EMC® INFRASTRUCTURE FOR CITRIX XENDESKTOP 5.5

EMC VNX™ Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, XenApp 6.5, and XenServer 6

- Simplify management and decrease TCO
- Streamline Application Delivery
- Minimize the risk of virtual desktop deployment

EMC Solutions Group

Abstract

This Proven Solution Guide summarizes test validations of an EMC infrastructure for virtual desktops enabled by Cisco UCS, Citrix XenDesktop 5.5, XenApp 6.5, and XenServer 6 with an EMC VNX5300™ unified storage platform. It focuses on sizing and scalability, and highlights new features introduced in EMC VNX, Citrix XenDesktop, XenApp, and XenServer. EMC FAST Cache technology supports service-level agreements by optimizing performance of the virtual desktop environment.

January 2012
Copyright © 2012 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

Part Number: H8304.1
# Table of contents

## 1 Introduction ............................................................................................................. 9

- Introduction to the new EMC VNX Series ................................................................. 9
  - Software suites available ....................................................................................... 10
  - Software packs available ..................................................................................... 10
- Document overview ................................................................................................ 10
  - Use case definition ............................................................................................... 10
  - Purpose ................................................................................................................. 11
  - Scope .................................................................................................................... 11
  - Not in scope .......................................................................................................... 11
  - Audience .............................................................................................................. 11
  - Prerequisites ....................................................................................................... 11
  - Terminology ........................................................................................................ 12
- Reference architecture ............................................................................................. 12
  - Corresponding reference architecture ................................................................ 12
  - Reference architecture diagram ......................................................................... 13
- Configuration ........................................................................................................... 14
  - Test results .......................................................................................................... 14
  - Hardware resources ............................................................................................. 14
  - Software resources .............................................................................................. 15

## 2 Citrix Virtual Desktop Infrastructure ..................................................................... 16

- Citrix XenDesktop 5.5 .............................................................................................. 16
  - Introduction ......................................................................................................... 16
  - Deploying Citrix XenDesktop components .......................................................... 16
  - Citrix XenDesktop controller ............................................................................. 17
  - Machine Creation Services ................................................................................ 17
- Citrix XenApp 6.5 .................................................................................................... 17
  - XenApp overview ............................................................................................... 17
  - Deploying Citrix XenApp .................................................................................... 18
- Citrix XenServer 6 infrastructure ......................................................................... 18
  - XenServer 6 overview ....................................................................................... 18
  - XenServer resource pool ................................................................................... 18
- Windows infrastructure .......................................................................................... 19
  - Introduction ........................................................................................................ 19
  - Microsoft Active Directory .............................................................................. 19
  - Microsoft SQL Server ......................................................................................... 19
  - DNS Server ........................................................................................................ 19
3 Storage Design

EMC VNX series storage architecture ................................................................. 21
   Introduction ........................................................................................................ 21
   Storage layout ..................................................................................................... 22
   Storage layout overview ................................................................................... 22
   File system layout ............................................................................................. 23
   EMC VNX FAST Cache ...................................................................................... 24
   XenServer storage layout .................................................................................. 25
   VNX shared file systems ................................................................................ 25
   Roaming profiles and folder redirection .......................................................... 25
   EMC VNX for File Home Directory feature .................................................... 25
   Profile export ..................................................................................................... 26
   Capacity ............................................................................................................... 26

4 Network Design................................................................................................. 27

   Considerations ..................................................................................................... 27
   Network layout overview ................................................................................ 27
   Logical design considerations ......................................................................... 28
   Link aggregation ................................................................................................ 28
   VNX for file network configuration ................................................................. 29
   Data Mover ports ............................................................................................... 29
   LACP configuration on the Data Mover .......................................................... 29
   Data Mover interfaces ...................................................................................... 29
   Enable jumbo frames on Data Mover interface ............................................. 30
   XenServer network configuration .................................................................... 31
   NIC bonding ........................................................................................................ 31
   Cisco Nexus 5020 configuration ....................................................................... 33
   Overview ............................................................................................................ 33
   Cabling ............................................................................................................... 33
   Enable jumbo frames on Nexus switch ............................................................ 33
   virtual Port Channel for Data Mover ports .................................................... 33
   Cisco UCS network configuration ................................................................. 35
   Enable jumbo frames for UCS servers ............................................................ 35
### 5 Installation and Configuration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation overview</td>
<td>36</td>
</tr>
<tr>
<td>Citrix XenDesktop components</td>
<td>37</td>
</tr>
<tr>
<td>Citrix XenDesktop installation overview</td>
<td>37</td>
</tr>
<tr>
<td>Citrix XenDesktop machine catalog configuration</td>
<td>37</td>
</tr>
<tr>
<td>Throttle commands to vCenter Server</td>
<td>41</td>
</tr>
<tr>
<td>Virtual desktop idle pool settings</td>
<td>42</td>
</tr>
<tr>
<td>Citrix XenApp components</td>
<td>44</td>
</tr>
<tr>
<td>Pass-through authentication method</td>
<td>44</td>
</tr>
<tr>
<td>Resource type</td>
<td>45</td>
</tr>
<tr>
<td>Application profiling</td>
<td>47</td>
</tr>
<tr>
<td>Publish application</td>
<td>47</td>
</tr>
<tr>
<td>Configuring XenDesktop virtual desktop agent for XenApp</td>
<td>55</td>
</tr>
<tr>
<td>Storage components</td>
<td>59</td>
</tr>
<tr>
<td>Storage pools</td>
<td>59</td>
</tr>
<tr>
<td>NFS active threads per Data Mover</td>
<td>59</td>
</tr>
<tr>
<td>NFS performance fix</td>
<td>59</td>
</tr>
<tr>
<td>Enable FAST Cache</td>
<td>60</td>
</tr>
<tr>
<td>VNX Home Directory feature</td>
<td>61</td>
</tr>
</tbody>
</table>

### 6 Testing and Validation

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validated environment profile</td>
<td>63</td>
</tr>
<tr>
<td>Profile characteristics</td>
<td>63</td>
</tr>
<tr>
<td>Use cases</td>
<td>64</td>
</tr>
<tr>
<td>Login VSI</td>
<td>64</td>
</tr>
<tr>
<td>Login VSI launcher</td>
<td>65</td>
</tr>
<tr>
<td>FAST Cache configuration</td>
<td>65</td>
</tr>
<tr>
<td>Boot storm results</td>
<td>66</td>
</tr>
<tr>
<td>Test methodology</td>
<td>66</td>
</tr>
<tr>
<td>Pool individual disk load</td>
<td>66</td>
</tr>
<tr>
<td>Pool LUN load</td>
<td>67</td>
</tr>
<tr>
<td>Storage processor IOPS</td>
<td>68</td>
</tr>
<tr>
<td>Storage processor utilization</td>
<td>69</td>
</tr>
<tr>
<td>FAST Cache IOPS</td>
<td>70</td>
</tr>
<tr>
<td>Data Mover CPU utilization</td>
<td>71</td>
</tr>
<tr>
<td>Data Mover NFS load</td>
<td>72</td>
</tr>
<tr>
<td>Data Mover NFS response time</td>
<td>73</td>
</tr>
<tr>
<td>XenServer CPU load</td>
<td>74</td>
</tr>
<tr>
<td>Antivirus results</td>
<td>75</td>
</tr>
<tr>
<td>Test methodology</td>
<td>75</td>
</tr>
</tbody>
</table>
Pool individual disk load .............................................................. 75
Pool LUN load ........................................................................... 76
Storage processor IOPS ............................................................... 77
Storage processor utilization ....................................................... 77
FAST Cache IOPS ..................................................................... 78
Data Mover CPU utilization ....................................................... 79
Data Mover NFS load ................................................................. 79
Data Mover NFS response time .................................................. 80
XenServer CPU load ................................................................. 81

Patch install results .................................................................. 82
Test methodology ..................................................................... 82
Pool individual disk load .......................................................... 82
Pool LUN load .......................................................................... 83
Storage processor IOPS ............................................................. 84
Storage processor utilization ..................................................... 85
FAST Cache IOPS ..................................................................... 86
Data Mover CPU utilization ..................................................... 87
Data Mover NFS load ............................................................... 87
Data Mover NFS response time ................................................ 88
XenServer CPU load ............................................................... 89

Login VSI results ...................................................................... 90
Test methodology ..................................................................... 90
Login VSI result summary ........................................................ 90
Login storm timing ................................................................. 92
Pool individual disk load .......................................................... 93
Pool LUN load .......................................................................... 94
Storage processor IOPS ............................................................ 95
Storage processor utilization .................................................... 95
FAST Cache IOPS ................................................................... 96
Data Mover CPU utilization .................................................... 97
Data Mover NFS load .............................................................. 97
Data Mover NFS response time ............................................... 98
XenServer CPU load .............................................................. 99

FAST Cache benefits ................................................................. 100
Case study ................................................................................ 100

7 Conclusion ............................................................................. 102
Summary .................................................................................. 102
References ................................................................................ 102
White papers ............................................................................ 102
List of Tables

Table 1. Terminology ........................................................................................................... 12  
Table 2. Solution hardware ............................................................................................... 14  
Table 3. Solution software ................................................................................................. 15  
Table 4. File systems .......................................................................................................... 25  
Table 5. Environment profile ............................................................................................ 63  

List of Figures

Figure 1. Referencere architecture ...................................................................................... 13  
Figure 2. Storage layout ...................................................................................................... 22  
Figure 3. NFS file system layout ......................................................................................... 23  
Figure 4. CIFS file system layout ....................................................................................... 24  
Figure 5. UNC path for roaming profiles .......................................................................... 26  
Figure 6. 10 gigabit connectivity ....................................................................................... 27  
Figure 7. Rear view of the two VNX5300 Data Movers ...................................................... 29  
Figure 8. NIC bonding configuration .................................................................................. 31  
Figure 9. NIC bond mode .................................................................................................. 32  
Figure 10. UCS Manager - MTU configuration ................................................................ 35  
Figure 11. Select Create Catalog ....................................................................................... 37  
Figure 12. Select the Machine type .................................................................................... 38  
Figure 13. Select the cluster host and Master Image ........................................................... 38  
Figure 14. Specify the number of virtual machines ............................................................ 39  
Figure 15. Select an Active Directory location .................................................................. 40  
Figure 16. Review the summary ........................................................................................ 40  
Figure 17. Select Hosts ....................................................................................................... 41  
Figure 18. Select Change details ....................................................................................... 41  
Figure 19. Change Host Details dialog box ....................................................................... 42  
Figure 20. Advanced Host Details dialog box .................................................................... 42  
Figure 21. Select Authentication Methods ......................................................................... 44  
Figure 22. Configure Authentication Methods - PNAgent dialog box ................................. 45  
Figure 23. Properties - PNAgent dialog box ..................................................................... 45  
Figure 24. Select Resource Types ..................................................................................... 46  
Figure 25. Manage Resource Types – PNAgent dialog box .............................................. 46  
Figure 26. Save As window ............................................................................................... 47  
Figure 27. Select Publish application .................................................................................. 48  
Figure 28. Publish Application - Name page ...................................................................... 48  
Figure 29. Publish Application - Type page ....................................................................... 49  
Figure 30. Publish Application - Location page .................................................................. 50  
Figure 31. Publish Application – Offline access page ........................................................ 51  
Figure 32. Publish Application - Users page ...................................................................... 52  
Figure 33. Publish Application – Shortcut presentation page ............................................ 53  
Figure 34. Publish Application – Publish immediately page ............................................. 54  
Figure 35. Publish Application – Content redirection page .............................................. 55  
Figure 36. Install Virtual Desktop Agent ........................................................................... 56
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 37</td>
<td>Advanced Install</td>
<td>56</td>
</tr>
<tr>
<td>Figure 38</td>
<td>Select Components to Install page</td>
<td>57</td>
</tr>
<tr>
<td>Figure 39</td>
<td>Controller Location page</td>
<td>57</td>
</tr>
<tr>
<td>Figure 40</td>
<td>Virtual Desktop Configuration page</td>
<td>58</td>
</tr>
<tr>
<td>Figure 41</td>
<td>Summary page</td>
<td>58</td>
</tr>
<tr>
<td>Figure 42</td>
<td>Thirty 200 GB thick LUNs</td>
<td>59</td>
</tr>
<tr>
<td>Figure 43</td>
<td>FAST Cache tab</td>
<td>60</td>
</tr>
<tr>
<td>Figure 44</td>
<td>Enable FAST Cache</td>
<td>61</td>
</tr>
<tr>
<td>Figure 45</td>
<td>MMC snap-in</td>
<td>61</td>
</tr>
<tr>
<td>Figure 46</td>
<td>Sample virtual desktop properties</td>
<td>62</td>
</tr>
<tr>
<td>Figure 47</td>
<td>Boot storm - Disk IOPS for a single SAS drive</td>
<td>66</td>
</tr>
<tr>
<td>Figure 48</td>
<td>Boot storm - LUN IOPS and response time</td>
<td>67</td>
</tr>
<tr>
<td>Figure 49</td>
<td>Boot storm - Storage processor total IOPS</td>
<td>68</td>
</tr>
<tr>
<td>Figure 50</td>
<td>Boot storm - Storage processor utilization</td>
<td>69</td>
</tr>
<tr>
<td>Figure 51</td>
<td>Boot storm - FAST Cache IOPS</td>
<td>70</td>
</tr>
<tr>
<td>Figure 52</td>
<td>Boot storm – Data Mover CPU utilization</td>
<td>71</td>
</tr>
<tr>
<td>Figure 53</td>
<td>Boot storm – Data Mover NFS load</td>
<td>72</td>
</tr>
<tr>
<td>Figure 54</td>
<td>Boot storm – Data Mover NFS read/write response time</td>
<td>73</td>
</tr>
<tr>
<td>Figure 55</td>
<td>Boot storm - XenServer CPU load</td>
<td>74</td>
</tr>
<tr>
<td>Figure 56</td>
<td>Antivirus - Disk I/O for a single SAS drive</td>
<td>75</td>
</tr>
<tr>
<td>Figure 57</td>
<td>Antivirus - LUN IOPS and response time</td>
<td>76</td>
</tr>
<tr>
<td>Figure 58</td>
<td>Antivirus - Storage processor IOPS</td>
<td>77</td>
</tr>
<tr>
<td>Figure 59</td>
<td>Antivirus - Storage processor utilization</td>
<td>77</td>
</tr>
<tr>
<td>Figure 60</td>
<td>Antivirus - FAST Cache IOPS</td>
<td>78</td>
</tr>
<tr>
<td>Figure 61</td>
<td>Antivirus – Data Mover CPU utilization</td>
<td>79</td>
</tr>
<tr>
<td>Figure 62</td>
<td>Antivirus – Data Mover NFS load</td>
<td>80</td>
</tr>
<tr>
<td>Figure 63</td>
<td>Antivirus - Data Mover NFS read/write response time</td>
<td>80</td>
</tr>
<tr>
<td>Figure 64</td>
<td>Antivirus - XenServer CPU load</td>
<td>81</td>
</tr>
<tr>
<td>Figure 65</td>
<td>Patch install - Disk IOPS for a single SAS drive</td>
<td>82</td>
</tr>
<tr>
<td>Figure 66</td>
<td>Patch install - LUN IOPS and response time</td>
<td>83</td>
</tr>
<tr>
<td>Figure 67</td>
<td>Patch install - Storage processor IOPS</td>
<td>84</td>
</tr>
<tr>
<td>Figure 68</td>
<td>Patch install - Storage processor utilization</td>
<td>85</td>
</tr>
<tr>
<td>Figure 69</td>
<td>Patch install - FAST Cache IOPS</td>
<td>86</td>
</tr>
<tr>
<td>Figure 70</td>
<td>Patch install – Data Mover CPU utilization</td>
<td>87</td>
</tr>
<tr>
<td>Figure 71</td>
<td>Patch install – Data Mover NFS load</td>
<td>87</td>
</tr>
<tr>
<td>Figure 72</td>
<td>Patch install - Data Mover NFS read/write response time</td>
<td>88</td>
</tr>
<tr>
<td>Figure 73</td>
<td>Patch install - XenServer CPU load</td>
<td>89</td>
</tr>
<tr>
<td>Figure 74</td>
<td>Login VSI response times</td>
<td>91</td>
</tr>
<tr>
<td>Figure 75</td>
<td>Login storm timing</td>
<td>92</td>
</tr>
<tr>
<td>Figure 76</td>
<td>Login VSI - Disk IOPS for a single SAS drive</td>
<td>93</td>
</tr>
<tr>
<td>Figure 77</td>
<td>Login VSI - LUN IOPS and response time</td>
<td>94</td>
</tr>
<tr>
<td>Figure 78</td>
<td>Login VSI - Storage processor IOPS</td>
<td>95</td>
</tr>
<tr>
<td>Figure 79</td>
<td>Login VSI - Storage processor utilization</td>
<td>95</td>
</tr>
<tr>
<td>Figure 80</td>
<td>Login VSI - FAST Cache IOPS</td>
<td>96</td>
</tr>
<tr>
<td>Figure 81</td>
<td>Login VSI – Data Mover CPU utilization</td>
<td>97</td>
</tr>
<tr>
<td>Figure 82</td>
<td>Login VSI – Data Mover NFS load</td>
<td>97</td>
</tr>
<tr>
<td>Figure 83</td>
<td>Login VSI - Data Mover NFS read/write response time</td>
<td>98</td>
</tr>
<tr>
<td>Figure 84</td>
<td>Login VSI - XenServer CPU load</td>
<td>99</td>
</tr>
<tr>
<td>Figure 85</td>
<td>Antivirus scan – scan time comparison</td>
<td>100</td>
</tr>
<tr>
<td>Figure 86</td>
<td>Patch storm – NFS write latency comparison</td>
<td>101</td>
</tr>
</tbody>
</table>
Introduction

This chapter introduces the EMC® infrastructure for Citrix XenDesktop 5.5 solution and its components, and includes the following sections:

- Introduction to the new EMC VNX™ Series
- Document overview
- Reference architecture
- Configuration

Introduction to the new EMC VNX Series

VNX series delivers uncompromising scalability and flexibility for the midtier while providing market-leading simplicity and efficiency to minimize total cost of ownership. Customers can benefit from the new VNX features such as:

- Next-generation unified storage, optimized for virtualized applications
- Extended cache using Flash drives with FAST Cache and Fully Automated Storage Tiering for Virtual Pools (FAST VP) that can be optimized for the highest system performance and lowest storage cost simultaneously on both block and file
- Multiprotocol support for file, block, and object with object access through Atmos™ Virtual Edition (Atmos VE)
- Simplified management with EMC Unisphere™ for a single management interface for all NAS, SAN, and replication needs
- Up to three times improvement in performance with the latest Intel Xeon multicore processor technology, optimized for Flash
- 6 gigabit/s SAS back end with the latest drive technologies supported:
  - 3.5” 100 GB and 200 GB Flash, 3.5” 300 GB, and 600 GB 15k or 10k rpm SAS, and 3.5”, 1 TB, 2 TB, and 3 TB 7.2k rpm NL-SAS
  - 2.5” 100 GB and 200 GB Flash, 300 GB, 600 GB and 900 GB 10k rpm SAS
- Expanded EMC UltraFlex™ I/O connectivity—Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), Common Internet File System (CIFS), Network File System (NFS) including parallel NFS (pNFS), Multi-Path File System (MPFS), and Fibre Channel over Ethernet (FCoE) connectivity for converged networking over Ethernet

The VNX series includes five new software suites and three new software packs, making it easier and simpler to attain the maximum overall benefits.
Chapter 1: Introduction

Software suites available

- VNX FAST Suite—Automatically optimizes for the highest system performance and the lowest storage cost simultaneously (FAST VP is not part of the FAST Suite for the VNX5100).
- VNX Local Protection Suite—Practices safe data protection and repurposing.
- VNX Remote Protection Suite—Protects data against localized failures, outages and disasters.
- VNX Application Protection Suite—Automates application copies and proves compliance.
- VNX Security and Compliance Suite—Keeps data safe from changes, deletions, and malicious activity.

Software packs available

- VNX Total Efficiency Pack—Includes all five software suites (not available for the VNX5100).
- VNX Total Protection Pack—Includes local, remote and application protection suites
- VNX Total Value Pack—Includes all three protection software suites and the Security and Compliance Suite (the VNX5100 exclusively supports this package).

Document overview

EMC’s commitment to consistently maintain and improve quality is led by the Total Customer Experience (TCE) program, which is driven by Six Sigma methodologies. As a result, EMC has built Customer Integration Labs in its Global Solutions Centers to reflect realworld deployments in which TCE use cases are developed and executed. These use cases provide EMC with an insight into the challenges that are currently facing its customers.

This Proven Solution Guide summarizes a series of best practices that were discovered or validated during testing of the EMC Infrastructure for Citrix XenDesktop 5.5 solution by using the following products:

- EMC VNX series
- Cisco UCS B-series
- Citrix XenDesktop 5.5
- Citrix XenApp 6.5
- Citrix XenServer 6

Use case definition

The following use cases are examined in this solution:

- Boot storm
- Antivirus scan
Chapter 1: Introduction

- Microsoft security patch install
- Login storm
- User workload simulated with Login VSI tool

Chapter 6: Testing and Validation contains the test definitions and results for each use case.

Purpose

The purpose of this solution is to provide a virtualized infrastructure for virtual desktops powered by Citrix XenDesktop 5.5, XenApp 6.5, XenServer 6, Cisco UCS B-series servers, EMC VNX series (NFS), VNX FAST Cache, and storage pools.

This solution includes all the attributes required to run this environment, such as hardware and software, Active Directory, and the required Citrix XenDesktop configuration.

Information in this document can be used as the basis for a solution build, white paper, best practices document, or training.

Scope

This Proven Solution Guide contains the results observed from testing the EMC Infrastructure for Citrix XenDesktop 5.5 solution. The objectives of this testing are to establish:

- A reference architecture of validated hardware and software that permits easy and repeatable deployment of the solution.
- The storage best practices to configure the solution in a manner that provides optimal performance, scalability, and protection in the context of the midtier enterprise market.

Not in scope

Implementation instructions are beyond the scope of this document. Information on how to install and configure Citrix XenDesktop, XenApp, and XenServer components, Cisco UCS, and the required EMC products is outside the scope of this document. Links to supporting documentation for these products are provided where applicable.

Audience

The intended audience for this Proven Solution Guide is:

- EMC, Cisco, and Citrix customers
- EMC, Cisco, and Citrix partners
- Internal EMC, Cisco, and Citrix personnel

Prerequisites

It is assumed that the reader has a general knowledge of the following products:

- Citrix XenDesktop
- Citrix XenApp
- Citrix XenServer
- EMC VNX series
- Cisco UCS and Nexus switches
**Terminology**

Table 1 provides terms frequently used in this paper.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC VNX FAST Cache</td>
<td>EMC VNX FAST Cache is a feature that enables the use of EFD as an expanded cache layer for the array.</td>
</tr>
<tr>
<td>Machine Creation Services (MCS)</td>
<td>MCS is a collection of services that work together to create virtual desktops from a master desktop image on demand, optimizing storage utilization, and providing a pristine virtual desktop to each user every time they log on.</td>
</tr>
<tr>
<td>Login VSI</td>
<td>Login VSI is a third-party benchmarking tool developed by Login Consultants that simulates real-world Virtual Desktop Infrastructure (VDI) workload by using an AutoIT script, and determines the maximum system capacity based on the response time of the users.</td>
</tr>
</tbody>
</table>

**Reference architecture**

This Proven Solution Guide has a corresponding Reference Architecture document that is available on the EMC Online Support website and EMC.com. The *EMC Infrastructure for Citrix XenDesktop 5.5, EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, XenApp 6.5, and XenServer 6—Reference Architecture* provides more details.

Users who do not have access to these documents should contact an EMC representative.

The reference architecture and the results in this Proven Solution Guide are valid for 1,000 Windows 7 virtual desktops conforming to the workload described in “Validated environment profile” on page 63.
Figure 1 depicts the logical architecture of the midsize solution.
## Configuration

**Test results**

Chapter 6: Testing and Validation provides more information on the performance results.

**Hardware resources**

Table 2 lists the hardware used for the solution.

### Table 2. Solution hardware

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Quantity</th>
<th>Configuration</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC VNX5300™</td>
<td>1</td>
<td>• Two Data Movers (active/standby)</td>
<td>VNX shared storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Three DAEs configured with:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Forty 300 GB, 15k rpm 3.5&quot; SAS disks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Twenty-five 2 TB, 7200 rpm 3.5&quot; NL-SAS disks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Three 100 GB, 3.5&quot; Flash drives</td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 5020</td>
<td>2</td>
<td>Forty 10 Gb ports</td>
<td>Redundant LAN A/B configuration</td>
</tr>
<tr>
<td>Cisco UCS B200-M1 blades</td>
<td>20</td>
<td>• Memory: 72 GB RAM</td>
<td>Two XenServer resource pools to host 1,000 virtual desktops</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPU: Two Intel Xeon E5540 2.5 GHz quad-core processors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal storage: Two 146 GB internal SAS disks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External storage: VNX5300 (NFS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HBA/NIC: M71KR-Q Qlogic Converged Network Adapter (CNA)</td>
<td></td>
</tr>
<tr>
<td>Other servers</td>
<td>3</td>
<td>• Memory: 20 GB RAM</td>
<td>XenServer resource pool to host infrastructure virtual machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPU: Two Intel Xeon E5450 3.0 GHz quad-core processors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internal storage: One 67 GB disk</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External storage: VNX5300 (NFS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NIC: Two Broadcom NetXtreme II BCM 1000 Base-T Adapters</td>
<td></td>
</tr>
</tbody>
</table>
Table 3 lists the hardware used for the solution.

**Table 3. Solution Software**

<table>
<thead>
<tr>
<th>Software</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC VNX5300</td>
<td></td>
</tr>
<tr>
<td>VNX OE for File</td>
<td>Release 7.0.40.1</td>
</tr>
<tr>
<td>VNX OE for Block</td>
<td>Release 31 (05.31.000.5.509)</td>
</tr>
<tr>
<td><strong>Cisco UCS and Nexus</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco UCS B-Series server</td>
<td>Version 1.4(3q)</td>
</tr>
<tr>
<td>Cisco Nexus 5020</td>
<td>Version 4.2(1)N1(1)</td>
</tr>
<tr>
<td><strong>XenDesktop/XenApp Virtualization</strong></td>
<td></td>
</tr>
<tr>
<td>Citrix XenDesktop Controller</td>
<td>Version 5.5 Platinum Edition</td>
</tr>
<tr>
<td>Citrix XenApp server</td>
<td>Version 6.5</td>
</tr>
<tr>
<td>OS for XenDesktop Controller</td>
<td>Windows Server 2008 R2 Enterprise Edition</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Version 2008 Enterprise Edition (64-bit)</td>
</tr>
<tr>
<td><strong>Citrix XenServer</strong></td>
<td></td>
</tr>
<tr>
<td>XenServer</td>
<td>6.0 (Build 50762p)</td>
</tr>
<tr>
<td>XenCenter</td>
<td>6.0 (Build 50489)</td>
</tr>
<tr>
<td><strong>Virtual Desktops</strong></td>
<td></td>
</tr>
<tr>
<td>Software used to generate the test load</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>MS Windows 7 Enterprise (32-bit) SP1</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Office Enterprise 2007 SP2</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>8.0.7601.17514</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>9.1</td>
</tr>
<tr>
<td>McAfee Virus Scan</td>
<td>8.7.0i Enterprise</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>10.0.22.87</td>
</tr>
<tr>
<td>Bullzip PDF Printer</td>
<td>6.0.0.865</td>
</tr>
<tr>
<td>FreeMind</td>
<td>0.8.1</td>
</tr>
<tr>
<td>Login VSI (VDI workload generator)</td>
<td>3.0 Professional edition</td>
</tr>
</tbody>
</table>
Chapter 2: Citrix Virtual Desktop Infrastructure

2

Citrix Virtual Desktop Infrastructure

This chapter describes the general design and layout instructions that apply to the specific components used during the development of this solution. This chapter includes the following sections:

- Citrix XenDesktop 5.5
- Citrix XenApp 6.5
- Citrix XenServer 6 infrastructure
- Windows infrastructure
- Cisco unified computing and networking

Citrix XenDesktop 5.5

Introduction

Citrix XenDesktop offers a powerful and flexible desktop virtualization solution that enables users to deliver on-demand virtual desktops and applications anywhere, using any type of device. The XenDesktop’s FlexCast delivery technology, users can deliver every type of virtual desktop, tailored to individual performance and personalization needs for unprecedented flexibility and mobility.

Powered by Citrix HDX technologies, XenDesktop provides a superior user experience with Flash multimedia and applications, 3D graphics, webcams, audio, and branch office delivery, while using less bandwidth than alternative solutions. The high-speed delivery protocol provides unparalleled responsiveness over any network, including low bandwidth and high latency WAN connections.

Deploying Citrix XenDesktop components

This solution is deployed using two XenDesktop 5.5 controllers that are capable of scaling up to 1,000 virtual desktops.

The core elements of a Citrix XenDesktop 5.5 implementation are:

- Citrix XenDesktop 5.5 controllers
- Citrix License Server
- Citrix XenApp 6.5
- Citrix XenServer 6

Additionally, the following components are required to provide the infrastructure for a XenDesktop 5.5 deployment:

- Microsoft Active Directory
Chapter 2: Citrix Virtual Desktop Infrastructure

- Microsoft SQL Server
- DNS Server
- DHCP Server

**Citrix XenDesktop controller**

The Citrix XenDesktop controller is the central management location for virtual desktops and has the following key roles:

- Broker connections between users and virtual desktops
- Control the creation and retirement of virtual desktop images
- Assign users to desktops
- Control the state of the virtual desktops
- Control access to the virtual desktops

Two XenDesktop 5.5 controllers are used in this solution to provide high availability as well as load balancing of brokered desktop connections. A Citrix License Server is installed on one of the controllers.

**Machine Creation Services**

MCS is a new provisioning mechanism introduced in XenDesktop 5.5. It is integrated with Desktop Studio, the new XenDesktop management interface, to provision, manage, and decommission desktops throughout the desktop lifecycle management from a centralized point of management.

MCS allows several types of machines to be managed within a catalog in Desktop Studio, including dedicated and pooled machines. Desktop customization is persistent for dedicated machines; where a non-persistent desktop is appropriate, a pooled machine should be used.

In this solution, MCS provisions 1,000 virtual desktops that are running Windows 7. The desktops are deployed from two dedicated machine catalogs.

Desktops provisioned using MCS share a common base image within a catalog. Because of this, the base image is accessed with sufficient frequency to leverage EMC VNX FAST Cache, where frequently accessed data is promoted to Flash drives to provide optimal I/O response time with fewer physical disks.

**Citrix XenApp 6.5**

**XenApp overview**

Citrix XenApp is an on-demand application delivery solution that enables any Windows application to be virtualized, centralized, and managed in the datacenter and instantly delivered as a service to users anywhere on any device. XenApp reduces the cost of application management by as much as 50 percent, increases IT responsiveness when delivering an application to distributed users, and improves application and data security.
This solution is deployed using a server farm with two XenApp 6.5 servers that are capable of scaling up to 1,000 virtual desktops. Application streaming is used in this solution because of the following benefits:

- Install once, deliver anywhere
- Seamless updates
- Application isolation and caching
- Offline access
- Easy disaster recovery

All profiled applications (Adobe Reader, Microsoft Office 2007, and FreeMind) in this solution are stored in an App Hub, a central file share that resides on a VNX CIFS file system. Because applications are streamed from the central location to each desktop client, application update is performed once in the central location, which is backed up or replicated in case of disaster recovery. VNX file level deduplication and compression are leveraged to increase storage efficiency and lower TCO.

**Citrix XenServer 6 infrastructure**

**XenServer 6 overview**

Citrix XenServer is the complete server virtualization platform from Citrix. The XenServer package contains everything needed to create and manage a deployment of virtual x86 computers running on Xen, the open-source paravirtualizing hypervisor with near-native performance.

The High Availability (HA) features in XenServer resource pool along with Workload Balancing (WLB) and XenMotion enable seamless migration of virtual desktops from one XenServer to another with minimal or no impact to customers' usage.

**XenServer resource pool**

Two XenServer resource pools are deployed to house 1,000 desktops in this solution. Each resource pool consists of eight XenServers to support 500 desktops, resulting in 62-63 virtual machines per XenServer. Each resource pool has access to four NFS based Storage Repositories (SR) for desktop provisioning, for a total of 125 virtual machines per SR.

The Infrastructure resource pool consists of three XenServers and holds the following virtual machines:

- Windows 2008 R2 domain controller—provides DNS, Active Directory, and dynamic host configuration protocol (DHCP) services.
- XenDesktop 5 controllers on Windows 2008 R2—provide services for managing virtual desktops.
- XenApp 6.5 servers on Windows 2008 R2—provide centralized application management and delivers applications as a cost effective, on-demand service.
Chapter 2: Citrix Virtual Desktop Infrastructure

Windows infrastructure

Introduction
Microsoft Windows provides the infrastructure used to support the virtual desktops and includes the following components:

- Microsoft Active Directory
- Microsoft SQL Server
- DNS Server
- DHCP Server

Microsoft Active Directory
The Windows domain controller runs the Active Directory service that provides the framework to manage and support the virtual desktop environment. Active Directory performs the following functions:

- Manages the identities of users and their information
- Applies group policy objects
- Deploys software and updates

Microsoft SQL Server
Microsoft SQL Server is a relational database management system (RDBMS). A dedicated SQL Server 2008 SP2 is used to provide the required databases to XenDesktop controllers and XenApp server farm.

DNS Server
DNS is the backbone of Active Directory. It provides the primary name resolution mechanism for Windows servers and clients.

In this solution, the DNS role is enabled on the domain controller.

DHCP Server
The DHCP Server provides the IP address, DNS Server name, gateway address, and other information to the virtual desktops.

In this solution, the DHCP role is enabled on the domain controller. The DHCP scope is configured to accommodate the range of IP addresses for 1,000 or more virtual desktop machines.

Cisco unified computing and networking

Cisco UCS B-Series servers
Cisco Unified Computing System (UCS) is a next-generation data center platform that integrates computing, networking, storage access, and virtualization into a cohesive system designed to reduce TCO and increase business agility.

The Cisco UCS B-Series blade server platform used to validate this solution is the B200 M1 blade server, a half-width, two-socket blade server. The system uses two Intel Xeon 5500 Series processors, as much as 96 GB of double data rate type three (DDR3) memory, two optional hot-swappable small form factor (SFF) serial attached SCSI (SAS) disk drives, and a single mezzanine connector for up to 20 gigabits/s of I/O throughput. The server balances simplicity, performance, and density for production-level virtualization and other mainstream data center workloads.
Cisco Nexus 5000 series

The Cisco Nexus 5000 series is first and foremost a family of outstanding access switches for 10-gigabit Ethernet connectivity. Most of the switch features are designed for high performance with 10-gigabit Ethernet. The Cisco Nexus 5000 series also supports Fibre Channel over Ethernet (FCoE) on each 10-gigabit Ethernet port. FCoE is used to implement a unified data center fabric, consolidating LAN, SAN, and server clustering traffic.
3 Storage Design

The storage design described in this section applies to the specific components of this solution.

EMC VNX series storage architecture

Introduction

The EMC VNX series is a dedicated network server optimized for file and block access that delivers high-end features in a scalable and easy-to-use package.

The VNX series delivers a single-box block and file solution, which offers a centralized point of management for distributed environments. This makes it possible to dynamically grow, share, and cost-effectively manage multiprotocol file systems and provide multiprotocol block access. Administrators can take advantage of the simultaneous support for NFS and CIFS protocols by enabling Windows and Linux/UNIX clients to share files by using the sophisticated file-locking mechanism of VNX for File and VNX for Block for high-bandwidth or for latency-sensitive applications.

This solution uses file-based storage to leverage the benefits that each of the following provides:

- File-based storage over the Network File System (NFS) protocol is used to store the VHD files for all virtual desktops.
- File-based storage over the CIFS protocol is used to store user data, roaming profiles, and XenApp profiles. This has the following benefits:
  - Redirection of user data, roaming profiles, and XenApp profiles to a central location for easy backup and administration.
  - Single instancing and compression of unstructured user data and XenApp profiles to provide the highest storage utilization and efficiency.

This section explains the configuration of the storage that is provided over NFS to the XenServer resource pools to store the VHD images, and configuration of the storage that is provided over CIFS to redirect user data, roaming profiles, and XenApp profiles.
Figure 2 shows the storage layout of the disks in this reference architecture.

Storage layout overview

The following storage configuration is used in the solution:

- Four SAS disks (0_0_0 to 0_0_3) are used for the VNX OE.
- Disks 0_0_4, 0_1_10, 0_1_11, and 0_2_9 are hot spares. These disks are marked as hot spare in the storage layout diagram.
- Thirty SAS disks (0_0_5 to 0_0_14, 1_0_0 to 1_0_14, and 0_1_0 to 0_1_4) on the RAID 5 storage pool 1 are used to store virtual desktops. FAST Cache is enabled for the entire pool. Thirty LUNs of 200 GB each are carved out of the pool to provide the storage required to create eight NFS file systems. The file systems are presented to the XenServers as NFS SRs.
- Two Flash drives (0_1_12 and 0_1_13) are used for EMC VNX FAST Cache. There are no user-configurable LUNs on these drives.
- Five SAS disks (0_1_5 to 0_1_9) on the RAID 5 storage pool 2 are used to store the infrastructure virtual machines. A 1 TB LUN is carved out of the pool to form an NFS file system. The file system is presented to the XenServers as an NFS SR.
- Twenty-four NL-SAS disks (1_1_0 to 1_1_14, and 0_2_0 to 0_2_8) on the RAID 6 storage pool 3 are used to store user data, roaming profiles, and XenApp profiles. FAST Cache is enabled for the entire pool. Twenty-five LUNs
of 1 TB each are carved out of the pool to provide the storage required to create three CIFS file systems.

- Disks 0_1_14, and 0_2_10 to 0_2_14 are unbound. They were not used for testing this solution.

**File system layout**

Figure 3 shows the layout of the NFS file systems used to store the virtual desktops:

Thirty LUNs of 200 GB each are carved out of the RAID 5 storage pool configured with 30 SAS drives. The LUNs are presented to VNX File as dvols that belong to a system defined pool. Eight file systems are then carved out of the Automatic Volume Management (AVM) system pool and are presented to the XenServers as NFS SRs. 1,000 virtual desktops are evenly distributed among the eight NFS SRs.

Starting in VNX File version 7.0.35.3, AVM is enhanced to intelligently stripe across dvols that belong to the same block-based storage pool. There is no need to manually create striped volumes and add them to user defined file-based pools.

Like the NFS file systems, CIFS file systems are provisioned from AVM system pool to store user home directories, roaming user profiles, and XenApp App Hub, a centralized file share on which application profiles reside. The three file systems are grouped in the same storage pool because their I/O profiles are sequential.
Figure 4 shows the layout of the CIFS file systems:

![Diagram showing CIFS file system layout]

Twenty-five LUNs of 1TB each are carved out of the RAID 6 storage pool configured with 24 NL-SAS drives. Twenty-four drives are used because block-based storage pool internally creates 6+2 RAID 6 groups. Therefore, the number of NL-SAS drives used is a multiple of eight. Likewise, twenty-five LUNs are used because AVM stripes across five dvols, so the number of dvols is a multiple of five.

FAST Cache is enabled on both storage pools that are used to store the NFS and CIFS file systems.

EMC VNX FAST Cache

VNX FAST Cache, a part of the VNX FAST Suite, enables Flash drives to be used as an expanded cache layer for the array. The VNX5300 is configured with two 100 GB Flash drives in a RAID 1 configuration for a 93 GB read/write-capable cache. This is the minimum amount of FAST Cache. Larger configurations are supported for scaling beyond 1,000 desktops.

FAST Cache is an array-wide feature available for both file and block storage. FAST Cache works by examining 64 KB chunks of data in FAST Cache-enabled objects on the array. Frequently accessed data is copied to the FAST Cache and subsequent accesses to the data chunk are serviced by FAST Cache. This enables immediate promotion of very active data to Flash drives. The use of Flash drives dramatically improves the response time for the active data and reduces data hot spots that occur within the LUN.

FAST Cache is an extended read/write cache that enables XenDesktop to deliver consistent performance at Flash-drive speeds by absorbing read-heavy activities such as boot storms and antivirus scans, and write-heavy workloads such as operating system patches and application updates.
Chapter 3: Storage Design

EMC Infrastructure for Citrix XenDesktop 5.5
EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, XenApp 6.5, and XenServer 6—Proven Solution Guide

This extended read/write cache is an ideal caching mechanism for MCS in XenDesktop 5.5 because the base desktop image and other frequently accessed user data are serviced directly from the Flash drives without having to access the slower drives at the lower storage tier.

XenServer storage layout

A storage pool of 30 x 300 GB SAS drives is configured on the VNX to provide the storage required for the virtual desktops. Eight NFS file systems are carved out of the pool to present to the XenServers as eight storage repositories. Each of these 768 GB storage repositories accommodates 125 virtual machines, enabling each desktop to grow to a maximum average size of 6 GB. The pool of desktops created in XenDesktop is balanced across all eight SRs.

VNX shared file systems

Virtual desktops use three VNX shared file systems to:

- Store user roaming profiles
- Redirect user storage that resides in home directories
- Store XenApp profiles in an App Hub

Each file system is exported to the environment through a CIFS share.

Table 4 shows the file systems used with their initial data size set for user profiles, redirected user storage, and XenApp profiles storage in App Hub.

Table 4. File systems

<table>
<thead>
<tr>
<th>File system</th>
<th>Use</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>profiles_fs</td>
<td>Users’ profile data</td>
<td>2 TB</td>
</tr>
<tr>
<td>userdata1_fs</td>
<td>Users’ data</td>
<td>4 TB</td>
</tr>
<tr>
<td>xaprofile_fs</td>
<td>XenApp profiles</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

Roaming profiles and folder redirection

The local user profile is not recommended in a VDI environment. A performance penalty is incurred when a new local profile is created whenever a user logs in to a new desktop image. On the other hand, roaming profiles and folder redirection enables user data to be stored centrally on a network location that resides on a CIFS share hosted by VNX. This reduces the performance hit during user logon while enabling user data to roam with the profiles.

Alternative profile management tools such as Citrix User Profile Manager, or a third-party tool such as AppSense Environment Manager, provide more advanced and granular features to manage various user profile scenarios. Refer to User Profile Planning Guide on the Citrix website for further details.

EMC VNX for File Home Directory feature

The EMC VNX for File Home Directory feature uses the userdata1_fs file system to automatically map the H: drive of each virtual desktop to the users’ own dedicated subfolder on the share. This ensures that each user has exclusive rights to a dedicated home drive share. This share is not created manually. The Home Directory feature automatically maps this share for each user.
The Documents folder for each user is also redirected to this share. This enables users to recover the data in the Documents folder by using the VNX Snapshots for File. The file system is set at an initial size of 1 TB, and extends itself automatically when more space is required.

**Profile export**

The profiles_fs file system is used to store user roaming profiles. It is exported through CIFS. The Universal/Uniform Naming Convention (UNC) path to the export is configured in Active Directory for roaming profiles as shown in **Figure 5**:

![Figure 5. UNC path for roaming profiles](image)

**Capacity**

The file systems leverage Virtual Provisioning™ and compression to provide flexibility and increased storage efficiency. If single instancing and compression are enabled, unstructured data such as user documents typically leads to a 50 percent reduction in consumed storage.

The file systems for user profiles, documents, and XenApp profiles are configured as follows:

- profiles_fs is configured to consume 2 TB of space. With a 50 percent space savings, each profile can grow up to 4 GB in size. The file system size can be extended, if required.
- userdata1_fs is configured to consume 4 TB of space. With a 50 percent space savings, each user is able to store 8 GB of data. The file system size can be extended, if required.
- xaprobe_f is configured to consume 1 TB of space. With a 50 percent space savings, the XenApp server farm is able to store 2 TB of profiled applications in an App Hub. The file system size can be extended, if required.
Network Design

This chapter describes the network design used in this solution and contains the following sections:

- Considerations
- VNX for file network configuration
- XenServer network configuration
- Cisco Nexus 5020 configuration
- Cisco UCS network configuration

Considerations

Figure 6 shows the 10-gigabit Ethernet connectivity between the Cisco UCS B-Series servers and the EMC VNX platform. Uplink Ethernet ports from the Nexus 5020 switches can be used to connect to a 1 gigabit/s or 10 gigabit/s external LAN. In this solution, a 1 gigabit/s LAN is used to extend Ethernet connectivity to the desktop clients, XenDesktop management components, and Windows server infrastructure.
Logical design considerations

This validated solution uses virtual local area networks (VLANs) to segregate network traffic of various types to improve throughput, manageability, application separation, high availability, and security.

The IP scheme for the virtual desktop network must be designed with enough IP addresses in one or more subnets for the DHCP Server to assign them to each virtual desktop.

Link aggregation

VNX platforms provide network high availability or redundancy by using link aggregation. This is one of the methods used to address the problem of link or switch failure.

Link aggregation enables multiple active Ethernet connections to appear as a single link with a single media access control (MAC) address, and potentially multiple IP addresses.

In this solution, Link Aggregation Control Protocol (LACP) is configured on VNX, combining two 10-gigabit Ethernet ports into a single virtual device. If a link is lost in the Ethernet port, the link fails over to another port. All network traffic is distributed across the active links.
VNX for file network configuration

Data Mover ports

The VNX5300 consists of two Data Movers. The Data Movers can be configured in an active/active or active/passive configuration. In the active/passive configuration, the passive Data Mover serves as a failover device for the active Data Mover. In this solution, the Data Movers operate in the active/passive mode.

The VNX5300 Data Movers are configured with two 10-gigabit interfaces on a single I/O module. LACP is used to configure ports fxg-1-0 and fxg-1-1 to support virtual machine traffic, home folder access, and external access for roaming profiles.

Figure 7 shows the rear view of the two VNX5300 Data Movers that include two 10-gigabit optical Ethernet (fxg) ports each in I/O expansion slot 1.

Figure 7. Rear view of the two VNX5300 Data Movers

LACP configuration on the Data Mover

To configure the link aggregation that uses fxg-1-0 and fxg-1-1 on Data Mover 2, run the following command:

```
$ server_sysconfig server_2 -virtual -name <Device Name> -create trk -option "device=fxg-1-0,fxg-1-1 protocol=lacp"
```

To verify if the ports are channeled correctly, run the following command:

```
$ server_sysconfig server_2 -virtual -info lacpl
server_2:
*** Trunk lacpl: Link is Up ***
*** Trunk lacpl: Timeout is Short ***
*** Trunk lacpl: Statistical Load Balancing is IP ***
Device   Local Grp  Remote Grp    Link   LACP Duplex Speed
--------------------------------------------------------------
fxg-1-0     10000  4480     Up   Up   Full    10000 Mbs
fxg-1-1     10000  4480     Up   Up   Full    10000 Mbs
```

The remote group number must match for both ports, and the LACP status must be “Up.” Verify if the appropriate speed and duplex are established as expected.

Data Mover Interfaces

EMC recommends creation of two Data Mover interfaces and IP addresses on the same subnet with the management interface on the XenServers. Half of the NFS SRs are accessed through one IP address and the other half are accessed through the second IP. This balances the NFS traffic to be among the XenServer NIC bonding members.
The following command shows an example of assigning two IP addresses to the same virtual interface named lacp1:

```
$ server_ifconfig server_2 -all
server_2:
lacp1-1 protocol=IP device=lacp1
   inet=192.168.16.2 netmask=255.255.255.0 broadcast=192.168.16.255
   UP, Ethernet, mtu=9000, vlan=276, macaddr=0:60:48:1b:76:92
lacp1-2 protocol=IP device=lacp1
   inet=192.168.16.3 netmask=255.255.255.0 broadcast=192.168.16.255
   UP, Ethernet, mtu=9000, vlan=276, macaddr=0:60:48:1b:76:93
```

To enable jumbo frames for the link aggregation interface in the previous step, run the following command to increase the Maximum Transmission Unit (MTU) size:

```
$ server_ifconfig server_2 lacp1-1 mtu=9000
```

To verify if the MTU size is set correctly, run the following command:

```
$ server_ifconfig server_2 lacp1-1
server_2:
lacp1 protocol=IP device=lacp1
   inet=192.168.16.2 netmask=255.255.255.0 broadcast=192.168.16.255
   UP, Ethernet, mtu=9000, vlan=276, macaddr=0:60:48:1b:76:92
```

Enable jumbo frames on Data Mover interface
XenServer network configuration

NIC bonding

All network interfaces on the UCS B-Series servers in this solution use 10-gigabit Ethernet connections. All XenServers have two 10-gigabit adapters that are bonded together to provide multipathing and network load balancing as shown in Figure 8.

<table>
<thead>
<tr>
<th>Networks</th>
<th>MAC address</th>
<th>Link Status</th>
<th>Speed</th>
<th>Duplex</th>
<th>Vendor</th>
<th>Device</th>
<th>PCI Bus/Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC 1</td>
<td>00:20:55:01:00:1A</td>
<td>Disconnected</td>
<td>-</td>
<td>-</td>
<td>Intel Corporation</td>
<td>82580AC L2-10-Gigabit AT Physical Port Network Connection: 0x08/00.0</td>
<td></td>
</tr>
<tr>
<td>NIC 2</td>
<td>00:20:55:01:00:7A</td>
<td>Disconnected</td>
<td>-</td>
<td>-</td>
<td>Intel Corporation</td>
<td>82580AC L2-10-Gigabit AT Physical Port Network Connection: 0x08/00.0</td>
<td></td>
</tr>
<tr>
<td>Bond 91.1</td>
<td>00:20:55:01:00:7F</td>
<td>Disconnected</td>
<td>-</td>
<td>-</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8. NIC bonding configuration
Set the NIC bond mode for the XenServer to **Active-active** as shown in Figure 9. Select **Automatically add this network to new virtual machines** so that the bonded interface is automatically attached to the newly created virtual machines.

**Note:** Jumbo frame is only supported if vSwitch network is configured for XenServer. Do not increase the MTU size on this page to enable jumbo frame if Linux network stack is used.

![Figure 9. NIC bond mode](image-url)
Cisco Nexus 5020 configuration

Overview
Two 40-port Cisco Nexus 5020 switches provide redundant high-performance, low-latency 10-gigabit Ethernet, delivered by a cut-through switching architecture for 10-gigabit Ethernet server access in next-generation data centers.

Cabling
In this solution, the XenServer and VNX Data Mover cabling are evenly spread across two Nexus 5020 switches to provide redundancy and load balancing of the network traffic.

Enable jumbo frames on Nexus switch
The following excerpt of the switch configuration illustrates the commands required to enable jumbo frames at the switch level because per-interface MTU is not supported:

```
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
system qos
  service-policy type network-qos jumbo
```

virtual Port Channel for Data Mover ports
virtual Port Channel (vPC) is configured on both switches because the Data Mover connections for the two 10-gigabit network ports are spread across two Nexus switches and LACP is configured for the two Data mover ports.

The following excerpt is an example of the switch configuration pertaining to the vPC setup for one of the Data Mover ports. The configuration on the peer Nexus switch is mirrored for the second Data Mover port.

```
n5k-1# show running-config
...
feature vpc
...
vpc domain 2
  peer-keepalive destination <peer-nexus-ip>
...
interface port-channel3
  description channel uplink to n5k-2
  switchport mode trunk
  vpc peer-link
  spanning-tree port type network
interface port-channel4
  switchport mode trunk
  vpc 4
  switchport trunk allowed vlan 275-277
...
interface Ethernet1/4
  description 1/4 vnx dm2 fxg-1-0
  switchport mode trunk
  switchport trunk allowed vlan 275-277
  channel-group 4 mode active
```
interface Ethernet1/5
  description 1/5 uplink to n5k-2 1/5
  switchport mode trunk
  channel-group 3 mode active
interface Ethernet1/6
  description 1/6 uplink to n5k-2 1/6
  switchport mode trunk
  channel-group 3 mode active

To verify if the vPC is configured correctly, run the following command on both switches and the output should look like this:

n5k-1# show vpc
Legend:
  (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 2
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: success
vPC role                        : secondary
Number of vPCs configured       : 1
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -

vPC Peer-link status
------------------------------------------------------------------
id   Port   Status       Active vlans
--   ----   ------      ------------
1    Po3    up     1,275-277

vPC status
------------------------------------------------------------------
id   Port   Status       Consistency Reason       Active vlans
----- ----   ------      --------------        --------------
4    Po4    up     success       success         275-277
MTU size for each UCS B-Series server is set in a service profile, service profile template, or vNIC template. Figure 10 shows an example of setting the MTU size to 9000 for vNIC eth0 in a service profile template using the UCS Manager GUI.

Figure 10. UCS Manager - MTU configuration
Chapter 5: Installation and Configuration

5

Installation and Configuration

This chapter describes how to install and configure this solution and includes the following sections:

- Installation overview
- Citrix XenDesktop components
- Citrix XenApp components
- Storage components

Installation overview

This section provides an overview of the configuration of the following components:

- Desktop pools
- Storage pools
- FAST Cache
- VNX Home Directory

The installation and configuration steps for the following components are available on the Citrix (www.citrix.com) and Cisco (www.cisco.com) websites:

- Citrix XenDesktop 5.5
- Citrix XenApp 6.5
- Citrix XenServer 6
- Cisco UCS and Nexus switches

The installation and configuration steps for the following components are not covered:

- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Active Directory, DNS, and DHCP
- Microsoft SQL Server 2008 SP2
Citrix XenDesktop components

Citrix XenDesktop installation overview

The Citrix online product documentation (Citrix eDocs) available on the Citrix website provides the detailed procedures to install XenDesktop 5.5. There are no special configuration requirements for this solution.

Citrix XenDesktop machine catalog configuration

In this solution, persistent desktops are created using MCS to allow users to maintain their desktop customization. Complete the following steps to create a dedicated machine catalog with persistent desktops:

1. On the XenDesktop 5.5 controller, select Start > All Programs > Citrix > Desktop Studio. The Citrix Desktop Studio window appears.

2. In the left navigation pane, right-click Machines, and then select Create Catalog. The Create Catalog window appears.

![Citrix Desktop Studio](image)

Figure 11. Select Create Catalog
3. In the **Machine type** page, select **Dedicated** from **Machine type** list box.

4. Click **Next**. The **Master Image and Hosts** page appears.

5. In the **Hosts** list, select the cluster host from which the virtual desktops are to be deployed.

6. Click the ![ ] button to select a virtual machine or VM snapshot as the master image.
7. Click Next. The Number of VMs page appears.

8. In the Number of virtual machines to create box, type or select the number of virtual machines to be created. Adjust the virtual machine specifications in Master Image and Active Directory computer accounts areas, if needed. In this example, the Create new accounts option is selected.

![Create Catalog]

Figure 14. Specify the number of virtual machines

9. Click Next. The Create Accounts page appears.
   
   Complete the following steps:
   
   a. In the Domain area, select an Active Directory container to store the computer accounts.

   b. In the Account naming scheme field, type the account naming scheme of your choice. An example of xd#### will create computer account names xd0001 through xd0500. These names are used even when the virtual machines are created.
Figure 15. Select an Active Directory location

10. Click Next. The Administrators page appears.

11. In the Administrators page, make any required changes, and then click Next. The Summary page appears.

12. In the Summary page, verify the settings for the catalog and in the Catalog name field, type a name for the catalog.

Figure 16. Review the summary

13. Click Finish to start the deployment of the machines.
Chapter 5: Installation and Configuration

Check the machine creation status by monitoring the green progress bar while browsing the list of catalogs. Once the machines are created, add them to a desktop group before any user accesses the virtual desktops.

### Throttle commands to vCenter Server

The number of concurrent requests sent from XenDesktop controllers to the XenServer resource pool are adjusted to either expedite powering on/off of virtual machines, or back off the number of concurrent operations so that the resource pool is not overwhelmed.

To change the throttle rate, complete the following steps:

1. Open Desktop Studio on one of the XenDesktop 5.5 controllers.
2. In the left navigation pane of the Citrix Desktop Studio window, expand Configuration, and then select Hosts.

![Desktop Studio](image)

**Figure 17.** Select Hosts

3. In the right pane, right-click the existing host connection, and then select Change details. The Change Host Details dialog box appears.

![Change Host Details](image)

**Figure 18.** Select Change details
4. In the **Change Host Details** dialog box, click **Advanced**.

![Change Host Details dialog box]

Figure 19. Change Host Details dialog box

5. In the **Advanced Host Details** dialog box, make the required changes and click **OK** twice to save the changes.

![Advanced Host Details dialog box]

Figure 20. Advanced Host Details dialog box

XenDesktop controllers manage the number of idle virtual desktops based on time, and automatically optimize the idle pool settings in the desktop group based on the number of virtual desktops in the group.

The default idle pool settings is adjusted based on customer requirements to have virtual machines powered on in advance to avoid a boot storm scenario. During the validation testing, the idle desktop count is set to match the number of desktops in the group to ensure that all desktops are powered on in a steady state, and ready for client connections immediately.
To change the idle pool settings for a desktop group that consists of dedicated machines, complete the following steps:

1. Open Desktop Studio on one of the XenDesktop 5.5 controllers.

   a. In the left navigation pane of the Citrix Desktop Studio window, select Desktop Studio.

   b. In the right pane, select the Powershell tab.

   c. In the bottom-right-corner of the right pane, select Launch PowerShell. The PowerShell window appears.

2. In the PowerShell window, enter the following command where XD5DG1 is the desktop group name, and PeakBufferSizePercent and OffPeakBufferSizePercent are percentages of desktops to be powered on during peak and off-peak hours:

   ```powershell
   PS C:\> set-BrokerDesktopGroup XD5DG1 -PeakBufferSizePercent 100 -OffPeakBufferSizePercent 100
   ```
Citrix XenApp components

Pass-through authentication method

There are several authentication methods to access the XenApp services website including prompt, pass-through, pass-through with smart card, and so on. Pass-through authentication method is used in this solution because users can authenticate using the credentials they provided when they log on to their desktop sessions. Users do not need to re-enter their credentials and their resource set appears automatically, providing seamless user experience when virtualized applications are deployed.

To enable pass-through authentication for the XenApp services site, complete the following steps:

1. On a XenApp server, select \Start\All Programs\Citrix\Management Consoles\Citrix Web Interface Management. The Citrix Web Interface Management console appears.

   Complete the following steps:

   a. In the left navigation pane, select XenApp Services Sites.
   b. In the middle pane select the required site. In this example, the PNAgent site is selected.
   c. In the Actions pane, select Authentication Methods. The Configure Authentication Method - PNAgent dialog box appears.

   ![Figure 21. Select Authentication Methods](image)

   **Figure 21. Select Authentication Methods**
2. Select the **Pass-through** checkbox and clear all other checkboxes.

![Configure Authentication Methods - PNAgent dialog box](image)

Figure 22. Configure Authentication Methods - PNAgent dialog box

3. Click **Properties**. The **Properties – PNAgent** dialog box appears.

4. Select **Kerberos Authentication**, and then select **Use Kerberos only** checkbox.

![Properties - PNAgent dialog box](image)

Figure 23. Properties - PNAgent dialog box

5. Click **OK** twice to save the changes.

---

**Resource type**

When configuring a XenApp services site, the default resource type is set to online mode, which enables users to access application resources hosted on XenApp servers. Users need a network connection to work with their resources.

The offline streamed applications are deployed in this solution. Therefore, the resource type is set to offline or dual mode. Complete the following steps to change to dual mode that provides both online and offline application access from the web interface:

1. On a XenApp server, click **Start → All Programs → Citrix → Management Consoles → Citrix Web Interface Management**. The **Citrix Web Interface Management** console appears.

   Complete the following steps:

   a. In the left pane, select **XenApp Services Sites**.
b. In the middle pane, select the required site. In this example, the **PNAgent** site is selected.

c. In the **Actions** pane, click **Resource Types**. The **Manage Resource Types - PNAgent** dialog box appears.

![Select Resource Types](image1)

**Figure 24. Select Resource Types**

2. In the **Manage Resource Types - PNAgent** dialog box, select **Dual Mode**, and then click **OK** to save the change.

![Manage Resource Types - PNAgent dialog box](image2)

**Figure 25. Manage Resource Types – PNAgent dialog box**
XenApp application profile is created using Citrix streaming profiler. After a profile is edited, it is saved to an App Hub, a UNC path where the VNX CIFS share resides, as shown in the Figure 26.

Figure 26.  Save As window

Refer to the Citrix online product documentation (Citrix eDocs) available on the Citrix website for more information on how to prepare an application profile.

After an application is profiled using streaming profiler and its profile is stored on the VNX CIFS share, complete the following steps to publish the application and make it available to the clients:

1. On a XenApp server, click Start > All Programs > Citrix > Management Consoles > Citrix Delivery Services Console.
   a. In the left navigation pane of the Delivery Services Console, select Citrix AppCenter > Citrix Resources > XenApp > <farm name>.
   b. Right-click on Applications and select Publish application. The Publish Application wizard appears.
Chapter 5: Installation and Configuration

EMC Infrastructure for Citrix XenDesktop 5.5

EMC VNX Series (NFS), Cisco UCS, Citrix XenDesktop 5.5, XenApp 6.5, and XenServer 6—Proven Solution Guide

Figure 27. Select Publish application

2. In the **Name** page, type the name and description of the application to be published.

Figure 28. Publish Application - Name page
3. Click **Next**. The **Type** page appears.

4. In the **Choose the type of application to publish** area, select **Application**, and in the **Application type** frame, select **Streamed to client**.

![Figure 29. Publish Application - Type page](image)
5. Click **Next**. The **Location** page appears.

6. Browse for the VNX CIFS share folder using the UNC path that contains the `.profile` file that was created when the application was profiled using Citrix streaming profiler.

![Publish Application - Location page](image)

**Figure 30. Publish Application - Location page**
7. Click **Next**. The **Offline access** page appears.

8. Select **Enable offline access** and **Cache application at launch time**.

*Note:* The Citrix offline plug-in must be installed on the client to access offline application.

Figure 31. Publish Application – Offline access page
9. Click **Next**. The **Users** page appears.

10. Select the domain users/groups that are to be granted access to the published application.

![Figure 32. Publish Application - Users page](image)

**Figure 32. Publish Application - Users page**
11. Click **Next**: The **Shortcut presentation** page appears.
12. In the **Application shortcut placement** area, select **Add to the client’s Start menu**.

![Image of Shortcut presentation page](image)

Figure 33. **Publish Application – Shortcut presentation page**
13. **Click Next.** The **Publish immediately** page appears.

14. **Select Configure advanced application settings now.**

   ![Publish Application - Publish immediately page](image)

   **Figure 34.** Publish Application – Publish immediately page

15. **Click Next.** The **Access control** page appears.
16. Click Next. The Content redirection page appears.

17. Click Select all tab to select all file types to be associated with the application.

![Content redirection page](image)

Figure 35. Publish Application – Content redirection page

18. Click Next. The Alternate profiles page appears.

19. Click Next. The User privileges page appears.

20. Click Finish to publish the application.

When installing XenDesktop virtual desktop agent (VDA) on the desktop client, complete the following steps to install Citrix Receiver and offline plug-in to enable access to XenApp applications:

1. Run AutoSelect.exe from the XenDesktop 5.5 install media on the desktop client.
2. Select **Install Virtual Desktop Agent** on the main page.

![Figure 36. Install Virtual Desktop Agent](image)

3. Select **Advanced Install** on the second page.

   **Note:** If the **Quick Deploy** option is selected, the option to install Citrix Receiver and the offline plug-in is not provided.

![Figure 37. Advanced Install](image)

4. In the **Licensing Agreement** page, select *I accept the terms and conditions*, and then click **Next**.
5. Select **Virtual Desktop Agent** on the next page and, then click **Next**. The **Select Components to Install** page appears.

6. Select **Citrix Receiver** and type the URL specified in the XenApp services site for XenApp delivery as follows:

![Select Components to Install page](image)

**Figure 38. Select Components to Install page**

7. Click **Next**. The **Controller Location** page appears.

8. Type the fully qualified domain names of the XenDesktop controllers separated by spaces.

![Controller Location page](image)

**Figure 39. Controller Location page**
9. Click **Next** on the Virtual Desktop Configuration page to accept the default options.

![Virtual Desktop Configuration page]

**Figure 40. Virtual Desktop Configuration page**

10. Click **Install** on the **Summary** page to install the VDA, Citrix Receiver, and the offline plug-in.

![Summary page]

**Figure 41. Summary page**
Chapter 5: Installation and Configuration

Storage components

Storage pools

Storage pools in the EMC VNX OE support heterogeneous drive pools. In this solution, a RAID 5 storage pool is configured from 30 SAS drives. Thirty 200 GB thick LUNs are created from this storage pool as shown Figure 42. FAST Cache is enabled for the pool.

![Figure 42. Thirty 200 GB thick LUNs](image)

NFS active threads per Data Mover

The default number of threads dedicated to serve NFS requests is 384 per Data Mover on VNX. Since 1,000 desktop connections are required in this solution, it is recommended to increase the number of active NFS threads to the maximum of 2,048 on each Data Mover. The nthreads parameter is set using the following command:

```
#server_param server_2 -facility nfs -modify nthreads -value 2048
```

Reboot the Data Mover for the change to take effect.

Type the following command to confirm the value of the parameter:

```
#server_param server_2 -facility nfs -info nthreads
```

NFS performance fix

VNX file software contains a performance fix that significantly reduces NFS write latency. The minimum software patch required for the fix is 7.0.13.0. The performance fix takes effect only when the NFS file system is mounted using the “uncached” option as shown in the following command:

```
#server_mount server_2 -option uncached fs1 /fs1
```
The uncached option is verified using the following command:

```bash
#server_mount server_2
server_2:
root_fs_2 on / ufsx,perm,rw
root_fs_common on ./etc_common ufsx,perm,ro
userprofiles on /userprofiles ufsx,perm,rw
homedir on /homedir ufsx,perm,rw
InfraOS on /InfraOS ufsx,perm,rw,uncached
pool_nfs_1_fs1 on /pool_nfs_1_fs1 ufsx,perm,rw,uncached
pool_nfs_2_fs2 on /pool_nfs_2_fs2 ufsx,perm,rw,uncached
pool_nfs_3_fs3 on /pool_nfs_3_fs3 ufsx,perm,rw,uncached
pool_nfs_4_fs4 on /pool_nfs_4_fs4 ufsx,perm,rw,uncached
pool_nfs_5_fs5 on /pool_nfs_5_fs5 ufsx,perm,rw,uncached
pool_nfs_6_fs6 on /pool_nfs_6_fs6 ufsx,perm,rw,uncached
pool_nfs_7_fs7 on /pool_nfs_7_fs7 ufsx,perm,rw,uncached
pool_nfs_8_fs8 on /pool_nfs_8_fs8 ufsx,perm,rw,uncached
```

Enable FAST Cache

FAST Cache is enabled as an array-wide feature in the system properties of the array in Unisphere™. Select the FAST Cache tab, click Create, and then select the Flash drives to create the FAST Cache. There are no user-configurable parameters for FAST Cache.

![Figure 43. FAST Cache tab](image-url)
To enable FAST Cache for any LUN in a pool, go to the pool properties in Unisphere and click the **Advanced** tab. Select **Enabled** to enable FAST Cache, as shown in Figure 44.

![Enable FAST Cache](image)

**Figure 44. Enable FAST Cache**

The VNX Home Directory installer is available on the NAS Tools and Applications CD for each VNX OE for file release, and can be downloaded from the EMC Online Support website.

After the VNX Home Directory feature is installed, use the MMC snap-in to configure the feature. A sample configuration is shown Figure 45, and Figure 46.

![MMC snap-in](image)

**Figure 45. MMC snap-in**
For any user account that ends with a suffix between 1 and 1,000, the sample configuration shown Figure 46 automatically creates a user home directory in the following location and maps the H: drive to this path:

\userdata1_fs file system in the format \userdata1_fs\<domain>\<user>

Each user has exclusive rights to the folder.

Figure 46. Sample virtual desktop properties
This chapter provides a summary and characterization of the tests performed to validate the solution. The goal of the testing was to characterize the performance of the solution and its component subsystems during the following scenarios:

- Boot storm of all desktops
- McAfee antivirus full scan on all desktops
- Security patch install with Microsoft System Center Configuration Manager (SCCM) on all desktops
- User workload testing using Login Virtual Session Indexer (VSI) on all desktops

Validated environment profile

Table 5 provides the environment profile that was used to validate the solution.

<table>
<thead>
<tr>
<th>Profile characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of virtual desktops</td>
<td>1,000</td>
</tr>
<tr>
<td>Virtual desktop OS</td>
<td>Windows 7 Enterprise (32-bit) SP1</td>
</tr>
<tr>
<td>CPU per virtual desktop</td>
<td>1 vCPU</td>
</tr>
<tr>
<td>Number of virtual desktops per CPU core</td>
<td>6.25</td>
</tr>
<tr>
<td>RAM per virtual desktop</td>
<td>1 GB</td>
</tr>
<tr>
<td>Desktop provisioning method</td>
<td>MCS</td>
</tr>
<tr>
<td>Average storage available for each virtual desktop</td>
<td>6 GB</td>
</tr>
<tr>
<td>Average IOPS per virtual desktop at steady state</td>
<td>9 IOPS</td>
</tr>
<tr>
<td>Average peak IOPS per virtual desktop during boot storm</td>
<td>20 IOPS</td>
</tr>
<tr>
<td>Number of SRs to store virtual desktops</td>
<td>8</td>
</tr>
<tr>
<td>Number of virtual desktops per SR</td>
<td>125</td>
</tr>
<tr>
<td>Disk and RAID type for SRs</td>
<td>RAID 5, 300 GB, 15k rpm, 3.5” SAS disks</td>
</tr>
</tbody>
</table>
Use cases

Four common use cases were executed to validate whether the solution performed as expected under heavy load situations.

The tested use cases are:

- Simultaneous boot of all desktops
- Full antivirus scan of all desktops
- Installation of a security update using SCCM on all desktops
- Login and steady state user load simulated using the Login VSI medium workload on all desktops

In each use case, a number of key metrics is presented showing the overall performance of the solution.

Login VSI

This solution used Login VSI to run a user load against the desktops. Login VSI provided the guidance to gauge the maximum number of users a desktop environment can support. The Login VSI workload is categorized as light, medium, heavy, and custom. A medium workload with the following characteristics was selected for testing:

- The workload emulated a medium knowledge worker who uses Microsoft Office, Internet Explorer, and Adobe Acrobat Reader.
- After a session started, the medium workload repeated every 12 minutes.
- The response time was measured every 2 minutes during each loop.
- The medium workload opened up to five applications simultaneously.
- The type rate was 160 ms for each character.
- Approximately 2 minutes of idle time were included to simulate realworld users.

Each loop of the medium workload opened and used the following applications:

- Microsoft Outlook 2007 — Browsed 10 messages.
- Microsoft Internet Explorer — One instance was left open to BBC.co.uk, one instance browsed Wired.com, Lonelyplanet.com, and a heavy Flash application gettheglass.com (not used with MediumNoFlash workload).

<table>
<thead>
<tr>
<th>Profile characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk and RAID type for CIFS shares to host roaming user profiles, home directories, and XenApp profiles</td>
<td>RAID 6, 2 TB, 7200 rpm, 3.5” NL-SAS disks</td>
</tr>
<tr>
<td>Number of XenServer resource pools</td>
<td>2</td>
</tr>
<tr>
<td>Number of XenServer hosts per resource pool</td>
<td>8</td>
</tr>
<tr>
<td>Number of virtual machines per resource pool</td>
<td>500</td>
</tr>
</tbody>
</table>
Chapter 6: Testing and Validation

- Microsoft Word 2007 — One instance to measure the response time, and one instance to edit a document.
- Bullzip PDF Printer and Adobe Acrobat Reader — The Word document was printed, and the PDF was reviewed.
- Microsoft Excel 2007 — A very large sheet was opened and random operations were performed.
- Microsoft PowerPoint 2007 — A presentation was reviewed and edited.
- 7-zip — Using the command line version, the output of the session was zipped.

Login VSI launcher

A Login VSI launcher is a Windows system that launches desktop sessions on target virtual desktops. There is only one system running the VSI management console that manages all launchers and their sessions in a given test bed, and there can be as many launchers as required.

The number of desktop sessions a launcher can run is limited by CPU or memory resources. Login consultants recommend using a maximum of 45 sessions per launcher with two CPU cores (or two dedicated vCPUs) and 2 GB RAM, when the GDI limit is not tuned (default). With the GDI limit tuned, this limit extends to 60 sessions per two-core machine.

In this validated testing, 1,000 desktop sessions were launched from 32 launchers. There were around 32 sessions per launcher. Each launcher was allocated two vCPUs and 4 GB of RAM. There were no bottlenecks observed on the launchers during the VSI-based tests.

FAST Cache configuration

For all tests, FAST Cache was enabled for the storage pool holding eight storage repositories that were used to house the 1,000 desktops, and the storage pool holding the CIFS shares for user home directories, roaming profiles, and XenApp profiles.
Boot storm results

Test methodology
This test was conducted by executing a script on a XenServer that powers on a maximum of 50 virtual machines concurrently within the resource pool. Overlays are added to the graphs to show when the last power on task completed and when the IOPS to the pool LUNs achieved a steady state.

For the boot storm test, all the desktops were powered on within 27 minutes and achieved steady state approximately 3 minutes later. The total start-to-finish time for all desktops to register with the XenDesktop controllers was approximately 30 minutes. This section describes the boot storm results when powering on the desktop pools.

Pool individual disk load
Figure 47 shows the disk IOPS for a single SAS drive in the storage pool that stores the eight storage repositories for the virtual desktops. Each drive in the pool had similar statistics. Therefore, only a single drive result is reported for clarity and readability of the graph.

![Boot storm - Disk IOPS for a single SAS drive](image)

Figure 47. Boot storm - Disk IOPS for a single SAS drive

During peak load, the disk serviced a maximum of 127 IOPS. FAST Cache and Data Mover cache helped to reduce the disk load.
Figure 48 shows the LUN IOPS, and response time from one of the storage repositories. Each LUN had similar statistics. Therefore, only a single LUN result is reported for clarity and readability of the graph.

During peak load, the LUN response time did not exceed 3 ms and the storage repository serviced over 650 IOPS.

**Figure 48. Boot storm - LUN IOPS and response time**
Figure 49 shows the total IOPS serviced by the storage processor during the test.

![Storage processor IOPS Diagram]

**Figure 49.** Boot storm - Storage processor total IOPS
Figure 50 shows the storage processor utilization during the test. The pool-based LUNs were split across both SPs to balance the load equally.

Figure 50. Boot storm - Storage processor utilization

The virtual desktops generated high levels of I/O during the peak load of the boot storm test, while the SP utilization remained below 35 percent.
Figure 51 shows the IOPS serviced from FAST Cache during the test.

![FAST Cache IOPS](image)

**Figure 51. Boot storm - FAST Cache IOPS**

FAST Cache serviced over 11,000 IOPS from the storage repositories during peak load. The FAST Cache hits include IOPS serviced by Flash drives and SP memory cache. If memory cache hits are excluded, the pair of Flash drives alone serviced roughly 6,000 IOPS at peak load. A sizing exercise using EMC’s standard performance estimate (180 IOPS) for 15k rpm SAS drives suggests that it takes roughly 34 SAS drives to achieve the same level of performance.
Figure 52 shows the Data Mover CPU utilization during the boot storm test. The Data Mover achieved a CPU utilization of approximately 30 percent during peak load in this test.

Figure 52. Boot storm – Data Mover CPU utilization
Figure 53 shows the NFS operations per second on the Data Mover during the boot storm test. The Data Mover serviced nearly 20,000 IOPS for 1,000 desktops during peak load, yielding an average of 20 IOPS per desktop during boot storm.

![Graph showing NFS operations per second during boot storm](image)

**Figure 53.** Boot storm – Data Mover NFS load
Figure 54 shows the average NFS read/write response times reported by the server_stats command. These counters represent the response time for NFS read/write operations initiated to the storage array.

![Graph showing average NFS read/write response time](image)

**Figure 54. Boot storm – Data Mover NFS read/write response time**

The NFS read and write response time for the virtual desktops on the storage repositories was below 10 ms. This indicates excellent performance under this load.
Figure 55 shows the CPU load from the XenServers in the resource pools. Each server had similar statistics. Therefore, only a single server result is reported.

The XenServer achieved a CPU utilization of approximately 30 percent during peak load in this test. It should be noted that hyperthreading was enabled to double the number of logical CPUs.
Antivirus results

Test methodology  This test was conducted by scheduling a full scan of all desktops with a custom script using McAfee 8.7. The full scans were started on all the desktops over the course of 150 minutes. The total start-to-finish time was approximately 214 minutes.

Pool individual disk load  Figure 56 shows the disk I/O for a single SAS drive in the storage pool that housed the virtual desktops. Each drive in the pool had similar statistics. Therefore, only a single drive result is reported for clarity and readability of the graph.

![Figure 56. Antivirus - Disk I/O for a single SAS drive](image)

Although the individual drives in the pool serviced 231 IOPS during peak load, the disk response time was capped at 8 ms.
Figure 57 shows the LUN IOPS and response time from one of the storage repositories. Each LUN had similar statistics. Therefore, only a single LUN result is reported for clarity and readability of the graph.

During peak load, the LUN response time remained within 8 ms, and the storage repository serviced nearly 900 IOPS. The majority of the read I/O was served by the FAST Cache and not by the pool LUN.
Figure 58 shows the total IOPS serviced by the storage processor during the test.

The antivirus scan operations caused moderate CPU utilization during peak load. The load was shared between two SPs during the scan of each collection. The EMC VNX series has sufficient scalability headroom for this workload.
Figure 60 shows the IOPS serviced from FAST Cache during the test.

FAST Cache IOPS

FAST Cache serviced nearly 16,000 IOPS from the storage repositories during peak load. The FAST Cache hits include IOPS serviced by Flash drives and SP memory cache. If memory cache hits are excluded, the pair of Flash drives alone serviced almost all of the 16,000 IOPS at peak load. A sizing exercise using EMC’s standard performance estimate (180 IOPS) for 15k rpm SAS drives suggests that it takes roughly 89 SAS drives to achieve the same level of performance. However, EMC does not recommend using a 89:2 ratio for SAS to SSD replacement. EMC’s recommended ratio is 20:1 because workloads may vary.
Figure 61 shows the Data Mover CPU utilization during the antivirus scan test. The Data Mover achieved a CPU utilization of approximately 42 percent during peak load in this test.

Figure 62 shows the NFS operations per second from the Data Mover during the antivirus scan test. The Data Mover serviced nearly 24,000 IOPS for 1,000 desktops during peak load, yielding an average of 24 IOPS per desktop during this test.
Figure 62. Antivirus – Data Mover NFS load

Figure 63 shows the average NFS read/write response times reported by the server_stats command. These counters represent the response time for NFS read/write operations initiated to the storage array.

Figure 63. Antivirus - Data Mover NFS read/write response time

The peak NFS read and write response times for the virtual desktop storage never crossed 16 ms. The FAST Cache performed an enormous amount of read operations during this test.
Figure 64. Antivirus - XenServer CPU load

The CPU load on the XenServer was well within acceptable limits during this test. It should be noted that hyperthreading was enabled to double the number of logical CPUs.
Patch install results

Test methodology

This test was performed by pushing a security update to all desktops using Microsoft SCCM. The desktops were divided into five collections of 200 desktops each. The collections were configured to install updates in a 1-minute staggered schedule an hour after the patch was downloaded. All patches were installed within 10 minutes.

Pool individual disk load

Figure 65 shows the disk IOPS for a single SAS drive that is part of the storage pool. Each drive in the pool had similar statistics, so a single drive results are shown for clarity and readability of the graph.

![Figure 65. Patch install - Disk IOPS for a single SAS drive](image-url)

The drives did not get saturated during the patch download phase. During the patch installation phase, the disk serviced 289 IOPS at peak load while a response time spike of 16 ms was recorded within the 10-minute interval.
Figure 66 shows the LUN IOPS and response time from one of the storage repositories. Each LUN in the pool had similar statistics. Therefore, a single LUN results are shown for clarity and readability of the graph.

Figure 66. Patch install - LUN IOPS and response time

During peak load, the LUN response time was 5 ms, and the storage repository serviced nearly 800 IOPS.
Figure 67 shows the total IOPS serviced by the storage processor during the test.

![Graph showing storage processor IOPS](image)

**Figure 67. Patch install - Storage processor IOPS**

During peak load, the storage processors serviced over 16,000 IOPS. The load is shared between two SPs during the patch install operation on each collection of virtual desktops.
Figure 68 shows the storage processor utilization during the test.

The patch install operations caused moderate CPU utilization below 40% during peak load. The EMC VNX series has sufficient scalability headroom for this workload.
Figure 69 shows the IOPS serviced from FAST Cache during the test.

FAST Cache serviced nearly 10,000 IOPS from the storage repositories during peak load. The FAST Cache hits include IOPS serviced by Flash drives and SP memory cache. If memory cache hits are excluded, the pair of Flash drives alone serviced over 5,000 IOPS at peak load. A sizing exercise using EMC’s standard performance estimate (180 IOPS) for 15k rpm SAS drives suggests that it takes roughly 28 SAS drives to achieve the same level of performance.
**Chapter 6: Testing and Validation**

**Figure 70** shows the Data Mover CPU utilization during the patch install test. The Data Mover achieved a CPU utilization of approximately 31 percent during peak load in this test.

![Data Mover CPU utilization图](image)

**Figure 71** shows the NFS operations per second from the Data Mover during the patch install test. The Data Mover serviced over 16,000 IOPS for 1,000 desktops during peak load, yielding an average of 16 IOPS per desktop during patch install.

![Data Mover NFS load图](image)
Figure 72 shows the average NFS read/write response times reported by the server_stats command. These counters represent the response time for NFS read/write operations initiated to the storage array.

![Data Mover NFS response time](image)

**Figure 72. Patch install - Data Mover NFS read/write response time**

The NFS read and write response times for virtual desktop storage on the storage repositories were approximately 23 ms during peak load.
Figure 73 shows the CPU load from the XenServers in the resource pools. Each server had similar statistics. Therefore, only a single server results are shown for clarity and readability of the graph.

Figure 73.  Patch install - XenServer CPU load

The XenServer CPU load was well within the acceptable limits during the test. It should be noted that hyperthreading was enabled to double the number of logical CPUs.
Login VSI results

Test methodology
This test was conducted by scheduling 1,000 users to connect over Independent Computing Architecture (ICA) protocol in a 60-minute window, and starting the Login VSI-medium workload. The workload was run for one hour in a steady state to observe the load on the system.

Login VSI result summary
Login VSI version 3 introduces two methods of calculating the VSImax gating metric—VSImax Classic and VSImax Dynamic. VSImax Classic is based on the previous version of Login VSI, and is achieved when the average Login VSI response time is higher than a fixed threshold of 4,000 ms. This method proves to be reliable when no anti-virus or application virtualization is used.

Similar to VSImax Classic, VSI Dynamic is calculated when the response time is consistently above a certain threshold. However, this threshold is now dynamically calculated based on the average baseline response time of the first 15 Login VSI users on the system.

The formula for the dynamic threshold is:
average baseline response time × 125% + 3000.

As a result, if the baseline response time is 1800, the VSImax threshold will be 1800 x 125% + 3000 = 5250 ms.

When an application virtualization is used, the baseline response time varies significantly based on vendor and streaming strategy. Therefore, VSImax Dynamic is recommended when comparisons are made with application virtualization or anti-virus agents. When the baseline response time is relatively high, the VSImax Dynamic results are aligned again with saturation on a CPU, Memory, or Disk level.

This solution used VSImax Dynamic threshold because the XenApp application virtualization was used during the Login VSI test.
Figure 74 shows the response time in milliseconds compared to the number of active desktop sessions, as generated by the LoginVSI launchers. It shows that the average response time increases marginally as the user count increases. The VSLmax Dynamic threshold was not reached up to 1000 desktop users.
**Login storm timing**

To simulate a login storm, 1,000 desktops are powered on into a steady state by setting the idle desktop count to 1,000. The login time of each session is then measured by starting a LoginVSI test to establish the sessions with a custom interval of 3.6 seconds. The 1,000 sessions are logged in within 60 minutes, a period that models a burst of login activity occurring in the opening hour of a production environment.

The LoginVSI tool has a built-in login timer that measures the login time from the start of the logon script defined in the Active Directory group policy to the start of the LoginVSI workload for each session. Although it does not measure the total login time from an end-to-end user perspective, the measurement gives a good indication of how sessions will be affected in a login storm scenario.

*Figure 75* shows the trend of the login time in seconds as sessions started in rapid succession. The average login time for 1,000 sessions is approximately 4.7 seconds. The maximum login time is recorded at 7.3 seconds, while the minimum login time is 2 seconds.

This test results indicate that all users should receive their desktop sessions with a reasonable delay.

![Login Storm Timing](image-url)

*Figure 75. Login storm timing*
Figure 76 shows the disk IOPS from one of the storage repositories. Each disk had similar results, so only a single disk is reported for clarity and readability of the graph.

During peak load, the SAS disk serviced less than 160 IOPS and the disk response time was less than 7 ms.
Figure 77 shows the LUN IOPS and response time from one of the storage repositories. Each LUN had similar statistics. Therefore, only a single LUN result is reported for clarity and readability of the graph.

![Graph showing LUN IOPS and response time](image)

**Figure 77.  Login VSI - LUN IOPS and response time**

During peak load, the LUN response time remained under 3 ms and the storage repository serviced nearly 800 IOPS.
Figure 78 shows the total IOPS serviced by the storage processor during the test.

The storage processor peak utilization was below 35 percent during the logon storm. The load was shared between two SPs during the VSI load test.
Figure 80 shows the IOPS serviced from FAST Cache during the test.

The FAST Cache serviced over 11,000 IOPS from the storage repositories during peak load. The FAST Cache hits include IOPS serviced by Flash drives and SP memory cache. If memory cache hits are excluded, the pair of Flash drives alone serviced nearly 9,000 IOPS at peak load. A sizing exercise using EMC’s standard performance estimate (180 IOPS) for 15k rpm SAS drives suggests that it takes roughly 50 SAS drives to achieve the same level of performance. However, EMC does not recommend using a 50:2 (or 25:1) ratio for SAS to SSD replacement. EMC’s recommended ratio is 20:1 because workloads may vary.
**Figure 81.** Login VSI – Data Mover CPU utilization

The Data Mover achieved a CPU utilization of approximately 35 percent during peak load in this test.

**Figure 82.** Login VSI – Data Mover NFS load

The Data Mover serviced nearly 14,000 IOPS for 1,000 desktops during peak load, yielding an average of 14 IOPS per desktop during logon storm.
**Data Mover NFS response time**

Figure 83 shows the average NFS read/write response time reported by the server_stats command. These counters represent the response time for NFS read/write operations initiated to the storage array.

![Diagram](image)

**Figure 83. Login VSI - Data Mover NFS read/write response time**

The NFS read and write response time for the virtual desktops on the storage repositories was below 8 ms during the peak load.
Figure 84 shows the CPU load from the XenServers in the resource pools. A single server is reported because each server had similar results.

Figure 84. Login VSI - XenServer CPU load

The XenServer briefly achieved a CPU utilization of approximately 98 percent during peak load in this test. It should be noted that hyperthreading was enabled to double the number of logical CPUs.
FAST Cache benefits

Case study

To illustrate the benefits of enabling FAST Cache in a desktop virtualization environment, a study was conducted to compare performance with and without FAST Cache configuration. The non-FAST Cache configuration called for 60 SAS drives in a storage pool. The FAST Cache configuration called for 30 SAS drives backed by FAST Cache with 2 Flash drives, displacing 30 SAS drives from the non-FAST Cache configuration for a 15:1 ratio of drive savings. The following summary graphs demonstrate how FAST Cache benefits are realized in each use case.

Figure 85 shows that the antivirus scan is completed in 214 minutes with FAST Cache enabled, compared to 342 minutes without FAST Cache. With FAST Cache enabled, the overall scan time was reduced by roughly 35%, and the response time was reduced by 30%.

Figure 85. Antivirus scan – scan time comparison
Figure 86 shows that the peak NFS response time during patch storm for non-FAST Cache configuration is roughly 1.4 times higher than that of FAST Cache configuration.

Figure 86. Patch storm – NFS write latency comparison
Chapter 7: Conclusion

7 Conclusion

This chapter summarizes the test results of this solution and includes the following sections:

- Summary
- References

Summary

As shown in Chapter 6 Testing and Validation, EMC VNX FAST Cache provides measurable benefits in a desktop virtualization environment. It not only reduces response time for both read and write workloads, it effectively supports more users on fewer drives, and greater IOPS density with a lower drive requirement.

References

The following documents, located on the EMC Online Support website, provide additional and relevant information. Access to these documents depends on the user’s login credentials. Users who do not have access to a document should contact an EMC representative:

- **EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (NFS), Cisco UCS, VMware vSphere 4.1, and Citrix XenDesktop 5—Reference Architecture**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (NFS), Cisco UCS, VMware vSphere 4.1, and Citrix XenDesktop 5—Proven Solution Guide**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (FC), VMware vSphere 4.1, and Citrix XenDesktop 5—Reference Architecture**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (FC), VMware vSphere 4.1, and Citrix XenDesktop 5—Proven Solution Guide**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC Celerra Unified Storage (NFS), VMware vSphere 4, and Citrix XenDesktop 4—Reference Architecture**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC Celerra Unified Storage (NFS), VMware vSphere 4, and Citrix XenDesktop 4—Proven Solution Guide**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC Unified Storage (FC), Microsoft Windows Server 2008 R2 Hyper-V, and Citrix XenDesktop 4—Reference Architecture**
- **EMC Infrastructure for Virtual Desktops Enabled by EMC Unified Storage (FC), Microsoft Windows Server 2008 R2 Hyper-V, and Citrix XenDesktop 4—Proven Solution Guide**
Chapter 7: Conclusion

- *EMC Performance Optimization for Microsoft Windows XP for the Virtual Desktop Infrastructure—Applied Best Practices*
- *Deploying Microsoft Windows 7 Virtual Desktops with VMware View—Applied Best Practices Guide*
- *EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (NFS), VMware vSphere 4.1, VMware View 4.6 and VMware View Composer 2.6—Reference Architecture*
- *EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (NFS), VMware vSphere 4.1, VMware View 4.6 and VMware View Composer 2.6—Proven Solution Guide*

The following documents are available at [www.Citrix.com](http://www.Citrix.com) and [www.Cisco.com](http://www.Cisco.com):

- Citrix eDocs (Documentation Library)
- Cisco Unified Computing System