VSI benchmark, we measured server and client[1] CPU utilization and network bandwidth.

[1] See our companion report at http://www.principledtechnologies.com/clients/reports/Intel/RDS_client_performance_1010.pdf.

OCTOBER 2010
A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Intel Corp.

PROJECT OVERVIEW

This report highlights the server capacity impacts and benefits of using multimedia redirection with Remote Desktop Services (RDS), the current desktop virtualization solution from Microsoft. We used Login VSI's multimedia workload in our tests because its workload reflects what a typical office user would run on his or her system.

For consistency of performance benchmarking, we added virtual desktops until the server CPU utilization reached saturation at 100 percent. Please note that we report the maximum number of virtual desktops a server can support with the specified response times. The actual number of users supported on the server may be less for a typical production deployment.

Figure 1 shows the maximum number of virtual desktops the test server supported with MMR enabled and disabled as reported by the Login VSI Beta3 multimedia workload tool. With MMR enabled, the test server supported 73 virtual desktops, 17.7 percent more than the 62 virtual desktops the same server supported when running with MMR disabled.

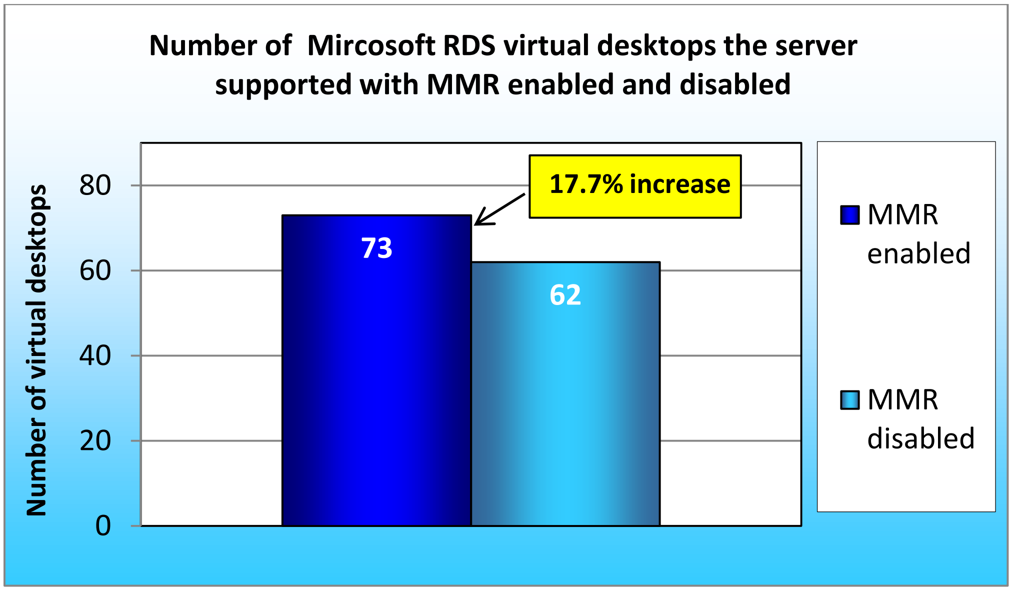

Figure 1: The number of Microsoft RDS virtual desktops the test server supported with MMR enabled and disabled. Higher numbers are better.

WHAT WE TESTED

About multimedia redirection

Multimedia redirection is a feature that lets physical clients use their local CPUs and graphics cards to format and play media content. Without MMR, this processing demand is on the hosting server, causing the server to utilize more resources per virtual desktop. Enabling MMR conserves server resources, allowing a given server to support more virtual desktops than it could without MMR running. In order to enable MMR, the physical client must support MMR and have sufficient resources to decode and render the media content. The user experience is greatly improved when using a more capable intelligent client.[2]

About Remote Desktop Services

RDS is one of the core virtualization technologies available in Windows Server 2008 R2. According to the Microsoft Web site, RDS represents the company's progress toward providing the best virtualization platform for accelerating and extending desktop and application deployments from the data center to any device. In addition to the traditional session virtualization scenario (formerly known as Terminal Services), RDS is expanding its role to provide an extensible platform for a Virtual Desktop Infrastructure (VDI). For more information on RDS, see http://www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx.

About Login VSI

Login VSI stresses virtual desktops by simulating a typical office user's work behavior. It does this by opening common office-related applications inside the virtual desktop. Specifically, the multimedia workload of Login VSI opens and closes the following applications and runs their respective tasks:

- Microsoft Outlook®: Browsing a message
- Microsoft Word® (TimerDoc): Response timer initiation
- Internet Explorer® instance one: Maximizing, scrolling, and minimizing
- Internet Explorer instance two: Navigating a Web site, maximizing, and scrolling
- Adobe® Flash®: Viewing a movie trailer
- Windows® Media Player: Opening an mp3 file
- Microsoft Word (UserRead): Reading and typing text, and printing to PDF
- Bullzip: Generating a PDF
- Adobe Reader®: Reading a PDF
- Microsoft PowerPoint®: Watching a presentation and adding a slide
- Windows Media Player: Viewing a720p WMV file at full-screen
- 7-Zip: Saving a zipfile

Login VSI benchmarks these virtual desktop sessions to determine how scalable a particular virtualized system is. Specifically, it benchmarks Terminal Server (TS), Virtual Desktop Infrastructure (VDI), and hypervisor performance by loading a system with these simulated Windows-based Office user workloads. It reports a Virtual Session Index (VSI) score as the maximum number of users the system supports while maintaining a 4,000-millisecond (4-second) response time. The workload begins by stressing a single virtual desktop and

[2] See our companion report at http://www.principledtechnologies.com/clients/reports/Intel/RDS_client_performance_1010.pdf.

then increases the number of virtual desktops by one at 1-minute increments. For testing, we had 90 virtual desktops powered on and sitting idle before starting the Login VSI multimedia workload.

For more information on Login VSI Beta3, see http://www.loginconsultants.com/index.php?option=com_content&task=view&id=390.

WHAT WE FOUND

To determine the impact of using MMR on a server running VDI sessions, we ran Login VSI on the same server configured two ways: with MMR enabled and with MMR disabled. We found that enabling MMR decreased both network bandwidth and server CPU utilization. We make comparisons of MMR enabled and MMR disabled at 50 virtual desktops to show how both perform at lower user counts, not just at maximum user counts. Figure 2 shows the network bandwidth and CPU utilization advantages with 50 users or virtual desktops. It is this reduction in resource utilization that gives the server the headroom necessary to support more virtual sessions with MMR enabled.

50 virtual desktops	Multimedia redirection enabled	Multimedia redirection disabled
MB/s	15.70	19.07
Percentage CPU utilization	65.52%	76.62%

Figure 2: MB/s and percentage CPU utilization with 50 virtual desktops running. Lower numbers are better.

We ran Login VSI while both enabling and disabling MMR to a total of 90 virtual desktops on the same server. Figures 3 and 4 show the network bandwidth and CPU utilization with varying numbers of users.

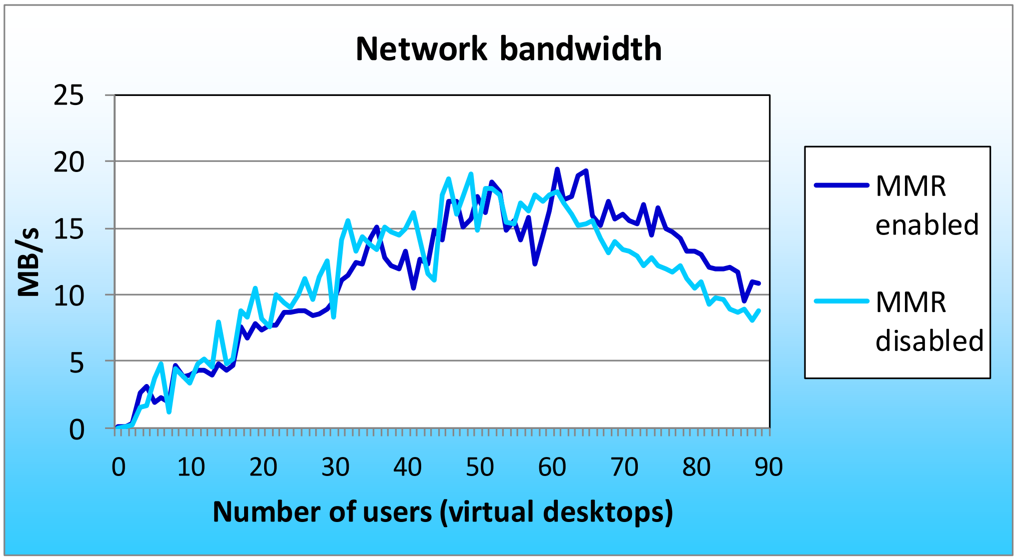

Figure 3: The network bandwidth in MB/s for each configuration at different virtual desktop counts. Lower numbers are better.

Figure 3 shows the network bandwidth, in MB/s, for each configuration at different user counts. At certain user counts, enabling MMR uses less network bandwidth. The network bandwidth with MMR both enabled and disabled decreases past the maximum number of virtual desktops supported while providing an acceptable response time (73 virtual desktops with MMR enabled and 62 virtual desktops with MMR disabled). This is because of system congestion due to the server reaching saturation. A server with MMR enabled uses more network bandwidth at the higher user counts (80 to 90) because the server handles more virtual desktops, thus requiring more users to hit the saturation point. Because a server with MMR disabled reaches saturation sooner, the network bandwidth begins to degrade earlier. We attribute this degradation to a higher dropped frame rate as the server exceeds saturation.

Figure 4 shows the percentage of server CPU utilization for each configuration at different virtual desktop counts. Enabling MMR results in less CPU utilization, thus freeing up processor cycles for other tasks.

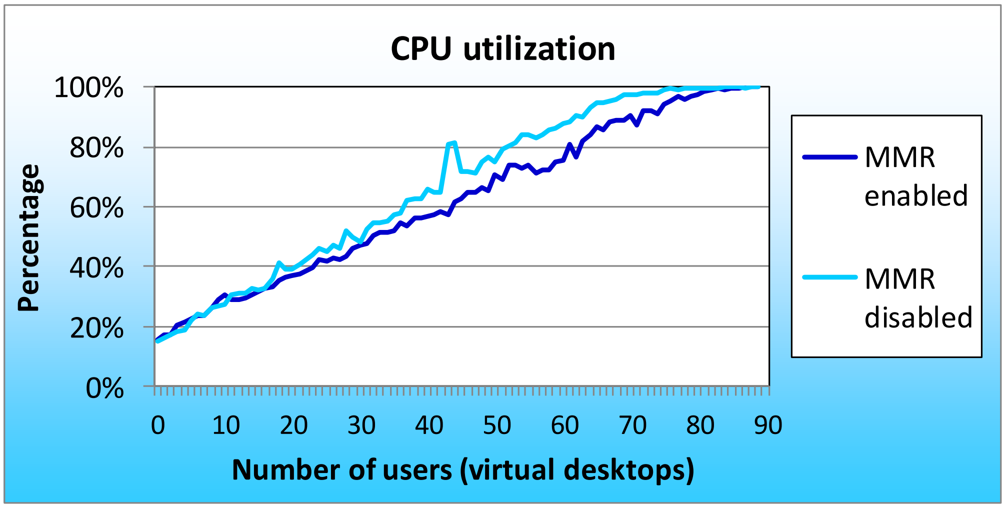

Figure 4: The percentage CPU utilization for each configuration at different virtual desktop counts. Lower numbers are better.

In a production environment, a VDI server would be run below saturation to provide ample headroom for variation in user workload. For a typical design point of 75 percent server CPU utilization, as shown in Figure 4, the server can support 60 virtual desktops with MMR enabled and can support 50 virtual desktops with MMR disabled. In this case, enabling MMR improves the server's virtual desktop loading by 20 percent.

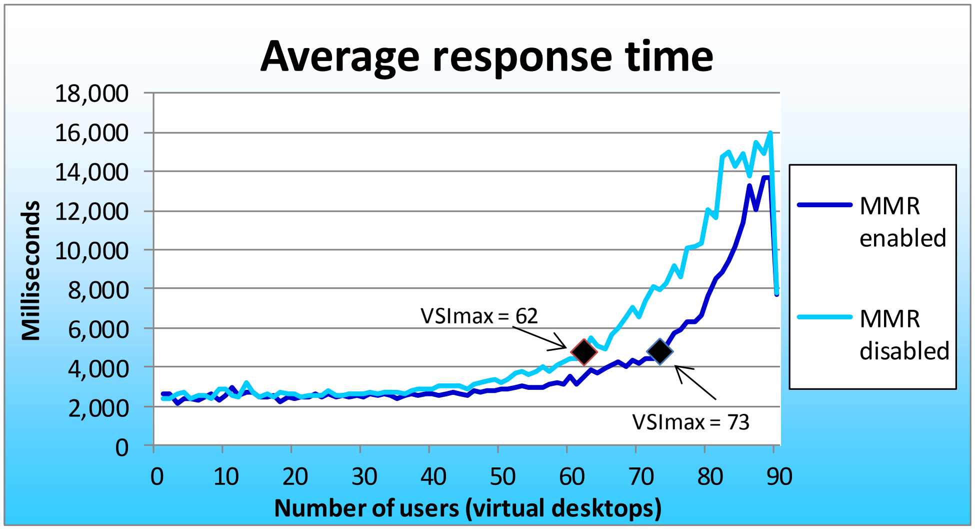

Figure 5: The average response time for MMR enabled and MMR disabled at different virtual desktop counts. Lower numbers are better.

Figure 5 shows the average response times for both MMR enabled and MMR disabled at varying user counts, and shows the VSImax for reference. Please note that the Login VSImax numbers differ slightly from the average response times due to the way Login VSI calculates results. The Login VSImax is based off the average response time, but it removes 2 percent from the minimum and maximum response times before calculating the average. Therefore, the Login VSImax shown on this graph is slightly higher than the 4-second acceptable response time.

One should also note that Login VSI results are based on average response time. Individual user response may vary as indicated by the maximum response.

For corresponding results with Citrix® XenDesktop™, please refer to http://www.principledtechnologies.com/clients/reports/Intel/MMR_effect_VDI_XenDesktop_1010.pdf.

SUMMARY

Organizations deploying VDIs often worry about the cost of such deployments. By utilizing Microsoft Windows Server 2008 R2 with Remote Desktop Services and enabling multimedia redirection, organizations can expect to purchase fewer servers to handle the amount of virtual desktop users they have. In our tests, we found that enabling MMR increased the amount of virtual desktops an Intel Xeon processor X5570-powered server running Remote Desktop Services could support by over 17 percent. By delegating tasks to the client machine instead of the server and lessening CPU utilization, MMR lessens server load and allows the organization more virtual desktop users for each server.

HOW WE TESTED

Setting up DC1 (infrastructure server)

Installing Windows Server 2008 R2 Enterprise Edition

1. Boot the infrastructure server, and insert the Windows Server 2008 R2 installation DVD in the DVD-ROM drive.
2. At the Language Selection Screen, click Next.
3. Click Install Now.
4. Select Windows Server 2008 Enterprise Edition R2 (Full Installation), and click Next.
5. Click the I accept the license terms check box, and click Next.
6. Click Custom.
7. Click Drive options (advanced).
8. Ensure you select the proper drive, and click New.
9. Click Apply.
10. Click Next.
11. When the installation completes, open Server Manager→Configuration→Local Users and Computers→Users, select Administrator, and right click the Administrator. Set Password to `Password1`
12. Log out, and log in as Administrator.
13. Open Server Manager.
14. Select Change System Properties.
15. In the systems properties dialog box, rename the computer name to `DC1`
16. Reboot the system.
17. Set the password to `Password1`
18. At the Your password has been changed screen, click OK.

Installing system updates in Windows Server 2008 R2

Using the Windows Update feature, we installed the following updates:

- Security Update for Microsoft .NET Framework 3.5.1, Windows 7, and Windows Server 2008 R2 for x64-based Systems (KB2416471)
- Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB2398632)
- Security Update for Windows Server 2008 R2 x64 Edition (KB2347290)
- Security Update for Windows Server 2008 R2 x64 Edition (KB981550)
- Security Update for .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 for x64-based Systems (KB983590)
- Security Update for Windows Server 2008 R2 x64 Edition (KB2160329)
- Security Update for Windows Server 2008 R2 x64 Edition (KB2079403)
- Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB2183461)
- Security Update for Windows Server 2008 R2 x64 Edition (KB978886)
- Security Update for Windows Server 2008 R2 x64 Edition (KB981852)
- Windows Malicious Software Removal Tool x64 - September 2010 (KB890830)
- Update for Windows Server 2008 R2 x64 Edition (KB2158563)

- Security Update for Windows Server 2008 R2 x64 Edition (KB982799)
- Security Update for Windows Server 2008 R2 x64 Edition (KB980436)
- Security Update for Windows Server 2008 R2 x64 Edition (KB982214)
- Security Update for Windows Server 2008 R2 x64 Edition (KB2286198)
- Windows Malicious Software Removal Tool x64 - July 2010 (KB890830)
- Security Update for Windows Server 2008 R2 x64 Edition (KB2032276)
- Rules Update for Active Directory Domain Services Best Practice Analyzer for Windows Server 2008 R2 x64 Editions (KB980360)
- Microsoft .NET Framework 3.5 SP1 Update for Windows 7 and Windows Server 2008 R2 for x64-based Systems (KB982526)
- Security Update for Windows Server 2008 R2 x64 Edition (KB977894)
- Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB980195)
- Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB982381)
- Update for Windows Server 2008 R2 x64 Edition (KB977074)
- Security Update for Windows Server 2008 R2 x64 Edition (KB979309)
- Security Update for Windows Server 2008 R2 x64 Edition (KB972270)
- Security Update for Windows Server 2008 R2 x64 Edition (KB980232)
- Security Update for Windows Server 2008 R2 x64 Edition (KB979683)
- Update for Windows Server 2008 R2 x64 Edition (KB976662)
- Windows Malicious Software Removal Tool x64 - June 2010 (KB890830)
- Security Update for Windows Server 2008 R2 x64 Edition (KB974571)
- Security Update for Windows Server 2008 R2 x64 Edition (KB979482)
- Security Update for Windows Server 2008 R2 x64 Edition (KB979559)
- Update for Best Practices Analyzer for Application Server for Windows Server 2008 R2 x64 Edition (KB981392)
- Update for Best Practices Analyzer for File Services for Windows Server 2008 R2 x64 Edition (KB981111)
- Security Update for Windows Server 2008 R2 x64 Edition (KB975560)
- Microsoft .NET Framework 3.5 SP1 Security Update for Windows 7 and Windows Server 2008 R2 for x64-based Systems (KB979916)
- Update for Best Practices Analyzer for HYPER-V for Windows Server 2008 R2 x64 Edition (KB977238)
- Security Update for Windows Server 2008 R2 x64 Edition (KB971468)
- Microsoft .NET Framework 3.5 SP1 Update for Windows 7 and Windows Server 2008 R2 for x64-based Systems (KB982526)
- Update for Windows Server 2008 R2 x64 Edition (KB981793)
- Update for Best Practices Analyzer for DHCP Server for Windows Server 2008 R2 x64 Edition (KB977236)
- Security Update for Windows Server 2008 R2 x64 Edition (KB980218)
- Update for Windows Server 2008 R2 x64 Edition (KB982519)
- Update for Best Practices Analyzer for Network Policy and Access Services for Windows Server 2008 R2 x64 Edition (NPAS) (KB977239)

- Update for Windows Server 2008 R2 x64 Edition (KB974431)
- Update for Windows Server 2008 R2 x64 Edition (KB980846)
- Security Update for Windows Server 2008 R2 x64 Edition (KB978542)
- Update for Windows Server 2008 R2 x64 Edition (KB978637)
- Security Update for Windows Server 2008 R2 x64 Edition (KB978601)
- Update for Best Practices Analyzer for Windows Server Update Services for Windows Server 2008 R2 x64 Edition (KB981390)
- Update for Rights Management Services Client for Windows Server 2008 R2 x64 Edition (KB979099)
- Update for Best Practices Analyzer for Active Directory Rights Management Services for Windows Server 2008 R2 x64 Edition (KB981391)
- Security Update for Windows Server 2008 R2 x64 Edition (KB981332)
- Update for Windows Server 2008 R2 x64 Edition (KB980408)
- Update for Internet Explorer 8 Compatibility View List for Windows Server 2008 R2 x64 Edition (KB982632)
- Security Update for Windows Server 2008 R2 x64 Edition (KB975467)

Setting up network configuration on DC1

1. Click Start→Run, and type `ncpa.cpl`
2. Right-click the active adaptor, and click Properties.
3. Select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. At the Internet Protocol Version 4 (TCP/IPv4) Properties screen, select the Use the following IP address radio button.
5. Type `192.168.1.220` for the default subnet mask, and `255.255.254.0` and `192.168.1.220` for the gateway.
6. Click OK, and click Close to exit.

Installing Active Directory and DNS services on DC1

To install Active Directory, complete the following steps:

1. Click Start→Run, type `dcpromo` and click OK.
2. At the Active Directory Domain Services Installation Wizard welcome screen, check the Use advanced mode installation option, and click Next.
3. In the Choose a Deployment Configuration dialog box, select Create a new domain in a new forest, and click Next.
4. At the FQDN page, type `login-vsi.com` and click Next.
5. At the NetBIOS name prompt, leave the name LOGIN-VSI, and click Next.
6. At the Forest Functionality level, select Windows Server 2008 R2, click Next.
7. At the additional Domain Controller Options, leave DNS server selected, and click Next.
8. At the System Folder Location screen, leave the default options, and click Next.
9. Assign a Directory Services Restore Mode Administrator account password, and click Next.
10. At the Summary screen, review your selections, and click Next.
11. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.

Setting up DHCP services on DC1

1. Click Start→Administrative Tools→Server Manager→Add Roles.

2. Select DHCP Server, and click Next.
3. At the Introduction to DHCP Server screen, click Next.
4. At the Specify IPv4 DNS Settings screen, type `loginvsi.com` for the parent domain.
5. Set the preferred DNS server IPv4 address to `192.168.1.220` and click Next.
6. At the Specify IPv4 WINS Server Settings screen, select WINS is not required for applications on the network, and click Next.
7. At the Add or Edit DHCP Scopes screen, click Add.
8. At the Add Scope screen, enter the Name DHCP Scope name.
9. In the next box, set the following values, and click OK.
   - Starting IP Address: `192.168.0.1`
   - Ending IP Address: `192.168.1.199`
   - Subnet mask: `255.255.254.0`
10. Check the Activate This Scope box.
11. At the Add or Edit DHCP Scopes screen, click Next.
12. Click the Enable DHCP v6 Stateless Mode radio button, and click Next.
13. Leave the default IPv6 DNS Settings, and click Next.
14. At the Authorize DHCP server dialog box, select Use current credentials.
15. At the Confirm Installation Selections screen, click Next. If the installation is set up correctly, a screen displays that DHCP Server Install Succeeded.
16. Click Close.

Setting up RDS-V (server under test)

Installing Windows Server 2008 R2 Enterprise Edition

1. Boot the server under test, and insert the Windows Server 2008 R2 installation DVD in the DVD-ROM drive.
2. At the Language Selection Screen, click Next.
3. Click Install Now.
4. Select Windows Server 2008 Enterprise Edition R2 (Full Installation), and click Next.
5. Click the I accept the license terms check box, and click Next.
6. Click Custom.
7. Click Drive options (advanced).
8. Ensure you select the proper drive, and click New.
9. Click Apply.
10. Click Next.
11. When the installation completes, open the Server Manager→Configuration→Local Users and Computers→Users, select Administrator, and right click. Set Password to `Password1`
12. Log out, and log in as Administrator.
13. Open Server Manager.
14. Select Change System Properties.
15. In the Systems Properties dialog box, rename the computer name to `RDS-V`
16. Reboot the system.
17. Set the password to `Password1`
18. At the Your password has been changed screen, click OK.

Installing system updates in Windows Server 2008 R2

Using the Windows Update feature, we installed the same update we list above.

Setting up network configuration on RDS-V

1. Click Start→Run, and type `ncpa.cpl`
2. Right click on the active adaptor, and click Properties.
3. Select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. At the Internet Protocol Version 4 (TCP/IPv4) Properties screen, select the Use the following IP address radio button.
5. Type `192.168.1.220` for the default subnet mask, and `255.255.254.0` and `192.168.1.220` for the gateway. Type `192.168.1.220` for DNS server
6. Click OK, and click Close to exit.

Enabling the Hyper-V role on RDS-V

1. Click Start→Administrative Tools→Server Manager.
2. Click Roles.
3. Click Add Roles.
4. Click Next.
5. Select the Hyper-V role by checking the box beside it, and click Next.
6. Check the box beside the Ethernet Card you wish to use for client/server traffic, and click Next.
7. Click Install to begin the Hyper-V installation.
8. When the installation finishes, click Close.
9. When the installer prompts you to restart now, click Yes.
10. Follow the prompt to log onto the system.
11. Enter the password, and click the arrow to continue. The Resuming Configuration Wizard should start automatically.
12. Once the Resuming Configuration Wizard completes, the installation results appear with a message that the installation succeeded.
13. Click Close.

Configuring virtual networks

1. Open Hyper-V Manager.
2. From the Actions menu, click Virtual Network Manager.
3. Under Create virtual network, select External network. Use one physical NIC that is connected to the private 192.168.0.x network. Click Add, and the New Virtual Network page appears.
4. Type `VSI-net` for the name of the new network. Review the other properties and modify them if necessary.
5. Click OK to create the virtual network and close Virtual Network Manager, or click Apply to create the virtual network and continue using Virtual Network Manager.

Adding a network adapter to a virtual machine

1. Open Hyper-V Manager, and Click Start→Administrative Tools→Hyper-V Manager.
2. In the Results pane, under Virtual Machines, select the virtual machine that you want to configure.
3. In the Action pane, under the virtual machine name, click Settings.
4. In the Navigation pane, click Add Hardware.

5. On the Add Hardware page, choose a network adapter or a legacy network adapter. Note: You can only add network adapters to a virtual machine when the machine is off.
6. Click Add. The Network Adapter or Legacy Network Adapter page appears.
7. Under Network, select the virtual network you want to connect to.
8. If you want to configure a static MAC address or virtual LAN identifier, specify the address or identifier you want to use.
9. Click OK.

Installing the Windows 7 Enterprise (32 bit) virtual machine

1. Open Hyper-V Manager.
2. Right-click RDS-V, and select New Virtual Machine.
3. Name the virtual machine `WIN7EE1`
4. Assign Memory to 1024 MB, and click Next.
5. Configure networking change connection to local area connection – Virtual network.
6. Click Create virtual hard disk.
7. Set size to 14 GB, and click Next.
8. From Install options, select Install media.
9. Click Finish.
10. Start your VM with media ready.
11. When the installation prompts you, press any key to begin setup.
12. Enter your language preferences, and click Next.
13. Click Install.
14. Accept the license terms, and click Next.
15. Select Custom, and select the drive that will contain the OS.
16. Click Install. Setup begins.
17. Enter `WIN7EE1` for the username, enter `WIN7EE1-PC` for computer, and click Next.
18. Enter no password, and click Next.
19. For system protection, select Use recommended settings, and click Next.
20. Enter your time zone, and click Next.
21. Select the Work Network setting, and click Next.
22. Use Windows Update to patch the Windows 7 installation.

Installing system updates in Windows 7 Enterprise

Using the Windows Update feature, we installed the following updates:

- Security Update for Windows 7 (KB978886)
- Security Update for .NET Framework 3.5.1 on Windows 7 x86 (KB983590)
- Update for Windows 7 (KB975496)
- Security Update for Windows 7 (KB975467)
- Security Update for Windows 7 (KB978601)
- Security Update for Windows 7 (KB2347290)
- Update for Windows 7 (KB974332)
- Microsoft .NET Framework 3.5 SP1 Update for Windows 7 x86 (KB982526)
- Security Update for Windows 7 (KB982665)
- Update for Windows 7 (KB977074)

- Update for Windows 7 (KB2158563)
- Cumulative Security Update for ActiveX Killbits for Windows 7 (KB980195)
- Security Update for Windows 7 (KB974571)
- Update for Windows 7 (KB980408)
- Security Update for Windows 7 (KB982799)
- Security Update for Windows 7 (KB978542)
- Security Update for Windows 7 (KB2079403)
- Definition Update for Windows Defender - KB915597 (Definition 1.91.1370.0)
- Update for Windows 7 (KB980846)
- Update for Windows 7 (KB2272691)
- Update for Windows 7 (KB974431)
- Security Update for Windows 7 (KB979482)
- Security Update for Windows 7 (KB982214)
- Cumulative Update for Media Center for Windows 7 (KB981078)
- Update for Windows 7 (KB976662)
- Security Update for Windows 7 (KB972270)
- Security Update for Windows 7 (KB977165)
- Security Update for Windows 7 (KB975560)
- Security Update for Windows 7 (KB981852)
- Cumulative Security Update for Internet Explorer 8 for Windows 7 (KB2183461)
- Security Update for Windows 7 (KB2286198)
- Windows Malicious Software Removal Tool - September 2010 (KB890830)
- Security Update for Windows 7 (KB981332)
- Update for Rights Management Services Client for Windows 7 (KB979099)
- Security Update for Windows 7 (KB979309)
- Update for Windows 7 (KB979538)
- Security Update for Windows 7 (KB980436)
- Security Update for Windows 7 (KB980232)
- Security Update for Windows 7 (KB2160329)
- Update for Internet Explorer 8 Compatibility View List for Windows 7 (KB2362765)
- Microsoft .NET Framework 3.5 SP1 Security Update for Windows 7 x86 (KB979916)
- Security Update for Windows 7 (KB980218)

Windows 7 guest: Turning on Remote desktop access

1. Click Start, right-click Computer, click Properties→Advanced system settings→Remote tab, and select Allow connections from any version of Remote Desktop. Click Apply.

Windows 7 guest: Turning off system restore

1. Click Start, right-click Computer, click Properties→Advanced system settings→System Protection→Configure →Turn off system protection, and click OK.

Windows 7 guest: Adjusting page file

1. Click Start, Right-click Computer, and click Properties→Advanced system settings→Advanced→Performance: Settings.

2. In Performance Settings, select the Advanced tab, and select Change for Virtual Memory.
3. De-select Automatically manage paging file size for all drives.
4. Select Custom size and for both values, enter `2048`, and select Set.

Windows 7 guest: Joining the login-vsi domain

1. Click Start, right-click Computer, and click Properties→Advanced system settings→Computer Name tab.
2. Select Change.
3. Select Domain under Member of.
4. Enter the domain name as `login-vsi.com` and click OK.
5. Enter the domain administrator account and password for the login-vsi domain.
6. Reboot the system.

Windows 7 guest: Installing the virtual audio cables driver

1. Navigate to http://software.muzychenko.net/eng/vac.htm#download, and download the audio cables driver.
2. Run setup.exe
3. Accept the licensing agreement.
4. Install to the default directory.

Windows 7 guest: Installing Office 2007 Professional

1. From the Office 2007 media, run Setup.
2. Enter the product key for Office 2007, and click Continue.
3. Accept the licensing agreement.
4. Select Custom Install.
5. Al the root of the install options, ensure that all Office components are set to Run from My Computer.
6. Click Install.
7. Download and run the Office 2007 Service Pack 2.
8. Reboot the system.

Setting up Login VSI components

Setting up Active Directory for Login VSI

1. Log into DC1, browse the Login VSI media folder open the AD Setup/AD Setup.exe file.
2. Run the Login VSI setup on DC1.
3. Set your amount of users to 250.
4. Set your username to `Login_VSI`
5. For your password, enter the password you set up earlier, `Password1`
6. Click Start. A command prompt appears and you see the setup creating users.
7. Once the script finishes, the command prompt displays AD preparation is completed. Click OK, and click Exit.
8. Click Start→`dsa.msc` to open Active Directory users and computers.
9. Expand loginvsi.com.
10. Expand Login_VSI.
11. Select Users to make sure that 250 are in place.
12. Right-click Login_VSI.
13. Select New, and select Group.

14. Set group name to `loginvsigroup`, select Global for Group Scope, and leave Group Type as Security. Click OK.
15. Select all the users, and right-click and select Add to group. Type `loginvsigroup` for the name of the group, and check Name. Click OK, and the users will have joined the group.
16. Click Start and type `GPMC.msc` to open Group Policy Manager.
17. Edit the VSI System Group Policy object: Click User Configuration→Policy→Administrative Templates→Windows Components→Desktop Windows Manager→Edit. Do not allow desktop composition, select Enabled, and click OK.
18. Close Group Policy editor.

Setting up file shares

1. On DC1, navigate to C:, click New Folder, and name it `VSI-Share`
2. Right-click the new folder, and select Properties.
3. Click Sharing→Advanced sharing, and check Share this folder.
4. Open Permissions.
5. Check Allow Full Control, click Apply, and click OK.
6. At the Advanced Sharing screen, click Apply, and click OK.

Setting up the target

1. On the Windows 7 guest WIN7EE1-PC, log in as Administrator.
2. Click Start, right-click Computer, and click Manage.
3. Open User Manager by clicking Local users and Groups→Groups→right-click Administrators, click Add to Group…
4. Select Add…
5. Type `loginvsigroup` in the Enter the object names to select text box. Click OK to close.
6. In the User Accounts wizard, add the loginvsigroup from the login-vsi domain.
7. Launch the /Target setup/setup.exe
8. Specify the vsi share (//dc1/vsi-share), and select Start.
9. Before the setup is complete, the setup prompts you to move the computer account to the Login_VSI\Computers OU and reboot. Do not reboot until this is done
10. Log into DC1, and click Start→Administrative Tools→Active Directory Users and Computers.
11. Browse to Active Directory Users and Computers→Login-vsi.com→Computers, and move the WIN7EE1-PC account to the OU located at Active Directory Users and Computers.
12. Go to the Windows 7 guest, and reboot the system to complete the Login VSI target setup.
13. When the setup is complete, run services.msc and change Windows Search from Disabled to Automatic (Delayed Start).
14. You are ready to use the Windows 7 image with Login VSI. To make multiple sessions, use Windows AIK and sysprep to create 90 VMs. For more information on how to use sysprep on Windows 7, see http://technet.microsoft.com/en-us/library/cc766514(WS.10).aspx.
15. Ensure that are all 90 virtual desktops are members of the login-vsi domain, and are moved to the login_vsi\computers OU (see Steps 10 and 11 above).
16. Reboot the 90 virtual desktops to ensure that the GPO linked to the OU are effective

Setting up Login VSI launchers

1. Install the VSI media\launcher\setup software on all physical desktop launchers.

2. For more information on how to use more than one Launcher in a master/slave relationship, refer to Page 37 in the Login VSI 2.3 Admin Guide.

Setting up the .rdp file for each RDS session

For each of the 90 Windows 7 sessions to be launched, we configured a .rdp file. See http://technet.microsoft.com/en-us/library/ff393699(WS.10).aspx for more details. To enable MMR, we used a rdp file with the following values:

- screen mode id:i:2
- use multimon:i:1
- desktopwidth:i:1920
- desktopheight:i:1200
- session bpp:i:32
- winposstr:s:0,1,1956,24,3817,1184
- compression:i:1
- keyboardhook:i:2
- audiocapturemode:i:1
- videoplaybackmode:i:1
- connection type:i:6
- displayconnectionbar:i:1
- disable wallpaper:i:0
- allow font smoothing:i:1
- allow desktop composition:i:1
- disable full window drag:i:0
- disable menu anims:i:0
- disable themes:i:0
- disable cursor setting:i:0
- bitmapcachepersistenable:i:1
- audiomode:i:0
- redirectprinters:i:1
- redirectcomports:i:0
- redirectsmartcards:i:1
- redirectclipboard:i:1
- redirectposdevices:i:0
- redirectdirectx:i:1
- autoreconnection enabled:i:1
- authentication level:i:2
- prompt for credentials:i:0
- negotiate security layer:i:1
- remoteapplicationmode:i:0
- alternate shell:s:
- shell working directory:s:

- gatewayhostname:s:
- gatewayusagemethod:i:4
- gatewaycredentialssource:i:4
- gatewayprofileusagemethod:i:0
- promptcredentialonce:i:1
- use redirection server name:i:0
- drivestoredirect:s:
- username:s:Login_VSI1
- full address:s:MS1-PC

To disable MMR, we changed the following items in each of the .rdp files:

- audiomode:i:1
- videoplaybackmode:i:0

APPENDIX A – SERVER CONFIGURATION INFORMATION

Figure 6 provides detailed configuration information about the test server.

System	Intel® Server Board S5520URT
Power supplies	
Total number	2
Vendor and model number	Delta Electronics –DPS-750PB
Wattage of each (W)	750
Cooling fans	
Total number	3
First type of cooling fan	
Number	2
Vendor and model number	Delta Electronics TFB0812UH3
Dimensions (h x w) of each	3-1/8” x 1-1/2”
Volts	12
Amps	2.34
Second type of cooling fan	
Number	1
Vendor and model number	Delta Electronics PFC0612DE
Dimensions (h x w) of each	2-3/8” x 1-1/2”
Volts	12
Amps	1.68
General	
Number of processor packages	2
Number of cores per processor	4
Number of hardware threads per core	2
System power management policy	Balanced
CPU	
Vendor	Intel
Name	Xeon®
Model number	X5570
Stepping	D0
Socket type	Socket LGA1366
Core frequency (GHz)	2.93
Bus frequency	6.4 GT/s
L1 cache	32 KB + 32 KB (per core)
L2 cache	256 KB (per core)
L3 cache	8 MB (shared)
Platform	
Vendor and model number	Intel Server Board S5520URT
Motherboard model number	S5520URT

System	**Intel® Server Board S5520URT**
Motherboard chipset	Intel 5520
BIOS name and version	S5500.86B.01.00.050 (05/06/2010)
BIOS settings	Default
Memory module(s)	
Total RAM in system (GB)	24
Vendor and model number	Micron MT36JSZ51272PY
Type	PC3-10600R
Speed (MHz)	1,333
Speed running in the system (MHz)	1,333
Timing/latency (tCL-tRCD-tRP-tRASmin)	9-9-9-24
Size (GB)	4
Number of RAM module(s)	6 x 4 GB
Chip organization	Double-sided
Rank	Dual
Hard disk	
Vendor and model number	Intel SSDDSA2M160G2GN
Number of disks in system	1
Size (GB)	160
Buffer size (MB)	N/A
RPM	N/A
Type	SATA II
Disk controller	
Vendor and model	Integrated Serial ATA-300
Controller cache	N/A
Controller driver	Intel 8.3.0.1011 (02/05/2007)
Controller firmware	1.2.5
RAID configuration	RAID 0
Operating system	
Name	Windows Server 2008 R2, Enterprise Edition
Build number	7600
Service pack	Service Pack 1
File system	NTFS
Kernel	ACPI x64-based PC
Language	English
Graphics	
Vendor and model number	Intel Server Engine LLC Pilot II Controller
Graphics memory	64 MB DDR2 SDRAM
Driver	Microsoft Standard VGA 6.1.7600.16385 (6/21/2006)

System	**Intel® Server Board S5520URT**
Ethernet	
Vendor and model number	Intel 82575EB Gigabit Ethernet
Type	Integrated
Driver	Intel 11.0.5.22 (04/6/2009)
Optical drive(s)	
Vendor and model number	TSSTcorp TS-L633A UO01
Type	DVD-RW
USB ports	
Number	6
Type	2.0

Figure 6: Test server configuration details.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Disclaimer of Warranties; Limitation of Liability:
PRINCIPLED TECHNOLOGIES, INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, PRINCIPLED TECHNOLOGIES, INC. SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT PRINCIPLED TECHNOLOGIES, INC., ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC. BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC.'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH PRINCIPLED TECHNOLOGIES, INC.'S TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.