TABLE OF CONTENTS

1 Executive Summary........................................................................................................... 8
   1.1 Reference Architecture Objectives............................................................................... 9
   1.2 Solution Overview ...................................................................................................... 10

2 Introduction ......................................................................................................................... 12
   2.1 Document Overview .................................................................................................. 12
   2.2 NetApp All-Flash FAS Overview ............................................................................... 12
   2.3 Citrix XenDesktop .................................................................................................... 18
   2.4 Login VSI ................................................................................................................. 23

3 Solution Infrastructure ......................................................................................................... 24
   3.1 Hardware Infrastructure ............................................................................................ 25
   3.2 Software Components ............................................................................................... 26
   3.3 VMware vSphere 5.5 ............................................................................................... 27
   3.4 NetApp Virtual Storage Console ............................................................................... 28
   3.5 Virtual Desktop vDisk .............................................................................................. 29
   3.6 Full-Clone Virtual Desktops ...................................................................................... 31
   3.7 Login VSI Server ..................................................................................................... 32
   3.8 Login VSI Launcher VM ........................................................................................... 34
   3.9 Microsoft Windows Infrastructure VM ...................................................................... 34

4 Storage Design ..................................................................................................................... 35
   4.1 Storage Design Overview .......................................................................................... 35
   4.2 Aggregate Layout ..................................................................................................... 35
   4.3 Volume Layout ......................................................................................................... 36
   4.4 NetApp Virtual Storage Console for VMware vSphere ........................................... 37

5 Network Design .................................................................................................................... 38
   5.1 Network Switching .................................................................................................... 38
   5.2 Host Server Networking ........................................................................................... 38
   5.3 Storage Networking .................................................................................................. 39

6 Citrix XenDesktop Design .................................................................................................. 39
   6.1 Overview ................................................................................................................ 39
   6.2 XenDesktop Storage Design .................................................................................... 39

7 Login VSI Workload ............................................................................................................ 40
   7.1 Login VSI Components ............................................................................................ 40
8 Testing and Validation: Nonpersistent Provisioning Server Desktops ................. 42
  8.1 Overview ........................................................................................................... 43
  8.2 Test Results Overview ..................................................................................... 45
  8.3 Storage Efficiency ............................................................................................ 46
  8.4 Provisioning 1,000 VDI Desktops .................................................................... 46
  8.5 Boot Storm Test ............................................................................................... 48
  8.6 Login, Steady State, and Logout (Login VSI Test) with Mandatory Profiles ........................................ 51
  8.7 Login, Steady State, and Logoff (Login VSI Test) with Roaming Profiles .......... 54

9 Testing and Validation: Persistent Full-Clone Desktops ..................................... 57
  9.1 Overview ........................................................................................................... 57
  9.2 Test Results Overview ..................................................................................... 59
  9.3 Storage Efficiency ............................................................................................ 59
  9.4 Test for Provisioning 2,000 Citrix XenDesktop Full Clones (Offloaded to VAAI) .................. 60
  9.5 Boot Storm Test Using vCenter ........................................................................ 62
  9.6 Boot Storm Test Using vCenter During Storage Failover .................................... 65
  9.7 Steady-State Login VSI Test ............................................................................. 68
  9.8 Unthrottled Virus Scan Test ............................................................................ 83
  9.9 Throttled Virus Scan Test ................................................................................. 86
  9.10 Test for Patching 1,000 Desktops on One Node ............................................... 88
  9.11 Test for Aggressive Deduplication While Patching 2,000 Desktops .................. 91

10 Additional Reference Architecture Testing ....................................................... 93
  10.1 Always-On Deduplication ............................................................................... 94
  10.2 Inline Zero Detection and Elimination in Data ONTAP 8.3 .............................. 96
  10.3 Advanced Drive Partitioning .......................................................................... 96

11 Conclusion ........................................................................................................... 96

12 References .......................................................................................................... 97

13 Acknowledgements ............................................................................................. 97

LIST OF TABLES
Table 1) Persistent desktop test results ................................................................. 10
Table 2) Persistent desktop test results ................................................................. 11
Table 3) All-Flash FAS8000 storage system technical specifications .................. 13
Table 4) Citrix XenDesktop VM configuration ...................................................... 21
Table 5) Citrix Provisioning Server VM configuration ........................................... 21
Table 6) Citrix Licensing Server VM configuration ................................................................. 22
Table 7) Citrix StoreFront Server VM configuration ............................................................... 22
Table 8) SQL Server VM configuration ..................................................................................... 23
Table 9) Hardware components of server categories .............................................................. 25
Table 10) Solution software components ............................................................................... 26
Table 11) VMware vCenter Server VM configuration .............................................................. 27
Table 12) Microsoft SQL Server database VM configuration .................................................... 28
Table 13) NetApp VSC VM configuration ............................................................................... 28
Table 14) vDisk configuration ................................................................................................. 30
Table 15) HSD vDisk configuration .......................................................................................... 30
Table 16) HSD and VDI installed software ............................................................................... 30
Table 17) Virtual desktop configuration .................................................................................. 31
Table 18) Login VSI server configuration ............................................................................... 33
Table 19) Login VSI launcher VM configuration ..................................................................... 34
Table 20) Windows infrastructure VM .................................................................................... 34
Table 21) Test results overview .............................................................................................. 45
Table 22) Results for provisioning 167 VDI desktops ............................................................... 47
Table 23) Results for 1,000-VDI desktop boot storm .............................................................. 49
Table 24) Power-on method, storage latency, and boot time .................................................. 51
Table 25) Results for 2,000 users during Login VSI initial login and workload ......................... 52
Table 26) Results for 2,000-user XenDesktop VSI initial login and workload ......................... 55
Table 27) Test results overview .............................................................................................. 59
Table 28) Efficiency results ..................................................................................................... 60
Table 29) Results for full-clone provisioning of 2,000 virtual desktops ..................................... 61
Table 30) Results for full-clone boot storm ............................................................................ 63
Table 31) Power-on method, storage latency, and boot time .................................................. 65
Table 32) Results for full-clone boot storm during storage failover ......................................... 66
Table 33) Power-on method, storage latency, and boot time .................................................. 68
Table 34) Results for full-clone Monday morning login and workload .................................... 69
Table 35) Results for full-clone Monday morning login and workload during storage failover .......................................................................................................................... 72
Table 36) Results for full-clone Tuesday morning login and workload .................................... 76
Table 37) Results for full-clone Tuesday morning login and workload during storage failover .......................................................................................................................... 79
Table 38) Results for persistent full-clone unthrottled virus scan operation ......................... 83
Table 39) Results for persistent full-clone throttled virus scan operation ............................... 86
Table 40) Results for patching 1,000 persistent full clones on one node ................................. 89
Table 41) Results for aggressively deduplicating and patching 2,000 persistent full clones on one node .......................................................... 91
Table 42) Disk types and protocols ......................................................................................... 96
LIST OF FIGURES

Figure 1) Nonpersistent and persistent desktop use cases .............................................................................. 9
Figure 2) Clustered Data ONTAP ......................................................................................................................... 14
Figure 3) Conceptual architecture of Citrix XenDesktop five-layer virtual desktop model (graphic supplied by Citrix). 20
Figure 4) Solution infrastructure for nonpersistent desktops .............................................................................. 24
Figure 5) Solution infrastructure for persistent desktops ...................................................................................... 25
Figure 6) Setting uuid.action in vmx file with Windows PowerShell. ................................................................. 32
Figure 7) VMware OS optimization tool. ............................................................................................................. 32
Figure 8) Login VSI launcher configuration. ......................................................................................................... 33
Figure 9) Multipath HA to DS2246 shelves of SSD ............................................................................................ 35
Figure 10) SSD layout. ......................................................................................................................................... 35
Figure 11) Volume layout for nonpersistent desktops. ............................................................................................ 36
Figure 12) Volume layout for persistent desktops. ................................................................................................. 37
Figure 13) Network topology of storage to server. ................................................................................................. 38
Figure 14) Recommended storage architecture for deploying desktops with Citrix PVS provisioning method. ...... 40
Figure 15) Login VSI components. ..................................................................................................................... 41
Figure 16) Desktop-to-launcher relationship. ......................................................................................................... 42
Figure 17) Decision points of nonpersistent pooled desktops and profile types. .................................................. 45
Figure 18) Throughput, IOPS, and latency for creation of 1,000 VDI desktops. .................................................. 47
Figure 19) I/O read/write ratio during VDI desktop creation. ............................................................................... 48
Figure 20) Throughput, IOPS, and latency for 1,000-VDI desktop boot storm. .................................................. 49
Figure 21) Storage controller CPU utilization for 1,000-VDI desktop boot storm. ............................................. 50
Figure 22) Read/write IOPS for 1,000-VDI desktop boot storm. ......................................................................... 50
Figure 23) VSImax results for PVS Login VSI initial login and workload ........................................................... 52
Figure 24) Throughput, IOPS, and latency for 2,000-user XenDesktop Login VSI initial login and workload. ....... 53
Figure 25) Storage controller CPU utilization for 2,000-user XenDesktop Login VSI initial login and workload. .... 53
Figure 26) Read/write IOPS for 2,000-user XenDesktop PVS write cache volume Login VSI initial login and workload. 54
Figure 27) Scatterplot for PVS Login VSI login times. .......................................................................................... 55
Figure 28) Throughput, IOPS, and latency for 2,000-user XenDesktop Login VSI initial login and workload .......... 56
Figure 29) Storage controller CPU utilization for 2,000-user XenDesktop desktops Login VSI initial login and workload. 57
Figure 30) XenDesktop machine catalog setup wizard ...................................................................................... 58
Figure 31) XenDesktop machine catalog setup wizard ...................................................................................... 58
Figure 32) Storage-efficiency savings .................................................................................................................. 60
Figure 33) Throughput, IOPS, and latency for full-clone creation. ...................................................................... 61
Figure 34) Storage controller CPU utilization for full-clone creation. .................................................................. 62
Figure 35) Throughput and IOPS for full-clone boot storm. .................................................................................. 63
Figure 36) Storage controller CPU utilization for full-clone boot storm. .............................................................. 64
Figure 37) Read/write IOPS for full-clone boot storm. .......................................................................................... 64
Figure 38) Read/write ratio for full-clone boot storm. .......................................................................................... 65
Figure 39) Throughput, IOPS, and latency for full-clone boot storm during storage failover ................................. 66
Figure 40) Storage controller CPU utilization for full-clone boot storm during storage failover ...................................................... 67
Figure 41) Read/write IOPS for full-clone boot storm during storage failover ................................................................. 67
Figure 42) Read/write ratio for full-clone boot storm during storage failover ................................................................. 67
Figure 43) VSImax results for full-clone Monday morning login and workload ................................................................. 68
Figure 44) Scatterplot of full-clone Monday morning login times ................................................................. 70
Figure 45) Throughput, IOPS, and latency for full-clone Monday morning login and workload ................................................................. 70
Figure 46) Storage controller CPU utilization for full-clone Monday morning login and workload ................................................................. 71
Figure 47) Read/write IOPS for full-clone Monday morning login and workload ................................................................. 71
Figure 48) Read/write ratio for full-clone Monday morning login and workload ................................................................. 72
Figure 49) VSImax results for full-clone Monday morning login and workload during storage failover ...................................... 73
Figure 50) Scatterplot of full-clone Monday morning login times during storage failover ................................................................. 73
Figure 51) Throughput, IOPS, and latency for full-clone Monday morning login and workload during storage failover 74
Figure 52) Storage controller CPU utilization for full-clone Monday morning login and workload during storage failover ................................................................. 74
Figure 53) Read/write IOPS for full-clone Monday morning login and workload during storage failover ...................... 75
Figure 54) Read/write ratio for full-clone Monday morning login and workload during storage failover ................................. 75
Figure 55) VSImax results for full-clone Tuesday morning login and workload ................................................................. 76
Figure 56) Scatterplot of full-clone Tuesday morning login times ................................................................. 77
Figure 57) Throughput, IOPS, and latency for full-clone Tuesday morning login and workload ................................................................. 77
Figure 58) Storage controller CPU utilization for full-clone Tuesday morning login and workload ................................................................. 78
Figure 59) Read/write IOPS for full-clone Tuesday morning login and workload ................................................................. 78
Figure 60) Read/write ratio for full-clone Tuesday morning login and workload ................................................................. 79
Figure 61) VSImax results for full-clone Tuesday morning login and workload during storage failover ................................................................. 80
Figure 62) Scatterplot of full-clone Tuesday morning login times during storage failover ................................................................. 80
Figure 63) Throughput, IOPS, and latency for full-clone Tuesday morning login and workload during storage failover 81
Figure 64) Storage controller CPU utilization for full-clone Tuesday morning login and workload during storage failover ................................................................. 81
Figure 65) Read/write IOPS for full-clone Tuesday morning login and workload during storage failover ...................... 82
Figure 66) Read/write ratio for full-clone Tuesday morning login and workload during storage failover ................................. 82
Figure 67) Script for starting virus scan on all VMs ............................................................................................................. 83
Figure 68) Throughput, IOPS, and latency for unthrottled virus scan operations ................................................................. 84
Figure 69) Storage controller CPU utilization for full-clone unthrottled virus scan operation ................................................................. 84
Figure 70) Read/write IOPS for full-clone unthrottled virus scan operation ................................................................. 84
Figure 71) Read/write ratio for full-clone unthrottled virus scan operation ................................................................. 85
Figure 72) Virus scan script ........................................................................................................................................... 86
Figure 73) Throughput, IOPS, and latency for throttled virus scan operations ................................................................. 87
Figure 74) Storage controller CPU utilization for full-clone throttled virus scan operation ................................................................. 87
Figure 75) Read/write IOPS for full-clone throttled virus scan operation ................................................................. 88
Figure 76) Read/write ratio for full-clone throttled virus scan operation ................................................................. 88
Figure 77) Throughput, IOPS, and latency for patching 1,000 persistent full clones on one node. .......................... 89
Figure 78) Storage controller CPU utilization for patching 1,000 persistent full clones on one node. .......................... 90
Figure 79) Read/write IOPS for patching 1,000 persistent full clones on one node. ........................................... 90
Figure 80) Read/write ratio for patching 1,000 persistent full clones on one node. ............................................. 91
Figure 81) Throughput, IOPS, and latency for aggressively deduplicating and patching 2,000 persistent full clones on one node. .......................................................... 91
Figure 82) Storage controller CPU utilization for aggressively deduplicating and patching 2,000 persistent full clones on one node. ................................................................. 92
Figure 83) Read/write IOPS for aggressively deduplicating and patching 2,000 persistent full clones on one node. .... 93
Figure 84) Read/write ratio for aggressively deduplicating and patching 2,000 persistent full clones on one node. .... 93
Figure 85) Configuring efficiency policy for always-on deduplication. ................................................................. 94
Figure 86) Always-on deduplication storage efficiency over time. ........................................................................ 95
Figure 87) Always-on deduplication latency. ........................................................................................................ 95
1 Executive Summary

The decision to virtualize desktops affects multiple aspects of an IT organization, including infrastructure and storage requirements, application delivery, end-user devices, and technical support. In addition, correctly architecting, deploying, and managing a virtual desktop infrastructure (VDI) can be challenging because of the large number of solution components in the architecture. Therefore, it is critical to build the solution on industry-proven platforms such as NetApp® storage and FlexPod® converged infrastructure, along with industry-proven software solutions from Citrix. Citrix and NetApp provide leading desktop virtualization and storage solutions, respectively, for customers to successfully meet these challenges and gain the numerous benefits available from a desktop virtualization solution, such as workspace mobility, centralized management, consolidated and secure delivery of data, and device independence.

New products are constantly being introduced that promise to solve all virtual desktop challenges of performance, cost, or complexity. Each new product introduces more choices, complexities, and risks to your business in an already complicated solution. NetApp, founded in 1993, has been delivering enterprise-class storage solutions for virtual desktops since 2006, and it offers real answers to these problems.

The criteria for determining the success of a virtual desktop implementation must include end-user experience. The end-user experience must be as good as or better than any previous experience on a physical PC or virtual desktop.

Citrix XenDesktop now has XenApp built in, and it can deliver full desktops or just applications to any mobile device. The Citrix XenDesktop 7.5 system incorporates traditional hosted virtual Windows® 7 or Windows 8 desktops, hosted applications, and hosted shared Windows Server® 2008 R2 or Windows Server 2012 R2 server desktops. Advancements in Citrix XenDesktop 7.5 provide unparalleled scale and management simplicity while extending the Citrix high-definition user experience (HDX) technologies and FlexCast models to additional mobile devices.

As a workload, desktop virtualization is highly variable, and it imposes cycles of heavy reads, heavy writes, and everything in between, along with varying block sizes for writes. Therefore, it should be no surprise that storage is often the leading culprit of unmet end-user performance expectations. The NetApp All-Flash FAS solution with the FAS8000 platform easily handles highly variable desktop virtualization workloads to deliver an end-user experience that exceeds expectations.

Another criterion of project success is solution cost. Storage has often been the most expensive part of the virtual desktop solution, especially when storage efficiency and flash acceleration technologies were lacking. It was also common practice to forgo an assessment. Skipping this critical step meant that companies often overbought or undersized the storage infrastructure because information is the key to making sound architectural decisions that result in wise IT spending.

NetApp has many technologies that help customers reduce the storage cost of a virtual desktop solution. Technologies such as deduplication, thin provisioning, and compression help reduce the total amount of storage required for VDI. Storage platforms that scale up and scale out with the NetApp clustered Data ONTAP® operating system help deliver the right architecture to meet the customer’s price and performance requirements. NetApp can customers achieve their cost and performance goals while providing rich data management features.

With the NetApp All-Flash FAS solution, customers might pay as little as US$55 per desktop for storage when deploying at scale. This figure includes the cost of NetApp hardware, software, and three years of 24/7 premium support with 4-hour parts replacement. A similarly low ratio of dollars per desktop can be achieved with the AFF8020 and AFF8040 storage systems if the XenDesktop solution is employed for a smaller number of desktops.

With Citrix and NetApp, companies can accelerate the virtual desktop end-user experience by using NetApp All-Flash FAS storage for Citrix XenDesktop and XenApp. NetApp All-Flash FAS storage, powered by the FAS8000 system, is the optimal platform for using high-performing solid-state drives (SSDs) without adding risk to desktop virtualization initiatives.
When a storage failure prevents users from working, that inactivity translates into lost revenue and productivity. That is why what used to be considered a tier 3 or 4 application is now critical to business operations. Having a storage system with a robust set of data management and availability features is key to keeping the users working and lessens the risk to the business. Clustered Data ONTAP has multiple built-in features to help improve availability, such as active-active high availability (HA) and nondisruptive operations to seamlessly move data in the storage cluster without user impact.

NetApp also provides the ability to easily increase storage system capacity by simply adding disks or shelves. There is no need to purchase additional controllers in order to add users when additional capacity is required. When the platform requires expansion, additional nodes can be added in a scale-out fashion and managed within the same management framework and interface. Workloads can then be nondisruptively migrated or balanced to the new nodes in the cluster without the users ever noticing.

### 1.1 Reference Architecture Objectives

In this reference architecture, NetApp and Citrix validated multiple desktop deployment use cases at scale:

- In the first deployment scenario, we validated 2,000 nonpersistent desktops with a Citrix XenDesktop–hosted VDI and XenApp-hosted shared desktop workloads.
- In the second deployment scenario, we validated 2,000 persistent desktops with NetApp full-clone desktops that were cloned by using VMware® vStorage APIs for Array Integration (VAAI).

In both of these scenarios, we were able to demonstrate that, regardless of the deployment use case, the NetApp All-Flash FAS solution can eliminate the most common barriers to virtual desktop adoption, especially the concern about high storage costs.

The testing covered common administrative tasks on 2,000 desktops (or on 4,000 desktops when tests were performed in a storage controller failed-over state). Including tasks such as mass virtual machine (VM) provisioning, boot storms, login storms, and steady-state operations made it possible to understand time to complete, storage response, and storage utilization. For the persistent desktop use case, we also tested virus scanning and patching of 2,000 desktops at the same time with the intent of understanding the time to complete the operation, storage response, and storage utilization.

Figure 1 shows the high-level overview of use cases for both nonpersistent and persistent desktops that were validated in this reference architecture.

**Figure 1) Nonpersistent and persistent desktop use cases.**
1.2 Solution Overview

The reference architecture described in this document is based on Citrix XenDesktop 7.5, Citrix Provisioning Server 7.1, and VMware vSphere® 5.5.

Nonpersistent Desktops Use Case

The setup for the nonpersistent test was used to host, provision, and run 1,000 VDI users based on Windows 7 virtual desktops and 1,000 XenApp users based on 36 Windows 2012 R2 servers. This test simulated a typical customer deployment with mixed VDI and XenApp users. The 2,000 users were hosted by a two-node NetApp All-Flash FAS8060 active-active storage system running the NetApp Data ONTAP 8.2.2 operating system (OS) configured with 36 400GB SSDs. The entire workload was contained on one storage node.

Persistent Desktop Use Case

The same setup was used to test 2,000 persistent desktop users on 2,000 VAAI full clones. The 2,000 users were hosted by a two-node NetApp All-Flash FAS8060 active-active storage system running the NetApp Data ONTAP 8.2.2 OS configured with 36 400GB SSDs. The entire workload was handled on two storage nodes.

Twelve Fibre Channel (FC) datastores were presented from the NetApp system to the VMware ESXi™ hosts for use by the desktops. A pair of Cisco Nexus® 5000 switches were used as the access layer, and 18 Cisco Unified Computing System™ (Cisco UCS®) B200 servers were used as the computing layer (16 for desktop servers and 2 for infrastructure servers). Host-to-host communication took place over a 10GbE network through VMware virtual network adapters. VMs were used for core infrastructure components such as Microsoft® Active Directory®, database servers, and other services.

In all tests, end-user login time, guest response time, and maintenance activities performance were excellent. The NetApp All-Flash FAS system performed well, averaging less than 50% controller utilization during most operations for both use cases. All test categories demonstrated that, based on the 2,000-user workload and maintenance operations, the All-Flash FAS8060 system should be capable of doubling the workload to 4,000 users while still being able to fail over in the event of a failure. At a density of 4,000 VMs on an All-Flash FAS8060 system with the same I/O profile, storage for VDI might be as low as US$55 per desktop. This figure includes the cost of hardware, software, and three years of 24/7 premium support with 4-hour parts replacement. Similar storage cost per desktop numbers can be achieved with FAS8020-based and FAS8040-based solutions if the requirement is lower than 4,000 desktops.

Table 1 lists the results obtained during testing for 2,000 nonpersistent users.

Table 1) Persistent desktop test results.

<table>
<thead>
<tr>
<th>Time to Complete</th>
<th>Peak IOPS</th>
<th>Average IOPS</th>
<th>Peak Throughput (MB/sec)</th>
<th>Average Throughput (MB/sec)</th>
<th>Peak Storage Latency (ms)</th>
<th>Average Storage Latency</th>
<th>Peak CPU</th>
<th>Average CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot storm test (VMware vCenter™ power-on operations, VM registered in XenDesktop)</td>
<td>8 min, 13 sec</td>
<td>9,516</td>
<td>7,463</td>
<td>116.00</td>
<td>73.00</td>
<td>0.426</td>
<td>0.406</td>
<td>10%</td>
</tr>
<tr>
<td>Boot storm test (XenDesktop power-on operations)</td>
<td>25 min, 8 sec</td>
<td>7,929</td>
<td>3,614</td>
<td>88.50</td>
<td>54.60</td>
<td>0.508</td>
<td>0.448</td>
<td>8.9%</td>
</tr>
<tr>
<td>Initial login test with mandatory profile</td>
<td>30 min (configured in Login VSI)</td>
<td>27,280</td>
<td>18,516</td>
<td>422</td>
<td>267</td>
<td>0.678</td>
<td>0.548</td>
<td>79%</td>
</tr>
</tbody>
</table>
Table 2 lists the results obtained during testing for 2,000 persistent desktops.

Table 2) Persistent desktop test results.

<table>
<thead>
<tr>
<th>Test</th>
<th>Time to Complete</th>
<th>Peak IOPS</th>
<th>Peak Throughput</th>
<th>Average Storage Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning 2,000 desktops</td>
<td>139 min</td>
<td>52,709</td>
<td>1.3GB/sec</td>
<td>0.936ms</td>
</tr>
<tr>
<td>Boot storm test (VMware vCenter power-on operations)</td>
<td>6 min, 34 sec</td>
<td>144,288</td>
<td>5.2GB/sec</td>
<td>12.696ms</td>
</tr>
<tr>
<td>Boot storm test during storage failover (VMware vCenter power-on operations)</td>
<td>&lt;12 min</td>
<td>66,456</td>
<td>1.9GB/sec</td>
<td>15.011ms</td>
</tr>
<tr>
<td>Boot storm test (50 Citrix XenDesktop concurrent power-on operations)</td>
<td>10 min, 5 sec</td>
<td>83,414</td>
<td>3.2GB/sec</td>
<td>1.768ms</td>
</tr>
<tr>
<td>Boot storm test during storage failover (50 Citrix XenDesktop concurrent power-on operations)</td>
<td>10 min, 3 sec</td>
<td>65,564</td>
<td>1.81GB/sec</td>
<td>1.578ms</td>
</tr>
<tr>
<td>Login VSI Monday morning login and workload</td>
<td>8.56 sec/VM</td>
<td>21,268</td>
<td>0.7GB/sec</td>
<td>0.650ms</td>
</tr>
<tr>
<td>Login VSI Monday morning login and workload during failover</td>
<td>8.48 sec/VM</td>
<td>20,811</td>
<td>0.7GB/sec</td>
<td>0.762ms</td>
</tr>
<tr>
<td>Login VSI Tuesday morning login and workload</td>
<td>6.95 sec/VM</td>
<td>10,428</td>
<td>0.5GB/sec</td>
<td>0.683ms</td>
</tr>
<tr>
<td>Login VSI Tuesday morning login and workload during failover</td>
<td>8.67 sec/VM</td>
<td>10,848</td>
<td>0.5GB/sec</td>
<td>0.830ms</td>
</tr>
<tr>
<td>Virus scan of 2,000 desktops (un throttled)</td>
<td>~51 min</td>
<td>145,605</td>
<td>6.0GB/sec</td>
<td>7.5ms</td>
</tr>
<tr>
<td>Virus scan of 1,000 desktops on one node (throttled for 80 minutes)</td>
<td>~80 min</td>
<td>46,940</td>
<td>2.3GB/sec</td>
<td>1.1ms</td>
</tr>
<tr>
<td>Patching of 1,000 desktops on one node with 118MB of patches</td>
<td>~23 min</td>
<td>74,385</td>
<td>2.4GB/sec</td>
<td>14.8ms</td>
</tr>
<tr>
<td>Patching of 2,000 desktops on one node with 111MB of patches over a 164-minute period with a 5-minute deduplication schedule</td>
<td>164 min</td>
<td>17,979</td>
<td>0.4GB/sec</td>
<td>0.646ms</td>
</tr>
</tbody>
</table>
2 Introduction

This section provides an overview of the NetApp All-Flash FAS solution for Citrix XenDesktop, explains the purpose of this document, and introduces Login VSI.

2.1 Document Overview

This document describes the solution components used in the 2,000-user Citrix XenDesktop deployment validation on a NetApp All-Flash FAS reference architecture. It covers the hardware and software used in the validation, the configuration of the hardware and software, use cases that were tested, and performance results of the tests completed. During these performance tests, many different scenarios were tested to validate the performance of the storage during the lifecycle of a virtual desktop deployment.

For nonpersistent desktops, the testing included the following criteria:

- Boot storm test of 2,000 desktops, with 1,000 hosted VDI VMs and 36 hosted shared desktop (HSD) VMs (for XenApp users)
- Login VSI initial login and steady-state workload

For persistent desktops, the testing included the following criteria:

- Provisioning of 2,000 Citrix XenDesktop full-clone desktops to high-performing, space-efficient NetApp FlexClone® desktops by using VAAI cloning offload
- Boot storm test of 2,000 desktops (with and without storage node failover) by using VMware vCenter and Citrix XenDesktop
- Monday morning login and steady-state workload with Login VSI 4.1 RC3 (with and without storage node failover)
- Tuesday morning login and steady-state workload with Login VSI 4.1 RC3 (with and without storage node failover)
- Virus scan of all 2,000 desktops (unthrottled and throttled)
- Patching of all 1,000 desktops (unthrottled on one node with 118MB of patches)
- Patching of 2,000 desktops on one node with 111MB of patches over a 164-minute period with a 5-minute deduplication schedule

Note: In this document, Login VSI 4.1 RC3 is referred to as Login VSI 4.1.

Storage performance and end-user acceptance were the main focus of the testing. If a bottleneck occurred in any component of the infrastructure, it was identified and remediated if possible. During some of the tests for persistent desktops, such as patching and virus scan, no mechanisms were used to slow the events. Normal best practice would be to stagger patching and virus scanning during maintenance windows of a certain period of time. NetApp does not recommend running every virus scan and patch at the same time; nevertheless, latencies averaged those of spinning media during these events.

2.2 NetApp All-Flash FAS Overview

Built on more than 20 years of innovation, Data ONTAP has evolved to meet the changing needs of customers and help drive their success. Clustered Data ONTAP provides a rich set of data management features and clustering for scale-out, operational efficiency, and nondisruptive operations to offer customers one of the most compelling value propositions in the industry. The IT landscape is undergoing a fundamental shift to IT as a service, a model that requires a pool of compute, network, and storage to serve a wide range of applications and deliver a wide range of services. Innovations such as clustered Data ONTAP are fueling this revolution.

Outstanding Performance

The NetApp All-Flash FAS solution shares the same unified storage architecture, Data ONTAP OS, management interface, rich data services, and advanced features set as the rest of the fabric-attached storage
(FAS) product families. This unique combination of all-flash media with Data ONTAP delivers the consistent low latency and high IOPS of all-flash storage with the industry-leading clustered Data ONTAP OS. In addition, it offers proven enterprise availability, reliability, and scalability; storage efficiency proven in thousands of VDI deployments; unified storage with multiprotocol access; advanced data services; and operational agility through tight application integrations.

**All-Flash FAS8000 Technical Specifications**

Table 3 provides the technical specifications for the four All-Flash FAS8000 series storage systems: FAS8080 EX, FAS8060, FAS8040, and FAS8020.

**Note:** All data in Table 3 applies to active-active, dual-controller configurations.

Table 3) All-Flash FAS8000 storage system technical specifications.

<table>
<thead>
<tr>
<th>Features</th>
<th>FAS8080 EX</th>
<th>FAS8060</th>
<th>FAS8040</th>
<th>FAS8020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum raw capacity with SSDs</td>
<td>384TB</td>
<td>384TB</td>
<td>384TB</td>
<td>384TB</td>
</tr>
<tr>
<td>Maximum number of SSDs</td>
<td>240</td>
<td>240</td>
<td>240</td>
<td>240</td>
</tr>
<tr>
<td>Controller form factor</td>
<td>Two 6U chassis, each with 1 controller and an IOXM</td>
<td>Single-enclosure HA; 2 controllers in single 6U chassis</td>
<td>Single-enclosure HA; 2 controllers in single 6U chassis</td>
<td>Single-enclosure HA; 2 controllers in single 3U chassis</td>
</tr>
<tr>
<td>Memory</td>
<td>256GB</td>
<td>128GB</td>
<td>64GB</td>
<td>48GB</td>
</tr>
<tr>
<td>Maximum Flash Cache™</td>
<td>24TB</td>
<td>8TB</td>
<td>4TB</td>
<td>3TB</td>
</tr>
<tr>
<td>Maximum Flash Pool™</td>
<td>36TB</td>
<td>18TB</td>
<td>12TB</td>
<td>6TB</td>
</tr>
<tr>
<td>Combined flash total</td>
<td>36TB</td>
<td>18TB</td>
<td>12TB</td>
<td>6TB</td>
</tr>
<tr>
<td>NVRAM</td>
<td>32GB</td>
<td>16GB</td>
<td>16GB</td>
<td>8GB</td>
</tr>
<tr>
<td>PCIe expansion slots</td>
<td>24</td>
<td>8</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Onboard I/O: UTA2 (10GbE/FCoE, 16Gb FC)</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Onboard I/O: 10GbE</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Onboard I/O: GbE</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Onboard I/O: 6Gb SAS</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Optical SAS support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage networking supported</td>
<td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP</td>
<td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP</td>
<td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP</td>
<td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB, HTTP, FTP</td>
</tr>
<tr>
<td>OS version</td>
<td>FAS8080 EX Data ONTAP 8.2.2 RC1 or later, FAS8060, FAS8040, FAS8020 Data ONTAP 8.2.1 RC2 or later</td>
<td>FAS8080 EX Data ONTAP 8.2.2 RC1 or later, FAS8060, FAS8040, FAS8020 Data ONTAP 8.2.1 RC2 or later</td>
<td>FAS8080 EX Data ONTAP 8.2.2 RC1 or later, FAS8060, FAS8040, FAS8020 Data ONTAP 8.2.1 RC2 or later</td>
<td>FAS8080 EX Data ONTAP 8.2.2 RC1 or later, FAS8060, FAS8040, FAS8020 Data ONTAP 8.2.1 RC2 or later</td>
</tr>
</tbody>
</table>
Scale-Out

Data centers require agility. In a data center, each storage controller has CPU, memory, and disk shelf limits. Scale-out means that, as the storage environment grows, additional controllers can be added seamlessly to the resource pool residing on a shared storage infrastructure. Host and client connections, as well as datastores, can be moved seamlessly and nondisruptively anywhere in the resource pool.

The benefits of scale-out include the following:

- Nondisruptive operations
- Ability to keep adding thousands of users to the virtual desktop environment without downtime
- Operational simplicity and flexibility

As Figure 2 shows, clustered Data ONTAP offers a way to meet the scalability requirements in a storage environment. A clustered Data ONTAP system can scale up to 24 nodes, depending on platform and protocol, and can contain different disk types and controller models in the same storage cluster.

![Clustered Data ONTAP](image)

**Note:** Storage virtual machines (SVMs), referred to in Figure 2, were formerly called Vservers.

Nondisruptive Operations

The move to shared infrastructure has made it nearly impossible to schedule downtime to accomplish routine maintenance. NetApp clustered Data ONTAP is designed to eliminate the planned downtime needed for maintenance and lifecycle operations, as well as the unplanned downtime caused by hardware and software failures.

Three standard tools make this elimination of downtime possible:

- DataMotion™ for volumes (vol move) allows you to move data volumes from one aggregate to another on the same or a different cluster node.
- Logical interface (LIF) migrate allows you to virtualize the physical Ethernet interfaces in clustered Data ONTAP. LIF migrate lets you move LIFs from one network port to another on the same or a different cluster node.
- Aggregate relocate (ARL) allows you to transfer complete aggregates from one controller in an HA pair to the other without data movement.

Used individually and in combination, these tools offer the ability to nondisruptively perform a full range of operations, from moving a volume from a faster to a slower disk to performing a complete controller and storage technology refresh.
As storage nodes are added to the system, all physical resources—CPUs, cache memory, network I/O bandwidth, and disk I/O bandwidth—can easily be kept in balance. Clustered Data ONTAP 8.2.1 systems enable users to:

- Add or remove storage shelves (over 23PB in an 8-node cluster and up to 69PB in a 24-node cluster)
- Move data between storage controllers and tiers of storage without disrupting users and applications
- Dynamically assign, promote, and retire storage, while providing continuous access to data as administrators upgrade or replace storage

These capabilities allow administrators to increase capacity while balancing workloads and can reduce or eliminate storage I/O hot spots without the need to remount shares, modify client settings, or stop running applications.

**Availability**

A shared-storage infrastructure can provide services to thousands of virtual desktops. In such environments, downtime is not an option. The NetApp All-Flash FAS solution eliminates sources of downtime and protects critical data against disaster through two key features:

- **High availability (HA).** A NetApp HA pair provides seamless failover to its partner in case of any hardware failure. Each of the two identical storage controllers in the HA pair configuration serves data independently during normal operation. During an individual storage controller failure, the data service process is transferred from the failed storage controller to the surviving partner.
- **RAID DP®.** During any virtualized desktop deployment, data protection is critical because any RAID failure might disconnect hundreds to thousands of end users from their desktops, resulting in lost productivity. RAID DP provides performance comparable to that of RAID 10, yet it requires fewer disks to achieve equivalent protection. RAID DP provides protection against double disk failure, in contrast to RAID 5, which can protect against only one disk failure per RAID group, in effect providing RAID 10 performance and protection at a RAID 5 price point.

**Optimized Writes**

The NetApp WAFL® (Write Anywhere File Layout) file system enables NetApp to process writes efficiently. When the Data ONTAP OS receives an I/O, it holds the I/O in memory, protecting it with a log copy in battery-backed NVRAM, and sends back an acknowledgement (or ACK) to notify the sender that the write is committed. Acknowledging the write before writing to storage allows Data ONTAP to perform many functions to optimize the data layout for optimal write/write coalescing. Before being written to storage, I/Os are coalesced into larger blocks because larger sequential blocks require less CPU for each operation.

**Enhancing Flash**

Data ONTAP and FAS systems have leveraged flash technologies since 2009 and have supported SSDs since 2010. This relatively long experience in dealing with flash has allowed NetApp to tune Data ONTAP features to optimize SSD performance and enhance flash media endurance.

As described in the previous sections, because Data ONTAP acknowledges writes after they are in DRAM and logged to NVRAM, SSDs are not in the critical write path. Therefore, write latencies are very low. Data ONTAP also enables efficient use of SSDs when destaging write memory buffers by coalescing writes into a single sequential stripe across all SSDs at once. Data ONTAP writes to free space whenever possible, minimizing overwrites for every dataset, not only for deduplicated or compressed data.

This wear-leveling feature of Data ONTAP is native to the architecture, and it also leverages the wear-leveling and garbage-collection algorithms built into the SSDs to extend the life of the devices. Therefore, NetApp provides up to a five-year warranty with all SSDs (a three-year standard warranty, plus the offer of an additional two-year extended warranty, with no restrictions on the number of drive writes).
The parallelism built into Data ONTAP, combined with the multicore CPUs and large system memories in the FAS8000 storage controllers, takes full advantage of SSD performance and has powered the test results described in this document.

Advanced Data Management Capabilities

This section describes the storage efficiencies, multiprotocol support, VMware integrations, and replication capabilities of the NetApp All-Flash FAS solution.

Storage Efficiencies

Most desktop virtualization implementations deploy thousands of desktops from a small number of golden VM images, resulting in large amounts of duplicate data. This is especially the case with the VM operating system.

The NetApp All-Flash FAS solution includes built-in thin provisioning, data deduplication, compression, and zero-cost cloning with FlexClone technology that offers multilevel storage efficiency across virtual desktop data, installed applications, and user data. The comprehensive storage efficiency enables a significantly reduced storage footprint for virtualized desktop implementations, with a capacity reduction of up to 10:1, or 90% (based on existing customer deployments and NetApp solutions lab validation). The following features make this storage efficiency possible:

- **Thin provisioning** allows multiple applications to share a single pool of on-demand storage, eliminating the need to provision more storage for one application while another application still has plenty of allocated but unused storage.

- **Deduplication** saves space on primary storage by removing redundant copies of blocks in a volume that hosts hundreds of virtual desktops. This process is transparent to the application and the user, and it can be enabled and disabled on the fly. To eliminate any potential concerns about postprocess deduplication causing additional wear on the SSDs, NetApp provides up to a five-year warranty with all SSDs (a three-year standard warranty, plus the offer of an additional two-year extended warranty, with no restrictions on the number of drive writes).

- **FlexClone** technology offers hardware-assisted rapid creation of space-efficient, writable, point-in-time images of individual VM files, LUNs, or flexible volumes. It is fully integrated with VMware VAAI and Microsoft offloaded data transfer (ODX). The use of FlexClone technology in VDI deployments provides high levels of scalability and significant cost, space, and time savings. Both file-level and volume-level cloning are tightly integrated with the VMware vCenter Server™ through the NetApp VSC Provisioning and Cloning vCenter plug-in and native VM cloning offload with VMware VAAI and Microsoft ODX. NetApp Virtual Storage Console (VSC) provides the flexibility to rapidly provision and redeploy thousands of VMs with hundreds of VMs in each datastore.

- **Inline zero elimination** saves space and improves performance by not writing zeroes. This feature is available in Data ONTAP 8.3. It increases performance by eliminating the zero write to disk, improves storage efficiency by eliminating the need to postprocess deduplicate the zeroes, improves cloning time for eager zero thick disk files, eliminates the zeroing of VMDKs that require zeroing prior to data write, and thus increases SSD life expectancy.

- **Inline compression** saves space by compressing data as it is coming into the storage controller. Inline compression can be beneficial for many of the different data types that compose a virtual desktop environment. Each of these different data types has different capacity and performance requirements, so some data types might be more suited for inline compression than others. Using inline compression and deduplication together can significantly increase storage efficiency over using each alone.

- **Advanced drive partitioning** distributes the root file system across multiple disks in a HA pair. It allows for higher overall capacity utilization by removing the need for dedicated root and spare disks. This feature is available in Data ONTAP 8.3.
Multiprotocol Support

By supporting all common NAS and SAN protocols on a single platform, NetApp unified storage enables:

- Direct access to storage by each client
- Network file sharing across different platforms without the need for protocol-emulation products such as SAMBA, NFS Maestro, or PC-NFS
- Simple and fast data storage and data access for all client systems
- Fewer storage systems
- Greater efficiency from each system deployed

Clustered Data ONTAP can support several protocols concurrently in the same storage system. The Data ONTAP 7G and 7-Mode versions also include support for multiple protocols. Unified storage is important to Citrix XenDesktop solutions, such as CIFS/SMB for user data, NFS or SAN for the VM datastores, and guest-connect iSCSI LUNs for Windows applications.

Data ONTAP supports the following protocols:

- NFS v3, v4, v4.1, including pNFS
- iSCSI
- FC
- Fibre Channel over Ethernet (FCoE)
- CIFS/SMB

VMware Integrations

The complexity of deploying and managing thousands of virtual desktops can be daunting without the right tools. NetApp Virtual Storage Console (VSC) for VMware vSphere is tightly integrated with VMware vCenter for rapidly provisioning, managing, configuring, and backing up a Citrix XenDesktop implementation. NetApp VSC significantly increases operational efficiency and agility by simplifying the deployment and management process for thousands of virtual desktops.

The following plug-ins and software features simplify deployment and administration of virtual desktop environments:

- **NetApp VSC Provisioning and Cloning** plug-in enables customers to rapidly provision, manage, import, and reclaim space of thinly provisioned VMs and redeploy thousands of VMs.
- **NetApp VSC Backup and Recovery** plug-in integrates VMware snapshot functionality with NetApp Snapshot® functionality to protect Citrix XenDesktop environments.

Replication

The NetApp VSC Backup and Recovery plug-in is a unique, scalable, integrated data protection solution for persistent desktop Citrix XenDesktop environments. This backup and recovery plug-in allows customers to leverage VMware snapshot functionality with NetApp array-based block-level Snapshot copies to provide consistent backups for the virtual desktops.

The backup and recovery plug-in is integrated with NetApp SnapMirror® replication technology, which preserves the deduplicated storage savings from the source to the destination storage array. Deduplication is then not required to be rerun on the destination storage array. When a Citrix XenDesktop environment is replicated with SnapMirror, the replicated data can quickly be brought online to provide production access during a site or data center outage.

In addition, SnapMirror is fully integrated with VMware Site Recovery Manager (SRM) and NetApp FlexClone technology to instantly create zero-cost writable copies of the replicated virtual desktops at the remote site that can be used for disaster recovery (DR) testing or for test and development work.
Citrix ShareFile on NetApp Storage

Citrix and NetApp provide a jointly validated reference architecture for ShareFile on NetApp storage that demonstrates the ability to deliver a scalable and integrated solution with secure infrastructure. This architecture offers a cost-effective and reliable solution that leverages the following clustered Data ONTAP features:

- Storage efficiency with deduplication, thin provisioning, and compression
- On-demand flexibility with ability to scale both Citrix and NetApp seamlessly
- Nondisruptive operations during maintenance and upgrades to prevent downtime
- Unified storage architecture to share NetApp storage infrastructure among Citrix XenDesktop, Citrix XenApp, and other components
- Data protection through NetApp Snapshot technology and NetApp Recovery Manager for Citrix ShareFile

NetApp Recovery Manager for Citrix ShareFile (NRM-CS), a Citrix Ready–certified product, uses on-premises NetApp storage to provide an administrator-driven user file–recovery solution for Citrix ShareFile StorageZones deployments. The Citrix ShareFile default action is to preserve the user files deleted from the ShareFile recycle bin for a period of seven days, after which the files are unavailable for restore from within native ShareFile. In such cases, NRM-CS empowers administrators to restore user files or folders by using, as applicable, NetApp Snapshot copies on primary storage, NetApp SnapMirror, or NetApp SnapVault® software.

For comprehensive details about the solution, refer to TR-4124: Citrix ShareFile StorageZones on NetApp Solution Guide.

2.3 Citrix XenDesktop

Citrix XenDesktop 7.5 integrates HSD and VDI desktop virtualization technologies into a unified architecture that enables a scalable, simple, efficient, and manageable solution for delivering Windows applications and desktops as a service.

Users can select applications from an easy-to-use store that is accessible from tablets, smartphones, PCs, Mac® computers, and thin clients. XenDesktop delivers a native touch-optimized experience with HDX high-definition performance, even over mobile networks.

XenDesktop Components

Citrix XenDesktop provides a complete virtual desktop delivery system by integrating several distributed components with advanced configuration tools that simplify the creation and real-time management of the virtual desktop infrastructure.

XenDesktop contains the following core components:

- **Desktop Delivery Controller.** Installed on servers in the data center, the controller authenticates users, manages the assembly of users' virtual desktop environments, and brokers connections between users and their virtual desktops. It controls the state of the desktops, starting and stopping them based on demand and administrative configuration. Desktop Delivery Controller also includes profile management, in some editions, to manage user personalization settings in virtualized or physical Windows environments.

- **Virtual Desktop Provisioning powered by Citrix Provisioning Services (PVS).** Citrix PVS creates and provisions virtual desktops from a single desktop image on demand, optimizing storage utilization and providing a pristine virtual desktop to each user every time they log on. Desktop provisioning also simplifies desktop images, provides better flexibility, and offers fewer points of desktop management for both applications and desktops.

- **Virtual Desktop Agent.** Installed on virtual desktops, the agent enables direct Independent Computing Architecture (ICA) connections between the virtual desktop and user devices.

- **Citrix online plug-in.** Installed on user devices, the Citrix online plug-in (formerly called Citrix Desktop Receiver) enables direct ICA connections from user devices to virtual desktops.
• **Citrix XenApp.** You can use XenApp to benefit from the efficiencies associated with application streaming and virtualization. XenApp provides a better-than-installed application experience for both users and administrators. Applications start up more quickly, the user experience is dramatically improved, and application management costs are significantly lowered.

• **Hypervisors.** Citrix XenDesktop is hypervisor agnostic, so any of the following three hypervisors can be used to host HSD-based and VDI-based desktops:
  - **VMware vSphere** composes the management infrastructure or virtual center server software and the hypervisor software that virtualizes the hardware resources on the servers. It offers features such as Distributed Resource Scheduler, vMotion®, HA, Storage vMotion®, Virtual Machine File System (VMFS), and a multipathing storage layer. For more information, refer to the VMware vSphere webpage.
  - **Windows Server with Hyper-V®** is available in standard, server core, and free versions. For more information, refer to the Windows Server 2012 R2 webpage.
  - **Citrix XenServer** is a complete managed-server virtualization platform built on the powerful Xen hypervisor. Xen technology is widely acknowledged as the fastest and most secure virtualization software in the industry. XenServer is designed for efficient management of Windows and Linux® virtual servers. It delivers cost-effective server consolidation and business continuity. For more information, refer to the XenServer webpage.

### XenDesktop Architecture

The [Citrix XenDesktop 7.6 Blueprint](#) provides a unified framework for developing a virtual desktop and application solution. Five layers provide flexibility for each user group to have its own set of access policies and resources, which can be shared by users and are all managed by a single, integrated control layer. The following list defines these layers:

• **The user layer** defines the unique user groups, endpoints, and locations.

• **The access layer** defines how a user group gains access to its resources. This layer focuses on secure access policies and on desktop and application stores. Users access a list of available resources through Citrix StoreFront. Users who are not on the internal, protected network must establish an SSL-encrypted tunnel across public network links to the Citrix NetScaler Gateway.

• **The resource layer** defines the virtual desktops, applications, and data provided to each user group, such as pooled desktops, personal desktops, hosted applications, or remote PC access.

• **The control layer** defines the underlying infrastructure required to support users in accessing their resources. The delivery controller authenticates users and enumerates resources from StoreFront while creating, managing, and maintaining the virtual resources. All configuration information about the XenDesktop site is stored in a SQL Server® database.

• **The hardware layer** defines the physical implementation of the overall solution. The corresponding hosts provide computing and storage resources to the resource layer workloads.

Figure 3 shows the conceptual relationship among all of the layers.
The reference architecture described in this document focuses on delivering a mixed workload consisting of 1,000 sessions of HSDs and 1,000 sessions of hosted VDIs.

The following sections describe the Citrix XenDesktop components used in this reference architecture:

- Citrix XenDesktop Delivery Controller VM
- Citrix Provisioning Server VM
- Citrix Licensing Server VM
- Citrix StoreFront Server VM

In addition, a Microsoft SQL Server VM is used for backup.

**Citrix XenDesktop Delivery Controller VM**

In a deployment, XenDesktop Delivery Controller is the server-side component that is responsible for managing user access as well as brokering and optimizing connections. Controllers also provide the Machine Creation Services that create desktop and server images.

A site must have at least one delivery controller. After the initial controller is installed and a site is created, more controllers can be added. Two primary benefits result from having more than one controller in a site:

- **Redundancy.** As a best practice, a production site should always have at least two controllers on different physical servers. If one controller fails, the others can manage connections and administer the site.
- **Scalability.** As site activity grows, so do CPU utilization on the controller and Microsoft SQL Server database activity. Additional controllers can improve overall responsiveness and provide the ability to handle more users, more applications, and more desktop requests.

Two XenDesktop servers are included in this reference architecture to provide HA. The configuration components are listed in Table 4.
Citrix XenDesktop VM configuration.

<table>
<thead>
<tr>
<th>Citrix XenDesktop Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>2</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
</tbody>
</table>

Citrix Provisioning Server VM

Citrix PVS takes a very different approach from that of traditional imaging solutions by fundamentally changing the relationship between hardware and the software that runs on it. By streaming a single shared disk image (vDisk) rather than copying images to individual machines, Citrix PVS enables organizations to reduce the number of disk images that they manage, even as the number of machines continues to grow. It simultaneously provides the efficiencies of a centralized management and the benefits of distributed processing.

In addition, because machines are streaming disk data dynamically and in real time from a single shared image, machine image consistency is provided, while at the same time large pools of machines can completely change their configuration, applications, and even OS in the time it takes them to reboot.

vDisks can exist on a provisioning server, on a file share, or in larger deployments on a storage system that can communicate with the provisioning server (through iSCSI, SAN, NAS, or CIFS/SMB). vDisks can be assigned to a single target device in private image mode or to multiple target devices in standard image mode. When a target device is turned on, it is set to boot from the network and to communicate with a provisioning server.

This reference architecture uses four provisioning servers. The configuration components are listed in Table 5.

Citrix Provisioning Server VM configuration.

<table>
<thead>
<tr>
<th>Citrix Provisioning Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>4</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
</tbody>
</table>
Citrix Licensing Server VM

Every Citrix product environment must have at least one shared or dedicated licensing server. Licensing servers are computers that are either partly or completely dedicated to storing and managing licenses. Citrix products request licenses from a licensing server when users attempt to connect. The configuration components are listed in Table 6.

Table 6) Citrix Licensing Server VM configuration.

<table>
<thead>
<tr>
<th>Citrix Licensing Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>1</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
</tbody>
</table>

Citrix StoreFront Server VM

Citrix StoreFront enables you to create enterprise app stores that aggregate resources from XenDesktop, XenApp, XenMobile App Controller, and VDI-in-a-Box in one place. The stores that you create give your users self-service access to their Windows desktops and applications, mobile applications, external software-as-a-service applications, and internal web applications through a single portal from all of their devices. You get a single place to manage the provisioning of corporate desktops and applications to your users. Consolidating the delivery of resources through StoreFront means that you no longer have to manage multiple delivery mechanisms for different applications or provide support for manual installations and updates.

This reference architecture uses two Citrix StoreFront servers. The configuration components are listed in Table 7.

Table 7) Citrix StoreFront Server VM configuration.

<table>
<thead>
<tr>
<th>Citrix StoreFront Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>2</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
</tbody>
</table>
Microsoft SQL Server VM

In XenDesktop, all information is stored on the database; controllers communicate only with the database and not with each other. A controller can be unplugged or turned off without affecting other controllers in the site. This means, however, that the database forms a single point of failure. If the database server fails, existing connections to virtual desktops continue to function until the user either logs off or disconnects from the virtual desktop; new connections cannot be established if the database server is unavailable.

Citrix recommends that you back up the database regularly so that you can restore from the backup if the database server fails. In addition to this good practice, three other HA solutions should be considered for supporting automatic failover.

For simplicity, this reference architecture uses only one SQL Server instance. The configuration components are listed in Table 8.

Table 8) SQL Server VM configuration.

<table>
<thead>
<tr>
<th>SQL Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>1</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
</tbody>
</table>

2.4 Login VSI

Login Virtual Session Indexer (Login VSI) is the industry-standard load-testing tool for testing the performance and scalability of centralized Windows desktop environments such as server-based computing (SBC) and VDI.

Login VSI is used for testing and benchmarking by all major hardware and software vendors and is recommended by both leading IT analysts and the technical community. Login VSI is vendor independent and works with standardized user workloads; therefore, conclusions based on Login VSI test data are objective, verifiable, and replicable.

SBC-oriented and VDI-oriented vendor organizations that are committed to enhancing end-user experience in the most efficient way use Login VSI as an objective method of testing, benchmarking, and improving the
performance and scalability of their solutions. VSImax provides the proof (vendor independent, industry standard, and easy to understand) to innovative technology vendors to demonstrate the power, the scalability, and the gains of their solutions.

Login VSI–based test results are published in technical white papers and presented at conferences. Login VSI is used by end-user organizations, system integrators, hosting providers, and testing companies. It is also the standard tool used in all tests executed in the internationally acclaimed Project Virtual Reality Check.

For more information about Login VSI or for a free test license, refer to the Login VSI website.

3 Solution Infrastructure

This section describes the software and hardware components of the solution. Figure 4 shows the solution infrastructure, which includes two Citrix XenDesktop VMs, two Citrix StoreFront VMs, one Citrix licensing server, and four Citrix provisioning servers.

All write cache volumes hosting write cache files for 2,000 users were hosted on one storage controller in the HA pair. Scale performance tests, such as boot, login, and steady-state tests, were performed to help validate that this All-Flash FAS array is capable of hosting 4,000 users with the standard configuration of two storage controllers.

Figure 4 shows the solution infrastructure for nonpersistent desktops, and Figure 5 shows the infrastructure for persistent desktops.

Figure 4) Solution infrastructure for nonpersistent desktops.
3.1 Hardware Infrastructure

During solution testing, 24 Cisco UCS blade servers were used to host the infrastructure and the desktop VMs. The desktops and infrastructure servers were hosted on discrete resources so that the workload to the NetApp All-Flash FAS system could be measured precisely. It is both a NetApp and an industry best practice to separate the desktop VMs from the infrastructure VMs because noisy neighbors or bully virtual desktops can affect the infrastructure and have a negative impact on all users, applications, and performance results.

Options to neutralize this problem include leveraging intelligent quality-of-service policies in Data ONTAP to eliminate noisy neighbor behavior, using intelligent sizing to account for infrastructure VMs, or putting infrastructure VMs on an existing or separate NetApp FAS storage system. For this lab validation, we used a separate NetApp FAS storage system (not shown) to host the infrastructure and the launcher. In the real world, infrastructure VMs can be on the same All-Flash FAS system that is hosting the virtual desktops. Table 9 lists the hardware specifications of each server category.

Table 9) Hardware components of server categories.

<table>
<thead>
<tr>
<th>Hardware Components</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure Servers</strong></td>
<td></td>
</tr>
<tr>
<td>Server quantity</td>
<td>2 Cisco UCS B200 M3 blade servers</td>
</tr>
<tr>
<td>CPU model</td>
<td>Intel® Xeon® CPU E5-2650 v2 at 2.60GHz (8-core)</td>
</tr>
<tr>
<td>Total number of cores</td>
<td>16 cores</td>
</tr>
<tr>
<td>Memory per server</td>
<td>256GB</td>
</tr>
<tr>
<td>Storage</td>
<td>One 10GB boot LUN per host</td>
</tr>
<tr>
<td><strong>Desktop Servers</strong></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5) Solution infrastructure for persistent desktops.
# Hardware Components

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server quantity</strong></td>
</tr>
<tr>
<td>16 Cisco UCS B200 M3 blade servers</td>
</tr>
<tr>
<td><strong>CPU model</strong></td>
</tr>
<tr>
<td>Intel Xeon CPU E5-2680 v2 at 2.80GHz (10-core)</td>
</tr>
<tr>
<td><strong>Total number of cores</strong></td>
</tr>
<tr>
<td>20 cores</td>
</tr>
<tr>
<td><strong>Memory per server</strong></td>
</tr>
<tr>
<td>6 with 256GB, 8 with 384GB</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
</tr>
<tr>
<td>One 10GB boot LUN per host</td>
</tr>
</tbody>
</table>

## Launcher Servers

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server quantity</strong></td>
</tr>
<tr>
<td>6 Cisco UCS B200 M3 blade servers</td>
</tr>
<tr>
<td><strong>CPU model</strong></td>
</tr>
<tr>
<td>Intel Xeon CPU E5-2650 at 2.00GHz (8-core)</td>
</tr>
<tr>
<td><strong>Total number of cores</strong></td>
</tr>
<tr>
<td>16 cores</td>
</tr>
<tr>
<td><strong>Memory per server</strong></td>
</tr>
<tr>
<td>192GB</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
</tr>
<tr>
<td>One 10GB boot LUN per host</td>
</tr>
</tbody>
</table>

## Networking

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Networking switch</strong></td>
</tr>
<tr>
<td>2 Cisco Nexus 5548UP</td>
</tr>
</tbody>
</table>

## Storage

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetApp system</strong></td>
</tr>
<tr>
<td>FAS8060 HA pair</td>
</tr>
<tr>
<td><strong>Disk shelf</strong></td>
</tr>
<tr>
<td>2 DS2246</td>
</tr>
<tr>
<td><strong>Disk drives</strong></td>
</tr>
<tr>
<td>36 400GB SSDs</td>
</tr>
</tbody>
</table>

### 3.2 Software Components

This section describes the purpose of each software product used to test the NetApp All-Flash FAS system and provides configuration details. Table 10 lists the software components and identifies the version of each component.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetApp FAS</strong></td>
<td></td>
</tr>
<tr>
<td>Clustered Data ONTAP</td>
<td>8.2.2</td>
</tr>
<tr>
<td>NetApp System Manager</td>
<td>3.1.1 RC1</td>
</tr>
<tr>
<td>NetApp VSC for VMware</td>
<td>5.0</td>
</tr>
<tr>
<td>Storage protocol for write cache</td>
<td>FC</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 5548UP</td>
<td>NX-OS software release 7.0(0)N1(1)</td>
</tr>
<tr>
<td>Cisco UCS 6248</td>
<td>UCSM 2.2(1c)</td>
</tr>
<tr>
<td><strong>Servers:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### VMware vSphere 5.5

This section describes the VMware vSphere components of the solution.

#### VMware ESXi 5.5

The tested reference architecture used VMware ESXi 5.5 across all servers. For hardware configuration information, refer to Table 9.

#### VMware vCenter 5.5 Configuration

The tested reference architecture used VMware vCenter Server 5.5 running on a Windows Server 2008 R2 server. This vCenter Server instance was configured to host the infrastructure cluster, the Login VSI launcher cluster, and the desktop clusters. For the vCenter Server database, a Windows Server 2008 R2 VM was configured with SQL Server 2008 R2. Table 11 lists the components of the vCenter Server VM configuration, and Table 12 lists the components of the SQL Server database VM configuration.

**Table 11) VMware vCenter Server VM configuration.**

<table>
<thead>
<tr>
<th>VMware vCenter Server VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>1</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>8</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
</tbody>
</table>
2.4 NetApp Virtual Storage Console

NetApp VSC is a management plug-in for VMware vCenter Server that enables simplified management and orchestration of common administrative tasks for NetApp storage. VSC cloning and provisioning operations benefit from the NFS Plug-In for VMware VAAI. The plug-in integrates with VMware virtual disk libraries to provide VAAI features, including copy offload and space reservations. These features can improve the performance of cloning operations because they do not have to go through the ESXi host.

This tested reference architecture used VSC for the following tasks:

- Setting NetApp best practices for ESXi hosts, including timeout values, host bus adapter (HBA), multipath input/output (MPIO), and Network File System (NFS) settings
- Provisioning datastores
- Cloning infrastructure VMs, Login VSI launcher machines, and 2,000 persistent desktops

VSC can be installed on the VMware vCenter Server instance when the Windows version of vCenter is used. For this reference architecture, a separate server was used to host VSC. Table 13 lists the components of the tested NetApp VSC VM configuration.

<table>
<thead>
<tr>
<th>Table 13) NetApp VSC VM configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp VSC VM</td>
</tr>
<tr>
<td>VM quantity</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>VM hardware version</td>
</tr>
<tr>
<td>vCPU</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>Network adapter type</td>
</tr>
<tr>
<td>Network adapters</td>
</tr>
<tr>
<td>Hard disk size</td>
</tr>
<tr>
<td>Hard disk type</td>
</tr>
</tbody>
</table>

3.4 NetApp Virtual Storage Console

NetApp VSC is a management plug-in for VMware vCenter Server that enables simplified management and orchestration of common administrative tasks for NetApp storage. VSC cloning and provisioning operations benefit from the NFS Plug-In for VMware VAAI. The plug-in integrates with VMware virtual disk libraries to provide VAAI features, including copy offload and space reservations. These features can improve the performance of cloning operations because they do not have to go through the ESXi host.

This tested reference architecture used VSC for the following tasks:

- Setting NetApp best practices for ESXi hosts, including timeout values, host bus adapter (HBA), multipath input/output (MPIO), and Network File System (NFS) settings
- Provisioning datastores
- Cloning infrastructure VMs, Login VSI launcher machines, and 2,000 persistent desktops

VSC can be installed on the VMware vCenter Server instance when the Windows version of vCenter is used. For this reference architecture, a separate server was used to host VSC. Table 13 lists the components of the tested NetApp VSC VM configuration.

<table>
<thead>
<tr>
<th>Table 13) NetApp VSC VM configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp VSC VM</td>
</tr>
<tr>
<td>VM quantity</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>VM hardware version</td>
</tr>
</tbody>
</table>

3.4 NetApp Virtual Storage Console

NetApp VSC is a management plug-in for VMware vCenter Server that enables simplified management and orchestration of common administrative tasks for NetApp storage. VSC cloning and provisioning operations benefit from the NFS Plug-In for VMware VAAI. The plug-in integrates with VMware virtual disk libraries to provide VAAI features, including copy offload and space reservations. These features can improve the performance of cloning operations because they do not have to go through the ESXi host.

This tested reference architecture used VSC for the following tasks:

- Setting NetApp best practices for ESXi hosts, including timeout values, host bus adapter (HBA), multipath input/output (MPIO), and Network File System (NFS) settings
- Provisioning datastores
- Cloning infrastructure VMs, Login VSI launcher machines, and 2,000 persistent desktops

VSC can be installed on the VMware vCenter Server instance when the Windows version of vCenter is used. For this reference architecture, a separate server was used to host VSC. Table 13 lists the components of the tested NetApp VSC VM configuration.

<table>
<thead>
<tr>
<th>Table 13) NetApp VSC VM configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp VSC VM</td>
</tr>
<tr>
<td>VM quantity</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>VM hardware version</td>
</tr>
</tbody>
</table>

3.4 NetApp Virtual Storage Console

NetApp VSC is a management plug-in for VMware vCenter Server that enables simplified management and orchestration of common administrative tasks for NetApp storage. VSC cloning and provisioning operations benefit from the NFS Plug-In for VMware VAAI. The plug-in integrates with VMware virtual disk libraries to provide VAAI features, including copy offload and space reservations. These features can improve the performance of cloning operations because they do not have to go through the ESXi host.

This tested reference architecture used VSC for the following tasks:

- Setting NetApp best practices for ESXi hosts, including timeout values, host bus adapter (HBA), multipath input/output (MPIO), and Network File System (NFS) settings
- Provisioning datastores
- Cloning infrastructure VMs, Login VSI launcher machines, and 2,000 persistent desktops

VSC can be installed on the VMware vCenter Server instance when the Windows version of vCenter is used. For this reference architecture, a separate server was used to host VSC. Table 13 lists the components of the tested NetApp VSC VM configuration.

<table>
<thead>
<tr>
<th>Table 13) NetApp VSC VM configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp VSC VM</td>
</tr>
<tr>
<td>VM quantity</td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>VM hardware version</td>
</tr>
</tbody>
</table>
3.5 Virtual Desktop vDisk

One significant advantage of delivering services through HSD and VDI is the way these technologies simplify desktop administration and management. Citrix PVS takes the approach of streaming a single shared virtual disk (vDisk) image rather than provisioning and distributing multiple OS image copies across multiple VMs. One advantage of this approach is that it constrains the number of disk images that must be managed, even as the number of desktops grows, providing image consistency. At the same time, using a single shared image (rather than hundreds or thousands of desktop images) significantly reduces the required storage footprint and dramatically simplifies image management.

Because there is a single master image, patch management is simple and reliable. All patching is done on the master image, which is then streamed as needed. When an updated image is ready for production, the administrator simply reboots to deploy the new image. Rolling back to a previous image is performed in the same manner. Local hard disk drives in user systems can be used for runtime data caching or in some scenarios removed entirely, lowering power usage, system failure rates, and security risks.

After the PVS components are installed and configured, a vDisk is created from a device’s hard drive by making a snapshot of the OS and the application image and then storing that image as a vDisk file on the network. vDisks can exist on a provisioning server, a file share, or in larger deployments, on a storage system with which the provisioning server can communicate (through iSCSI, SAN, NAS, or CIFS/SMB). vDisks can be assigned to a single target device in private image mode or to multiple target devices in standard image mode.

When a user device boots, the appropriate vDisk is located based on the boot configuration and mounted on the provisioning server. The software on that vDisk is then streamed to the target device, and it appears to the system as a regular hard drive. Instead of pulling all of the vDisk contents down to the target device (as is done in some imaging deployment solutions), the data is brought across the network in real time, as needed. This greatly improves the overall user experience because it minimizes desktop startup time.

To build the vDisk images, OS images of Windows 7 and Windows Server 2012, along with additional software, were initially installed and prepared as standard VMs on VMware vSphere. These master target VMs were then converted into separate Citrix PVS vDisk files. Citrix PVS and the XenDesktop Delivery Controller VMs use the golden vDisk images to instantiate new desktop VMs on VMware vSphere.

In this reference architecture, VMs for hosted shared desktops and hosted virtual desktops were created by using the XenDesktop setup wizard, which accomplishes the following tasks:

1. Creates VMs on a XenDesktop hosted hypervisor server from an existing template
2. Creates PVS target devices for each new VM in a new or existing collection matching the XenDesktop catalog name
3. Assigns a standard image vDisk to VMs in the collection
4. Adds virtual desktops to a XenDesktop machine catalog

Virtual desktops were optimized according to best practices for performance. The Optimize Performance checkbox was selected during installation of the XenDesktop Virtual Delivery Agent (VDA), and the Optimize
for Provisioning Services checkbox was selected during the PVS image creation process, using the PVS imaging wizard.

The hosted VDI vDisk was created with the virtual hardware and software listed in Table 14, Table 15, and Table 16. The VM hardware and software were installed and configured according to Login VSI documentation. The vDisk was located on an SMB 3 share.

Table 14) vDisk configuration.

<table>
<thead>
<tr>
<th>Desktop VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>1 vCPU</td>
</tr>
<tr>
<td>Memory</td>
<td>1.5GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET 3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>24GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
<tr>
<td>Guest OS</td>
<td>Windows 7 SP1 (32-bit)</td>
</tr>
</tbody>
</table>

Table 15) HSD vDisk configuration.

<table>
<thead>
<tr>
<th>Desktop VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET 3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>50GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
<tr>
<td>Guest OS</td>
<td>Windows Server 2012 SP1</td>
</tr>
</tbody>
</table>

Table 16) HSD and VDI installed software.

<table>
<thead>
<tr>
<th>Desktop VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM hardware version</td>
<td>ESXi 5.5 and later (VM version 10)</td>
</tr>
<tr>
<td>VMware tools version</td>
<td>9344 (default for VMware ESXi, 5.5.0, 1331820)</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>2010 version 14.0.4763.1,000</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>3.5</td>
</tr>
<tr>
<td>Adobe Acrobat Reader</td>
<td>11.0.00</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>11.5.502.146</td>
</tr>
</tbody>
</table>
3.6 Full-Clone Virtual Desktops

The desktop VM template was created with the virtual hardware and software listed in Table 17. The VM hardware and software were installed and configured according to Login VSI documentation.

Table 17) Virtual desktop configuration.

<table>
<thead>
<tr>
<th>Desktop VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java®</td>
<td>7.0.550</td>
</tr>
<tr>
<td>Doro PDF</td>
<td>1.82</td>
</tr>
<tr>
<td>Login VSI target software</td>
<td>4.1</td>
</tr>
<tr>
<td>XenDesktop VDA</td>
<td>7.5</td>
</tr>
<tr>
<td>Provisioning Server Target Device</td>
<td>7.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Desktop Software</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest OS</td>
<td>Windows 7 (32-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>ESXi 5.5 and later (VM version 10)</td>
</tr>
<tr>
<td>VMware tools version</td>
<td>9344 (default for VMware ESXi, 5.5.0, 1331820)</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>2010 version 14.0.4763.1,000</td>
</tr>
<tr>
<td>Microsoft .NET Framework</td>
<td>3.5</td>
</tr>
<tr>
<td>Adobe Acrobat Reader</td>
<td>11.0.00</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>11.5.502.146</td>
</tr>
<tr>
<td>Java</td>
<td>7.0.550</td>
</tr>
<tr>
<td>Doro PDF</td>
<td>1.82</td>
</tr>
<tr>
<td>Citrix XenDesktop Agent</td>
<td>7.5</td>
</tr>
<tr>
<td>Login VSI target software</td>
<td>4.1</td>
</tr>
</tbody>
</table>
After the desktops were provisioned, Windows PowerShell® was used to set the `uuid.action` in the `vmx` file on each VM in the desktop’s datastore so that during testing no questions would be asked about the movements of VMs. Figure 6 shows the complete command.

**Figure 6** Setting `uuid.action` in `vmx` file with Windows PowerShell.

```
Get-Cluster Desktops | Get-VM | Get-AdvancedSetting -Name uuid.action | Set-AdvancedSetting -Value "keep" -Confirm:$false
```

**Note:** This optional step was used to simplify our testing.

### Guest Optimization

Guest OS optimizations were applied to the template VMs used in this reference architecture. Figure 7 shows the VMware OS optimization tool that was used to perform the guest optimizations.

**Figure 7**) VMware OS optimization tool.

Although it might be possible to run desktops without guest optimizations, the impact of not optimizing must first be understood. Many recommended optimizations address services and features (such as hibernation, Windows update, or system restore) that do not provide value in a virtual desktop environment. To run services and features that do not add value would decrease the overall density of the solution and increase cost because these services and features would consume CPU, memory, and storage resources in relation to both capacity and I/O.

### 3.7 Login VSI Server

The Login VSI server is where the Login VSI binaries are run as well as the Windows share that hosts the user data, binaries, and workload results. The tested machine was configured with the virtual hardware listed in Table 18.
Table 18) Login VSI server configuration.

<table>
<thead>
<tr>
<th>Login VSI Server</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>1</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>4 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
</tbody>
</table>

The Login VSI launcher configuration is shown in Figure 8.

Figure 8) Login VSI launcher configuration.
3.8 Login VSI Launcher VM

We used Citrix Provisioning Server to create 80 Login VSI launchers. Table 19 lists the components of the Login VSI launcher VM configuration.

Table 19) Login VSI launcher VM configuration.

<table>
<thead>
<tr>
<th>Login VSI Launcher VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>80</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>4GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
</tbody>
</table>

3.9 Microsoft Windows Infrastructure VM

In the tested configuration, two VMs were provisioned and configured to serve Active Directory, Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) services for the reference architecture. The servers provided these services to both infrastructure and desktop VMs. Table 20 lists the components of the Microsoft Windows infrastructure VM.

Table 20) Windows infrastructure VM.

<table>
<thead>
<tr>
<th>Microsoft Windows Infrastructure VM</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM quantity</td>
<td>2</td>
</tr>
<tr>
<td>OS</td>
<td>Microsoft Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td>VM hardware version</td>
<td>10</td>
</tr>
<tr>
<td>vCPU</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>4GB</td>
</tr>
<tr>
<td>Network adapter type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1</td>
</tr>
<tr>
<td>Hard disk size</td>
<td>60GB</td>
</tr>
<tr>
<td>Hard disk type</td>
<td>Thin</td>
</tr>
</tbody>
</table>
4 Storage Design

This section provides an overview of the storage design, the aggregate and volume layout, and VSC.

4.1 Storage Design Overview

For this configuration, shown in Figure 9, we used a 6U FAS8060 controller and two DS2246 disk shelves that are 2RU per shelf for a total of 10RU. Note that the image in Figure 9, which shows two enclosures, is a logical view that illustrates multipath HA. In the FAS8060, both nodes reside in one 6U enclosure.

Figure 9) Multipath HA to DS2246 shelves of SSD.

4.2 Aggregate Layout

In this reference architecture, we used 36 400GB SSDs divided across the two nodes of a FAS8060 controller. As shown in Figure 10, each node had a 2-disk root aggregate, a 15-disk data aggregate, and one spare.

Figure 10) SSD layout.
4.3 Volume Layout

To adhere to NetApp best practices, all volumes were provisioned with NetApp VSC. During these tests, only 3.342TB of the total 8TB was consumed. Figure 11 shows how the volumes were arranged.

Figure 11) Volume layout for nonpersistent desktops.

A root volume for the virtual desktop storage virtual machine (SVM, formerly called Vserver) was present but is not depicted.

Note: The root volume was 1GB in size with 28MB consumed.

Figure 12 shows the volume layout for persistent desktops.
4.4 NetApp Virtual Storage Console for VMware vSphere

NetApp VSC was used to provision the datastores in this reference architecture. NetApp VSC for VMware vSphere provides integrated, comprehensive, end-to-end virtual storage management for your VMware infrastructure, including discovery, health monitoring, capacity management, provisioning, cloning, backup, restore, and disaster recovery. It integrates manageability for NetApp Flash Accel™ host-based caching solutions.

VSC lets your VMware administrators access and execute all of these capabilities from VMware vCenter. Using its built-in role-based access control (RBAC), you can control who does what, enhancing server and storage efficiencies without affecting your storage administrators’ policies. All VSC for VMware vSphere capabilities are supported on both clustered Data ONTAP and Data ONTAP operating in 7-Mode.
5 Network Design

Figure 13 shows the network topology linking the NetApp All-Flash FAS8060 switchless two-node cluster to the Intel X86 servers hosting virtual desktop VMs.

Figure 13) Network topology of storage to server.

5.1 Network Switching

Two Cisco Nexus 5548UP switches running NX-OS software release 7.0(0)N1(1) were used in this validation. These switches were chosen because of their ability to provide both IP Ethernet and FC/FCoE networking on one platform. FC zoning was done in these switches, and two SAN switching fabrics (A and B) were maintained. From an Ethernet perspective, virtual port channels (vPCs) were used, allowing a port channel from the storage to be spread across both switches.

5.2 Host Server Networking

Each host server had an FCoE HBA that provided two 10GB converged Ethernet ports containing FCoE for FC networking and Ethernet for IP networking. FCoE from the host servers was used both for FC SAN boot of the servers and for accessing FC VM datastores on the NetApp FAS8060 servers. From an Ethernet perspective,
each VMware ESXi host had a dedicated vSwitch with both Ethernet ports configured as active and with source MAC hashing.

5.3 Storage Networking

Each of the two NetApp FAS8060 storage systems had a two-port interface group or LACP port channel connected to a vPC across the two Cisco Nexus 5548UP switches. This switch was used for both Ethernet and FC traffic. In addition, four 8Gb/sec FC targets were configured from each FAS8060 system, with two going to each switch. ALUA was used to provide multipathing and load balancing of the FC links. This configuration allowed each of the two storage controllers to provide up to 32Gb/sec of FC aggregate bandwidth. Initiator groups were also configured on the FAS8060 systems to map datastore LUNs to the ESXi host servers.

6 Citrix XenDesktop Design

This section provides an overview of Citrix XenDesktop design and explains user assignment, automated desktop pools, linked-clones desktops, and the creation of desktop pools.

6.1 Overview

A pool of desktops (POD) is a building-block approach to architecting a solution. Using a POD-based design gives IT a simplified management model and a standardized way to scale linearly and predictably. By using clustered Data ONTAP, customers can have smaller fault domains that result in higher availability.

It is important to review carefully the XenDesktop documentation on configuration maximums associated with the various storage-related parameters critical to the system design.

These configuration parameters should help determine the following design parameters:

- Proposed number of VMs per hypervisor host
- Proposed number of hypervisor hosts per hypervisor cluster
- Proposed number of datastores (storage repositories) per hypervisor cluster
- Proposed number of VMs per hypervisor cluster
- Number of hypervisor clusters managed by a vCenter or XenCenter instance
- Proposed number of VMs per datastore (storage repository)
- Total number of datastores required for the project

Note: For VMware vSphere, review the VMware configuration described in VMware vSphere 5.5 Configuration Maximums.

6.2 XenDesktop Storage Design

This section outlines the recommended storage architecture for deploying a mix of various XenDesktop FlexCast delivery models (such as hosted VDI and HSDs) along with intelligent virtual desktop layering (such as profile management and user data management) on the same NetApp clustered Data ONTAP storage array.

Storage Architecture for PVS Deployment

NetApp recommends using the storage architecture shown in Figure 14 to deploy desktops through the Citrix PVS provisioning method.
The NetApp storage architecture for XenDesktop includes the following components:

- **Base OS image:**
  - **PVS vDisk.** CIFS/SMB 3 is the recommended protocol for hosting the PVS vDisk. CIFS/SMB 3 allows the same vDisk to be shared among multiple PVS servers, unlike the hosting of vDisk on an FC or iSCSI LUN, which requires one LUN per PVS server. When the vDisk is shared, only one vDisk must be patched or updated to roll out the updates to thousands of pooled desktops. This model results in significant operational savings and architectural simplicity.
  - **PVS write cache file.** The PVS write cache file can be hosted on SAN LUNs or NFS volumes.

- **Profile management.** To make sure that the user profiles and settings are preserved after the desktops are reprovisioned from the updated vDisk (as a result of desktop patches, updates, and so on), leverage the profile management software (for example, Citrix User Profile Manager) to redirect the user profiles to the CIFS/SMB home directories.

- **User data management.** NetApp recommends hosting the user data on CIFS/SMB home directories to preserve the data when the VM is rebooted or redeployed.

### 7 Login VSI Workload

Login VSI is an industry-standard workload-generation utility for VDI. The Login VSI tool works by replicating a typical user’s behaviors. Multiple different workloads can be selected, and the workload can be customized for specific applications and user profiles.

#### 7.1 Login VSI Components

As shown in Figure 15, Login VSI includes multiple different components to run and analyze user workloads. The Login VSI server was used to configure the components (such as Active Directory, the user workload profile, and the test profile) and to gather the data. In addition, a CIFS/SMB share was created on the Login VSI server that shared the user files that the workload would use. When the test was executed, the Login VSI share logged into the launcher servers, which in turn logged into the target desktops and began the workload.
Login VSI Launcher

The tested reference architecture followed the Login VSI best practice of having 25 VMs per launcher server. PCoIP was used as the display protocol between the launcher servers and the virtual desktops. Figure 16 shows the relationship between the desktops and the launcher server.
Workload
These tests used the Login VSI 4.1 office worker workload to simulate users working. The office worker workload, which is available in Login VSI 4.1, is a beta workload that is based on a knowledge worker workload. The team from Login VSI recommended using this workload with Login VSI 4.1 because it is very similar to the medium workload in Login VSI 3.7. The applications that were used are listed in Table 16.

8 Testing and Validation: Nonpersistent Provisioning Server Desktops
The purpose of this testing was to validate that a 2,000-desktop mixed workload of Citrix XenDesktop 7.5 VDIs and Citrix XenDesktop 7.5 HSD models (XenApp users) could be hosted on a NetApp All-Flash FAS8060 storage system running clustered Data ONTAP 8.2.2. The extensive 2,000-desktop performance testing described in this section proved that the system has plenty of headroom and showed that this All-Flash FAS8060 storage configuration can potentially scale to 4,000 desktops.

To cover a variety of customer use cases, we tested both roaming and mandatory profile types. Roaming profiles require more I/O than mandatory profiles. Our tests demonstrated that the All-Flash FAS8060 storage system could easily handle both profile scenarios without issues.

The information contained in this section provides data points that customers can reference in designing their own implementations. These validation results are an example of what is possible under the specific environment conditions outlined here; they do not represent the full characterization of XenDesktop with VMware vSphere.
8.1 Overview

This section defines both pooled and dedicated desktops and explains the concept of profile management.

Pooled Desktops

The machine type defines the type of hosting infrastructure used for desktops and the level of control that users have over their desktop environment, which determines the usage scenarios for which the desktops are best suited. When deciding which machine type to use, consider the tasks that users will perform with their desktops and the devices to which the desktops will be delivered. The type and amount of infrastructure available to host each desktop are also important considerations.

Pooled machines provide desktops that are allocated to users on a per-session, first-come, first-served basis. Pooled-random machines are assigned to users arbitrarily at each login and are returned to the pool when the users log out. Machines that are returned to the pool are available for other users to connect to. Alternatively, with pooled-static machines, users are assigned a specific machine from the pool when they first log in to XenDesktop and are connected to the same machines for all subsequent sessions. This allows the users of pooled-static machines to be associated with specific VMs, which is a licensing requirement for some applications. Pooled desktops are freshly created from the master VM when users log on, although profile management can be used to apply users’ personal settings to their desktops and applications. Any changes that users make to their desktops are stored for the duration of the session but are discarded when users log out. Maintaining a single master VM in the data center dramatically reduces the time and effort required to update and upgrade users’ desktops.

Pooled desktops are the right selection if your users:

- Are task workers who require standardized desktops, such as call-center operators and retail workers
- Use shared workstations, for example, students and faculty in educational institutions
- Do not need to or are not permitted to install applications on their desktops

Pooled desktops are also appropriate if you want to:

- Optimize hardware usage by providing only the number of desktops that are required at any one time rather than assigning each user a specific desktop
- Maintain control over desktops and increase security by preventing users from making permanent changes
- Minimize desktop management costs by providing a locked-down standardized environment for your users

Dedicated Desktops

Dedicated machines provide desktops that are assigned to individual users. Machines can be assigned manually, or they can be automatically assigned to the first user to connect to them. Whenever users request a desktop, they are always connected to the same machine, so you can allow users to personalize their desktops to suit their needs. Dedicated desktops are created from the master VM the first time that users log on, but all subsequent changes made to the desktops persist. As with traditional local desktops, changes and updates are permanent and must be managed on an individual basis or collectively by using third-party electronic software distribution tools. Changes made to desktops are stored in differencing disks that expand as required so that storage space is used only as it is needed.

Dedicated desktops are the right selection if your users:

- Are task or knowledge workers who require personalized desktops of which they can take ownership
- Are mobile workers who want to access the same desktop from a variety of devices over different networks
- Need to install their own applications on their desktops

Dedicated desktops are also appropriate if you want to:

- Standardize certain aspects of users’ desktops through the use of a common template
• Deliver users' desktops to any device, regardless of hardware capability
• Reduce desktop management costs while still offering your users a personalized desktop experience

Profile Management

A user profile solution, integrated with XenDesktop, overcomes many of the challenges associated with Windows local, mandatory, and roaming profiles through proper policy configuration. Citrix Profile Management improves the user experience by capturing user-based changes to the environment and by improving user login/logout speed.

A Windows user profile is a collection of folders, files, registry settings, and configuration settings that define the environment for a user who logs on with a particular user account. These settings might be customizable by the user, depending on the administrative configuration. Settings that can be customized include the following examples:

• Desktop settings, such as wallpaper and screen saver
• Shortcuts and start menu settings
• Internet Explorer favorites and home page
• Microsoft Outlook® signature
• Printers

Some user settings and data can be redirected by means of folder redirection. If folder redirection is not used, however, these settings are stored in the user profile.

The first stage in planning a profile management deployment is to decide on a set of policy settings that together form a suitable configuration for your environment and users. The automatic configuration feature simplifies some of this decision making for XenDesktop deployments. The user profile management interfaces establish policies for this reference’s HSD and VDI users (for testing purposes). Basic profile management policy settings are documented in Profile Management policy settings.

Mandatory profiles are read only, so a single mandatory profile can be used for large groups of users. A mandatory profile is copied from a CIFS/SMB share to the VM during login. During logout, any changes to the profile are not saved. Instead, the local copy of the mandatory profile is reset to its initial state at the next login. Therefore, storage requirements are minimal: a single mandatory profile is kept on the file servers instead of keeping thousands of roaming profiles. Mandatory profiles can be used only on kiosk-like systems.

In this reference architecture, we tested both a mandatory profile case and a roaming case. Figure 17 shows the decision points.
8.2 Test Results Overview

Table 21 lists the high-level results that were achieved during the reference architecture testing of 2,000 users on a single All-Flash FAS8060 controller.

Table 21) Test results overview.

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Time to Complete</th>
<th>Peak IOPS</th>
<th>Average IOPS</th>
<th>Peak Throughput (MB/sec)</th>
<th>Average Throughput (MB/sec)</th>
<th>Peak Storage Latency (ms)</th>
<th>Average Storage Latency</th>
<th>Peak CPU</th>
<th>Average CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot storm test (VMware vCenter power-on operations, VM registered in XenDesktop)</td>
<td>8 min, 13 sec</td>
<td>9,516</td>
<td>7,463</td>
<td>116.00</td>
<td>73.00</td>
<td>0.426</td>
<td>0.406</td>
<td>10%</td>
<td>8%</td>
</tr>
<tr>
<td>Boot storm test (XenDesktop power-on operations)</td>
<td>25 min, 8 sec</td>
<td>7,929</td>
<td>3,614</td>
<td>88.50</td>
<td>54.60</td>
<td>0.508</td>
<td>0.448</td>
<td>8.9%</td>
<td>4.8</td>
</tr>
<tr>
<td>Initial login test with mandatory profile</td>
<td>30 min (configured in Login VSI)</td>
<td>27,280</td>
<td>18,516</td>
<td>422</td>
<td>267</td>
<td>0.678</td>
<td>0.548</td>
<td>79%</td>
<td>51%</td>
</tr>
<tr>
<td>Initial login test with roaming profiles</td>
<td>30 min (configured in Login VSI)</td>
<td>48,181</td>
<td>27,855</td>
<td>524</td>
<td>303</td>
<td>1.479</td>
<td>0.813</td>
<td>88%</td>
<td>68%</td>
</tr>
<tr>
<td>Steady-state test with mandatory profile</td>
<td>30 min</td>
<td>19,509</td>
<td>14,859</td>
<td>344</td>
<td>265</td>
<td>0.618</td>
<td>0.544</td>
<td>55%</td>
<td>48%</td>
</tr>
</tbody>
</table>
8.3 Storage Efficiency

In this architecture, because of NetApp storage-efficiency technologies such as thin provisioning and deduplication, only a small amount of space was actually consumed on the SSDs. Of the total 7.62TB capacity required for supporting the write cache files for 2,000 users (both HSD and VDI), only 3.45TB of space was actually consumed throughout the duration of the various tests described in this document. Therefore, we achieved more than 55% data reduction.

The PVS write cache space had the following requirements:

- Storage required for PVS write cache files for 1,000 VDI VMs = 6GB/VM × 1,000 users = 5.86TB
- Storage required for PVS write cache files for 36 HDS VMs = 50GB/VM × 36 users = 1.76TB
- Total storage required for PVS write cache files for 1,000 VDI VMs and 36 HSD VMs = 7.62TB

Note: We used a Login VSI workload generator tool that creates a variety of files during the tests. These workloads might or might not represent your environment. The actual storage-efficiency savings for your environment might be much higher or lower, depending on the similarity of the data between the various users.

8.4 Provisioning 1,000 VDI Desktops

This section describes the test objectives and methodology and provides results from testing the provisioning of 1,000 VDI desktops. We used the Citrix Provisioning Server XenDesktop setup wizard to create desktops. The wizard provisions VMs with write cache drives, if the vDisk is in standard image mode and cache is set as cache on the local hard disk. To format the write cache drive, the wizard automatically boots the VMs in standard image mode with cache on server. After formatting is complete, the VMs are automatically shut down, and XenDesktop can boot the VMs as necessary.

There were six VDI volumes, each with 167 or 166 VMs. We configured one volume with one XenDesktop resource pool. We ran the XenDesktop setup wizard six times to complete the creation of 1,000 VDI desktops. There was very little IOPS or CPU utilization on the storage array during the provisioning.

Test Objectives and Methodology

The objective of this test was to determine how long it would take to provision 167 VDI desktops. Table 22 lists the provisioning data that was gathered.
Table 22) Results for provisioning 167 VDI desktops.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to provisioning 1,000 VDI desktops</td>
<td>66 min (all desktops had a status of Registered in Citrix XenDesktop Studio)</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.476ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>294</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>219</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>12MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>8MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>1%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>1%</td>
</tr>
</tbody>
</table>

**Throughput, IOPS, and Latency**

During the provisioning test, the storage controllers had a combined peak of 294 IOPS, a throughput of 12MB/sec, and an average of 16% utilization per storage controller with an average latency of 0.476ms. Figure 18 shows the throughput, IOPS, and latency for VDI creation. This IOPS is extremely low because PVS clones the write cache file by using VMware vSphere cloning.

**Figure 18**) Throughput, IOPS, and latency for creation of 1,000 VDI desktops.
I/O Read/Write Ratio

Figure 19 shows the I/O reads and writes during the VDI desktop creation. The read/write ratio is approximately 50/50.

Figure 19) I/O read/write ratio during VDI desktop creation.

Customer Impact (Test Conclusions)

During the provisioning of 1,000 VDI desktops, there were extremely low latencies, low CPU utilization, and minimal overall work being done on the storage controller.

8.5 Boot Storm Test

This section describes the test objectives and methodology and provides results from boot storm testing of 1,000 VDI desktops. The 1,000 HSD XenApp users required only 36 Windows 2012 VMs, which is an insignificant VM count compared to the 1,000 VDI Windows 7 VMs. So we focused the boot storm test on the much larger count of VDI desktops (the 1,000 Windows 7 VMs) instead of on the 36 Windows 2012 XenApp VMs.

Test Objectives and Methodology

The objective of this test was to determine how long it would take to boot 1,000 VDI desktops, which might happen, for example, after maintenance activities and server host failures.

This test was performed by powering on 1,000 VDI desktops from within the VMware vCenter server and observing when the status of all VMs in Citrix XenDesktop changed to Registered. Table 23 lists the boot storm data that was gathered.
Table 23) Results for 1,000-VDI desktop boot storm.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to boot 1,000 VDI desktops</td>
<td>8 min, 13 sec (all desktops had a status of Registered in Citrix XenDesktop Studio)</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.406ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>9,516</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>7,463</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>116MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>73MB/sec</td>
</tr>
<tr>
<td>Peak storage controller CPU utilization (all 1,000 VDI VMs were sending the I/O to a single AFF controller)</td>
<td>10%</td>
</tr>
<tr>
<td>Average storage controller CPU utilization (all 1,000 VDI VMs were sending the I/O to a single AFF controller)</td>
<td>8%</td>
</tr>
</tbody>
</table>

Throughput, IOPS, and Latency

During the boot storm test, the storage controllers had a combined peak of 9,516 IOPS, a throughput of 360MB/sec, and an average of 7% CPU utilization per storage controller with an average latency of 0.424ms.

Figure 20 shows the throughput, IOPS, and latency for the boot storm of 1,000 VDI desktops.

Figure 20) Throughput, IOPS, and latency for 1,000-VDI desktop boot storm.
Storage Controller CPU Utilization

Figure 21 shows the storage controller CPU utilization on the node on which the workload was running. The utilization average was 7% with a peak of 10%.

Figure 21) Storage controller CPU utilization for 1,000-VDI desktop boot storm.

Read/Write IOPS

Figure 22 shows the read/write IOPS on write cache volume for the boot storm test. The write cache had more than 90% write available.

Figure 22) Read/write IOPS for 1,000-VDI desktop boot storm.
Customer Impact (Test Conclusions)

During the boot of 1,000 VDI desktops, the storage controller had plenty of headroom to perform a significantly greater number of concurrent boot operations. The results indicated that the storage controller could have booted approximately 2,000 VDI desktops with no problem. At 1,000 VDIs, there was no latency difference between booting from XenDesktop and booting from VMware vCenter.

When we booted the VMs from XenDesktop, there was a throttle on the commands to the VM hosting infrastructure. When a high number of power on/off commands are sent to the VM hosting infrastructure (VMware Virtual Center, XenCenter, and Hyper-V), there is potential for the hosting infrastructure to become overwhelmed and unresponsive for a short period of time while all of the requests are queued and processed. By default, the communication between the pool management service on the Desktop Delivery Controller VM and the hosting infrastructure is throttled to 10% of the total pool. For example, if there are 500 VMs in the desktop group, only 50 VM power operation requests are sent at a time. If pools grow even larger (to more than 1,000 desktops), this might result in more than 100 power on/off requests being sent concurrently to the hosting infrastructure.

Table 24 lists the results for storage latency and boot time for each of the power-on methods.

<table>
<thead>
<tr>
<th>Power-On Method</th>
<th>Concurrent Power-On Operations</th>
<th>Storage Latency</th>
<th>Boot Time for 2,000 VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>From VMware vCenter</td>
<td>No throttle</td>
<td>0.424ms</td>
<td>8 min, 13 sec</td>
</tr>
<tr>
<td>From XenDesktop</td>
<td>10% of the total pool</td>
<td>0.452ms</td>
<td>25 min, 8 sec</td>
</tr>
</tbody>
</table>

8.6 Login, Steady State, and Logout (Login VSI Test) with Mandatory Profiles

This section describes the test objectives and methodology and provides results from steady-state Login VSI testing that included login, steady state, and logout.

Test Objectives and Methodology

The objective of this test was to run a Login VSI 4.1 office worker workload to determine how the storage controller performed and what the end-user experience was like. This Login VSI workload first had the users log in to their desktops and begin working. The login phase occurred over a 30-minute period.

Three different login scenarios were included because each has a different I/O profile. We measured storage performance as well as login time and VSImax, a Login VSI value that represents the maximum number of users who can be deployed on the given platform. VSImax was not reached in any of the Login VSI tests. The following sections define the login scenarios.

Note: All workloads were run on one storage node.

Login VSI Initial Login and Workload Test

In this scenario, 2,000 users (1,000 VDI and 1,000 HSD/XenApp) logged in and downloaded the Login VSI _VSI_Content package containing the user data to be used by Login VSI during the test. This content package is approximately 800MB. Therefore, during the first iteration of the Login VSI test, over 1.6TB of data was downloaded from the storage during the initial 30 minutes and copied to the VMs. Table 25 lists the initial login and workload results.
Table 25) Results for 2,000 users during Login VSI initial login and workload.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average storage latency (ms)</td>
<td>0.546ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>27,280</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>17,736</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>422MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>283MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>79%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>51%</td>
</tr>
</tbody>
</table>

Login VSI VSI max Results

Because the Login VSI VSI max v4.1 was not reached, more VMs could be deployed on this infrastructure. Figure 23 shows the VSI max results.

Figure 23) VSI max results for PVS Login VSI initial login and workload.

Throughput, IOPS, and Latency

During the Login VSI initial login and workload test for 2,000 users, the single storage controller on which all VMs were producing I/O had a peak of 27,280 IOPS, a throughput of 422MB/sec, and an average of 51% CPU utilization with an average latency of 0.546ms. Figure 24 shows the throughput, IOPS, and latency for the login and workload.

**Note:** The testing for all 2,000 users was done using a single storage controller to prove that the two-node AFF8060 storage controller can support 4,000 users and still survive a node failover without affecting end-user experience.
Figure 24) Throughput, IOPS, and latency for 2,000-user XenDesktop Login VSI initial login and workload.

Storage Controller CPU Utilization

Figure 25 shows the storage controller CPU utilization on one node of the two-node NetApp AFF8060 array. The utilization average was 51% with a peak of 79%. All of the workload is on one storage node to prove scalability to 4,000 users.

Figure 25) Storage controller CPU utilization for 2,000-user XenDesktop Login VSI initial login and workload.
Read/Write IOPS

Figure 26 shows the initial login and workload read/write IOPS. Provisioning server write cache volume was more than 90% of write I/O.

Figure 26) Read/write IOPS for 2,000-user XenDesktop PVS write cache volume Login VSI initial login and workload.

Customer Impact (Test Conclusions)

Although the desktop login time of 23 seconds per desktop might be considered a fair login time, the amount of work being performed during this period in our scenario was unusually large and is not typical of customer environments. This initial login copied a significant amount of profile data to prepare for the Login VSI test; therefore, it is not a common situation. Assessments should be performed to determine profile size so that the impact can be understood. Given the worst-case scenario of each user downloading 800MB of data at login, the storage controller performed very well at under 1ms latency and an average of 68% CPU utilization. These numbers indicate that the storage controller is capable of doing significantly more work.

8.7 Login, Steady State, and Logoff (Login VSI Test) with Roaming Profiles

This section describes the test objectives and methodology and provides results from steady-state Login VSI testing.

Test Objectives and Methodology

We put user profiles on an SMB share on a separate hybrid NetApp FAS3240 array with Flash Cache and 600GB 10K RPM SAS drives. During login, the user profiles were copied from the hybrid FAS3240 to the All-Flash FAS8060 system. In organizations, this design is typically used for locked-down environments in which the users are not allowed to make changes to the desktops.
Login VSI Initial Login and Workload Test

In this scenario, 2,000 users logged in and downloaded the Login VSI_VSI_Content package containing the user data to be used by Login VSI during the test. This content package is approximately 800MB. Therefore, during the first iteration of the Login VSI test, over 1.6TB of data was downloaded from the storage during the initial 30 minutes and copied to the VMs. Table 26 lists the initial login and workload results.

Table 26) Results for 2,000-user XenDesktop VSI initial login and workload.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average storage latency (ms)</td>
<td>0.741ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>48,181</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>26,393</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>524MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>334MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>88%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>68%</td>
</tr>
</tbody>
</table>

Desktop Login Time

During the Login VSI initial login, it took approximately 9.6 seconds for VDI desktops and 32 seconds for HSD desktops to log in. 800MB of data had to be copied from the Login VSI share to each desktop.

Figure 27 shows the login time for HSD and VDI desktops. The login time was around 9 seconds for VDI desktops and 30 seconds for HSD desktops.

Figure 27) Scatterplot for PVS Login VSI login times.
Throughput, IOPS, and Latency

During the Login VSI initial login and workload test, the storage controller had a peak of 48,181 IOPS, a throughput of 524MB/sec, and an average of 68% CPU utilization of the node on which 2,000 users were tested with an average latency of 0.741ms. Figure 28 shows the login and workload throughput, IOPS, and latency.

Figure 28) Throughput, IOPS, and latency for 2,000-user XenDesktop Login VSI initial login and workload.
Storage Controller CPU Utilization

Figure 29 shows the storage controller CPU utilization on one node of the NetApp cluster. The utilization average was 68% with a peak of 88%. All of the workload was on one storage node.

Figure 29) Storage controller CPU utilization for 2,000-user XenDesktop desktops Login VSI initial login and workload.

![2,000-User Initial Login, Workload, and Logout](image)

Customer Impact (Test Conclusions)

The desktop login time was 9 seconds for VDI desktops and 31.5 seconds for HSD desktops. Given the worst-case scenario of each user downloading 800MB of data at login, the storage controller performed very well at under 1ms latency and with an average of 68% CPU utilization. These numbers indicate that the storage controller is capable of doing significantly more work.

**Note:** Assessments should be performed to determine profile size so that the impact can be understood.

9 Testing and Validation: Persistent Full-Clone Desktops

This section describes the testing and validation of persistent Citrix XenDesktop full-clone desktops.

9.1 Overview

In the XenDesktop studio, we used the machine catalog setup wizard to create a machine catalog. As shown in Figure 30, we selected Another Service or Technology as the method for deploying machines.
Then we added the VMs created by NetApp VSC to XenDesktop, as shown in Figure 31.

![Figure 30) XenDesktop machine catalog setup wizard.](image)

![Figure 31) XenDesktop machine catalog setup wizard.](image)
Dedicated Desktops

The reference architecture used dedicated desktops with automated assignment. This approach allowed users to be assigned specific desktops.

9.2 Test Results Overview

Table 27 lists the high-level results that were achieved during the reference architecture testing.

<table>
<thead>
<tr>
<th>Test</th>
<th>Time to Complete</th>
<th>Peak IOPS</th>
<th>Peak Throughput</th>
<th>Average Storage Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning 2,000 desktops</td>
<td>139 min</td>
<td>52,709</td>
<td>1.3GB/sec</td>
<td>0.936ms</td>
</tr>
<tr>
<td>Boot storm test (VMware vCenter power-on operations)</td>
<td>6 min, 34 sec</td>
<td>144,288</td>
<td>5.2GB/sec</td>
<td>12.696ms</td>
</tr>
<tr>
<td>Boot storm test during storage failover (VMware vCenter power-on operations)</td>
<td>&lt;12 min</td>
<td>66,456</td>
<td>1.9GB/sec</td>
<td>15.011ms</td>
</tr>
<tr>
<td>Boot storm test (50 concurrent Citrix XenDesktop power-on operations)</td>
<td>10 min, 5 sec</td>
<td>83,414</td>
<td>3.2GB/sec</td>
<td>1.768ms</td>
</tr>
<tr>
<td>Boot storm test during storage failover (50 concurrent Citrix XenDesktop power-on operations)</td>
<td>10 min, 3 sec</td>
<td>65,564</td>
<td>1.81GB/sec</td>
<td>1.578ms</td>
</tr>
<tr>
<td>Login VSI Monday morning login and workload</td>
<td>8.56 sec/VM</td>
<td>21,268</td>
<td>0.7GB/sec</td>
<td>0.650ms</td>
</tr>
<tr>
<td>Login VSI Monday morning login and workload during failover</td>
<td>8.48 sec/VM</td>
<td>20,811</td>
<td>0.7GB/sec</td>
<td>0.762ms</td>
</tr>
<tr>
<td>Login VSI Tuesday morning login and workload</td>
<td>6.95 sec/VM</td>
<td>10,428</td>
<td>0.5GB/sec</td>
<td>0.683ms</td>
</tr>
<tr>
<td>Login VSI Tuesday morning login and workload during failover</td>
<td>8.67 sec/VM</td>
<td>10,848</td>
<td>0.5GB/sec</td>
<td>0.830ms</td>
</tr>
<tr>
<td>Virus scan run (unthrottled)</td>
<td>~51 min</td>
<td>145,605</td>
<td>6.0GB/sec</td>
<td>7.5ms</td>
</tr>
<tr>
<td>Virus scan run (throttled for 80 min)</td>
<td>~80 min</td>
<td>46,940</td>
<td>2.3GB/sec</td>
<td>1.1ms</td>
</tr>
<tr>
<td>Patching 1,000 desktops on one node with 118MB of patches</td>
<td>~20 min</td>
<td>74,385</td>
<td>2.4GB/sec</td>
<td>14.8ms</td>
</tr>
<tr>
<td>Patching 2,000 desktops on one node with 111MB of patches over a 164-minute period with a 5-minute deduplication schedule</td>
<td>164 min</td>
<td>17,979</td>
<td>0.4GB/sec</td>
<td>0.646ms</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

9.3 Storage Efficiency

During the tests, FlexClone technology was used to provision the VMs, and deduplication was enabled. On average, a 9.87:1 deduplication efficiency ratio, or 90% storage efficiency, was observed. This means that 9.87 virtual desktops consumed the storage of one desktop on disk. These high rates are due not only to deduplication but also to the ability of FlexClone technology to instantaneously create storage-efficient virtual desktops. Without these technologies, traditional storage environments would have consumed 31.24TB of
storage. With deduplication and FlexClone technology, 2,000 desktops consumed only 3.16TB of storage, a savings of over 90%. Figure 32 shows the significant difference in storage-efficiency savings.

Figure 32) Storage-efficiency savings.

![Storage-Efficiency Savings](image)

Because of the synthetic nature of the data used to perform these tests, these results are not typical of real-world savings. In addition, although thin provisioning was used for each volume and LUN, thin provisioning is not a storage-reduction technology and therefore was not reported on. Table 28 lists the efficiency results from the testing.

Table 28) Efficiency results.

<table>
<thead>
<tr>
<th>Point of Measurement</th>
<th>Storage Capacity Used</th>
<th>Deduplication Savings</th>
<th>Deduplication Percentage</th>
<th>Deduplication Efficiency Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,000 full-clone desktops</td>
<td>3.16TB</td>
<td>28.07TB</td>
<td>90%</td>
<td>9.87:1</td>
</tr>
</tbody>
</table>

9.4 Test for Provisioning 2,000 Citrix XenDesktop Full Clones (Offloaded to VAAI)

This section describes test objectives and methodology and provides results from testing the provisioning of 2,000 Citrix XenDesktop full clones.

Test Objectives and Methodology

The objective of this test was to determine how long it would take to provision 2,000 Citrix XenDesktop virtual desktops being offloaded to VAAI. This scenario is most applicable to the initial deployment of a new POD of persistent desktops.

Table 29 lists the provisioning data that was gathered.
Table 29) Results for full-clone provisioning of 2,000 virtual desktops.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time for provisioning 2,000 full-clone desktops with VAAI cloning offload</td>
<td>139 min</td>
</tr>
<tr>
<td>Note: All desktops had a status of Registered in Citrix XenDesktop.</td>
<td></td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.936 ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>52,709</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>36,244</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>1279MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>826MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>47%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>32%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

Throughput, IOPS, and Latency

During the provisioning test, the storage controllers had a combined peak of 52,709 IOPS, a throughput of 1279MB/sec, and an average of 32% utilization per storage controller with an average latency of 0.936ms. Figure 33 shows the throughput, IOPS, and latency for full-clone creation.

Figure 33) Throughput, IOPS, and latency for full-clone creation.
Storage Controller CPU Utilization

Figure 34 shows the storage controller CPU utilization across both nodes of the two-node NetApp cluster. The utilization average was 32% with a peak of 47%.

Customer Impact (Test Conclusions)

During the provisioning of 2,000 persistent desktops, the storage controller had enough headroom to perform a significantly greater number of concurrent provisioning operations. On average, the NetApp All-Flash FAS system and systems from other all-flash vendors provision at the rate of approximately 12 to 14 VMs per second. The extremely low latencies, low CPU utilization, and minimal overall work being done on the storage controller appear to indicate that storage performance is not a factor in full-clone provisioning time and therefore should not be used to differentiate platforms.

The offload of the clone creation from the ESXi host to VAAI allowed each of the clones to be created in a fast and storage-efficient manner. The process of cloning through VAAI for VMFS does not copy each block on storage but instead clones ranges of blocks in the LUN that only reference the original blocks. Therefore, the VMs are prededuplicated. This process delivers faster cloning, has less impact on the host, and reduces space during provisioning.

9.5 Boot Storm Test Using vCenter

This section describes test objectives and methodology and provides results from boot storm testing.

Test Objectives and Methodology

The objective of this test was to determine how long it would take to boot 2,000 virtual desktops from VMware vCenter, which might happen, for example, after maintenance activities and server host failures.

This test was performed by powering on all 2,000 VMs from within the VMware vCenter server and observing when the status of all VMs in Citrix XenDesktop changed to Registered. Table 30 lists the boot storm data that was gathered.
Table 30) Results for full-clone boot storm.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to boot 2,000 full-clone desktops using VMware vCenter</td>
<td>6 min, 34 sec</td>
</tr>
<tr>
<td>Note: All desktops had the status Registered in Citrix XenDesktop.</td>
<td></td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>12.695ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>144,288</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>108,882</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>5.10GB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>3.66GB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>84%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>56%</td>
</tr>
<tr>
<td>Note: As explained in the “Storage Controller CPU Utilization” section, the actual average was closer to 81%.</td>
<td></td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

**Throughput, IOPS, and Latency**

During the boot storm test, the storage controllers had a combined peak of 144,288 IOPS, a throughput of 5.1GB/sec, and an average of 56% CPU utilization per storage controller with an average latency of 12.695ms. Figure 35 shows the throughput and IOPS for the full-clone boot storm.

Figure 35) Throughput and IOPS for full-clone boot storm.
Storage Controller CPU Utilization

Figure 36 shows the storage controller CPU utilization across both nodes of the two-node NetApp cluster. The utilization average was 56% with a peak of 84%. Because of the short test length and having a 1-minute capture interval, the time between 0 and 1 minute and 6 and 6:34 in this graph skewed the average significantly. During the period of peak activity after the boot had actually started until it tapered off, the average CPU utilization was closer to 81%.

Figure 36) Storage controller CPU utilization for full-clone boot storm.

Read/Write IOPS

Figure 37 shows the read/write IOPS for the boot storm test.

Figure 37) Read/write IOPS for full-clone boot storm.
Read/Write Ratio

Figure 38 shows the read/write ratio for the boot storm test.

Figure 38) Read/write ratio for full-clone boot storm.

Customer Impact (Test Conclusions)

During the boot of 2,000 persistent desktops, the storage controller had enough headroom to perform a greater number of concurrent boot operations. Booting more desktops might, however, take longer as utilization increases. Citrix XenDesktop also allows you to boot virtual desktops in maintenance mode. Although this exercise took longer, the latency to the storage controller was much less. The focus of this test, however, was not on client latency but on restoring the users’ desktops as quickly as possible.

Table 31 lists the storage latency and boot time results for each power-on method.

Table 31) Power-on method, storage latency, and boot time.

<table>
<thead>
<tr>
<th>Power-On Method</th>
<th>Concurrent Power-On Operations</th>
<th>Average Storage Latency</th>
<th>Boot Time for 2,000 VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>From VMware vCenter</td>
<td>No throttle</td>
<td>12.695ms</td>
<td>6 min, 34 sec</td>
</tr>
<tr>
<td>From Citrix XenDesktop</td>
<td>50</td>
<td>3.2ms</td>
<td>&lt;12 min</td>
</tr>
</tbody>
</table>

9.6 Boot Storm Test Using vCenter During Storage Failover

This section describes test objectives and methodology and provides results from boot storm testing during storage controller failover.

Test Objectives and Methodology

The objective of this test was to determine how long it would take to boot 2,000 virtual desktops if the storage controller had a problem and was failed over. This test used the same methodologies and process that were used in section 8.5, “Boot Storm Test.”

Table 32 shows the data that was gathered for the boot storm during storage failover.
Table 32) Results for full-clone boot storm during storage failover.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to boot 2,000 full-clone desktops during storage failover</td>
<td>8 min, 51 sec</td>
</tr>
<tr>
<td><strong>Note</strong>: All desktops had the status of Registered in Citrix XenDesktop.</td>
<td></td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>42.650ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>73,727</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>51,846</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>2.36GB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>1.13GB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>85%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>61%</td>
</tr>
</tbody>
</table>

**Note**: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

**Throughput, IOPS, and Latency**

During the boot storm failover test, the storage controllers had a combined peak of 73,727 IOPS, a throughput of 2.36GB/sec, and an average of 61% physical CPU utilization per storage controller with an average latency of 42.650ms. Figure 39 shows the throughput, IOPS, and latency.

**Figure 39) Throughput, IOPS, and latency for full-clone boot storm during storage failover.**
Storage Controller CPU Utilization

Figure 40 shows the storage controller CPU utilization on one node of the two-node NetApp cluster while it was failed over. The utilization average was 61% with a peak of 85%.

Figure 40) Storage controller CPU utilization for full-clone boot storm during storage failover.

![Storage Controller CPU Utilization](image)

Read/Write IOPS

Figure 41 shows the read/write IOPS for the boot storm test during storage failover.

Figure 41) Read/write IOPS for full-clone boot storm during storage failover.

![Read/Write IOPS](image)
Read/Write Ratio

Figure 42 shows the read/write ratio for the boot storm test during storage failover.

Customer Impact (Test Conclusions)

During the boot of 2,000 VMware full clones with storage failed over, the storage controller was able to boot 2,000 desktops on one node in 8 minutes and 51 seconds. The VMs in the data from these tests were started by using vCenter. Citrix XenDesktop also makes it possible to boot virtual desktops by enabling a maintenance pool. Tests were conducted to measure the impact of using Citrix XenDesktop to boot the desktops. Although this exercise took longer, the latency to the storage controller was much less. The focus of this test, however, was not on client latency but on restoring the users’ desktops as quickly as possible.

Table 33 lists the storage latency and boot time results for the different power-on methods.

<table>
<thead>
<tr>
<th>Power-On Method</th>
<th>Concurrent Power-On Operations</th>
<th>Average Storage Latency</th>
<th>Boot Time for 2,000 VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>From VMware vCenter</td>
<td>No throttle</td>
<td>42.65ms</td>
<td>8 min, 51 sec</td>
</tr>
<tr>
<td>From Citrix XenDesktop</td>
<td>50</td>
<td>1.578ms</td>
<td>10 min, 3 sec</td>
</tr>
</tbody>
</table>

9.7 Steady-State Login VSI Test

This section describes test objectives and methodology and provides results from steady-state Login VSI testing.

Test Objectives and Methodology

The objective of this test was to run a Login VSI 4.1 office worker workload to determine how the storage controller performed and what the end-user experience was like. This Login VSI workload first had the users log in to their desktops and begin working. The login phase occurred over a 30-minute period.

Three different login scenarios were included because each has a different I/O profile. We measured storage performance as well as login time and VSImax, a Login VSI value that represents the maximum number of users who can be deployed on a given platform. VSImax was not reached in any of the Login VSI tests. The following sections define the login scenarios.
Monday Morning Login and Workload Test

In this scenario, 2,000 users logged in after the VMs had already been logged into once, the profile had been created, and the desktop had been rebooted. During this type of login, user and profile data, application binaries, and libraries had to be read from disk because they were not already contained in the VM memory. Table 34 shows the results.

Table 34) Results for full-clone Monday morning login and workload.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop login time</td>
<td>8.56 sec/VM</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.650ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>21,268</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>12,183</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>690MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>390MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>33%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>19%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

Login VSI VSImax Results

Because the Login VSI VSImax v4.1 was not reached, more VMs could be deployed on this infrastructure. Figure 43 shows the VSImax results for Monday morning login and workload.

Figure 43) VSImax results for full-clone Monday morning login and workload.
Desktop Login Time

Average desktop login time was 8.56 seconds, which is considered an excellent login time. Figure 44 shows a scatterplot of the Monday morning login times.

Figure 44) Scatterplot of full-clone Monday morning login times.

Throughput, IOPS, and Latency

During the Monday morning login test, the storage controllers had a combined peak of 21,268 IOPS, a throughput of 690MB/sec, and an average of 19% CPU utilization per storage controller with an average latency of 0.650ms. Figure 45 shows the throughput, IOPS, and latency for Monday morning login and workload.

Figure 45) Throughput, IOPS, and latency for full-clone Monday morning login and workload.
**Storage Controller CPU Utilization**

Figure 46 shows the storage controller CPU utilization across both nodes of the two-node NetApp cluster. The utilization average was 19% with a peak of 33%.

Figure 46) Storage controller CPU utilization for full-clone Monday morning login and workload.

![Figure 46](image1)

**Read/Write IOPS**

Figure 47 shows the read/write IOPS for Monday morning login and workload.

Figure 47) Read/write IOPS for full-clone Monday morning login and workload.

![Figure 47](image2)
Read/Write Ratio

Figure 48 shows the read/write ratio for Monday morning login and workload.

Figure 48) Read/write ratio for full-clone Monday morning login and workload.

Customer Impact (Test Conclusions)

During the Monday morning login test, the storage controller performed very well. The CPU utilization was not high during this test, latencies were under 1ms, and desktop performance was excellent. These results suggest that it might be possible to double the storage controller workload to 4,000 users or more and still maintain excellent end-user performance. The Monday morning login during storage failover test described in the following section reinforces that point.

Monday Morning Login and Workload During Storage Failover Test

In this scenario, 2,000 users logged in after the VMs had already been logged into once, the profile had been created, and the desktops had been rebooted, but during a storage failover event. During this type of login, user and profile data, application binaries, and libraries had to be read from disk because they were not already contained in the VM memory. Table 35 lists the results for Monday morning login and workload during storage failover.

Table 35) Results for full-clone Monday morning login and workload during storage failover.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop login time during storage failover</td>
<td>8.48 sec</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.779ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>20,811</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>12,939</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>720MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>430MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>64%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>40%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.
Login VSI VSImax Results

Because the Login VSI VSImax v4.1 limit was not reached, more VMs could be deployed on this infrastructure.

Figure 49 shows the VSImax results for Monday morning login and workload during storage failover.

Figure 49) VSImax results for full-clone Monday morning login and workload during storage failover.

Desktop Login Time

Average desktop login time was 8.48 seconds, which is considered an excellent login time, especially during a failover situation. Figure 50 shows a scatterplot of the Monday morning login times during storage failover.

Figure 50) Scatterplot of full-clone Monday morning login times during storage failover.
Throughput, IOPS, and Latency

During the test of Monday morning login during storage failover, the storage controllers had a combined peak of 20,811 IOPS, a throughput of 720MB/sec, and an average of 40% CPU utilization per storage controller with an average latency of 0.779ms. Figure 51 shows the throughput, IOPS, and latency for Monday morning login and workload during storage failover.

Figure 51) Throughput, IOPS, and latency for full-clone Monday morning login and workload during storage failover.

Storage Controller CPU Utilization

Figure 52 shows the storage controller CPU utilization on one node of the two-node NetApp cluster while it was failed over. The utilization average was 40% with a peak of 64%.

Figure 52) Storage controller CPU utilization for full-clone Monday morning login and workload during storage failover.
**Read/Write IOPS**

Figure 53 shows the read/write IOPS for Monday morning login and workload during storage failover.

Figure 53) Read/write IOPS for full-clone Monday morning login and workload during storage failover.

![Monday Morning Login and Workload During Storage Failover](image)

**Read/Write Ratio**

Figure 54 shows the read/write ratio for Monday morning login and workload during storage failover.

Figure 54) Read/write ratio for full-clone Monday morning login and workload during storage failover.

![Monday Morning Login and Workload During Storage Failover](image)

**Customer Impact (Test Conclusions)**

During the Monday morning login test during storage failover, the storage controller performed very well. The CPU utilization averaged less than 50%, latencies were under 1ms, and desktop performance was excellent. These results suggest that for this type of workload it might be possible to double the storage controller workload to 4,000 users total (2,000 per node) with excellent end-user performance and with the ability to tolerate a storage failover.
Tuesday Morning Login and Workload Test

In this scenario, 2,000 users logged in to virtual desktops that had been logged into previously and that had not been power-cycled. In this situation, VMs reduce the impact on storage by retaining user and profile data, application binaries, and libraries in memory. Table 36 lists the results for Tuesday morning login and workload.

Table 36) Results for full-clone Tuesday morning login and workload.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop login time</td>
<td>6.95 sec</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.683ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>10,428</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>7,700</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>503MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>311MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>24%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>17%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.

Login VSI VSImax Results

Because the Login VSI VSImax v4.1 was not reached, more VMs could be deployed on this infrastructure. Figure 55 shows the VSImax results for Tuesday morning login and workload.

Figure 55) VSImax results for full-clone Tuesday morning login and workload.
Desktop Login Time

Average desktop login time was 6.95 seconds, which is considered an excellent login time. Figure 56 shows a scatterplot of the Tuesday morning login times.

Figure 56) Scatterplot of full-clone Tuesday morning login times.

Throughput, IOPS, and Latency

During the test of Tuesday morning login, the storage controllers had a combined peak of 10,428 IOPS, a throughput of 503MB/sec, and an average of 17% CPU utilization per storage controller with an average latency of 0.683ms. Figure 57 shows throughput, IOPS, and latency for Tuesday morning login and workload.

Figure 57) Throughput, IOPS, and latency for full-clone Tuesday morning login and workload.
Storage Controller CPU Utilization

Figure 58 shows the storage controller CPU utilization on one node of the two-node NetApp cluster while it was failed over. The utilization average was 14% with a peak of 24%.

Figure 58) Storage controller CPU utilization for full-clone Tuesday morning login and workload.

Read/Write IOPS

Figure 59 shows the read/write IOPS for Tuesday morning login and workload.

Figure 59) Read/write IOPS for full-clone Tuesday morning login and workload.
Read/Write Ratio

Figure 60 shows the read/write ratio for Tuesday morning login and workload.

Figure 60) Read/write ratio for full-clone Tuesday morning login and workload.

Customer Impact (Test Conclusions)

During the Tuesday morning login test, the storage controller performed very well. The CPU utilization was not high during this test, latencies were under 1ms, and desktop performance was excellent. These results suggest that it might be possible to double the storage controller workload to 4,000 users or more and still maintain excellent end-user performance. The Tuesday morning login during storage failover test described in the following section reinforces that point.

Tuesday Morning Login and Workload During Storage Failover Test

In this scenario, 2,000 users logged in to virtual desktops that had been logged into previously and that had not been power-cycled, and the storage controller was failed over. In this situation, VMs retain user and profile data, application binaries, and libraries in memory, which reduces the impact on storage. Table 37 lists the results for Tuesday morning login and workload during storagefailover.

Table 37) Results for full-clone Tuesday morning login and workload during storage failover.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop login time</td>
<td>8.67 sec</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.830ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>10,848</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>7,410</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>469MB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>296MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>51%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>34%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.
Login VSI VSI\text{max} Results

Because the Login VSI VSI\text{max} v4.1 was not reached, more VMs could be deployed on this infrastructure. Figure 61 shows the VSI\text{max} results for Tuesday morning login and workload during storage failover.

Figure 61) VSI\text{max} results for full-clone Tuesday morning login and workload during storage failover.

![Graph showing VSI\text{max} results for Tuesday morning login and workload during storage failover.]

Desktop Login Time

Average desktop login time was 8.67 seconds, which is considered an excellent login time. Figure 62 shows a scatterplot of the Tuesday morning login times during storage failover.

Figure 62) Scatterplot of full-clone Tuesday morning login times during storage failover.

![Graph showing scatterplot of full-clone Tuesday morning login times during storage failover.]


**Throughput, IOPS, and Latency**

During the test of Tuesday morning login during storage failover, the storage controllers had a combined peak of 10,848 IOPS, a throughput of 469MB/sec, and an average of 34% CPU utilization per storage controller with an average latency of 0.830ms. Figure 63 shows throughput, IOPS, and latency for Tuesday morning login and workload during storage failover.

![Figure 63) Throughput, IOPS, and latency for full-clone Tuesday morning login and workload during storage failover.](image)

**Storage Controller CPU Utilization**

Figure 64 shows the storage controller CPU utilization on one node of the two-node NetApp cluster while it was failed over. The utilization average was 34% with a peak of 51%.

![Figure 64) Storage controller CPU utilization for full-clone Tuesday morning login and workload during storage failover.](image)
Read/Write IOPS
Figure 65 shows the read/write IOPS for Tuesday morning login and workload during storage failover.

Figure 65) Read/write IOPS for full-clone Tuesday morning login and workload during storage failover.

![Tuesday Morning Login and Workload During Storage Failover](image)

Read/Write Ratio
Figure 66 shows the read/write ratio for Tuesday morning login and workload during storage failover.

Figure 66) Read/write ratio for full-clone Tuesday morning login and workload during storage failover.

![Tuesday Morning Login and Workload During Storage Failover](image)

Customer Impact (Test Conclusions)
The purpose of this test was to demonstrate that an ordinary login and workload can be performed during a failover event. This is one of the easier workloads for the storage controller to perform.
9.8 Unthrottled Virus Scan Test

This section describes test objectives and methodology and provides results from unthrottled virus scan testing.

Test Objectives and Methodology

In this test, 2,000 virtual desktops performed a full virus scan. The test was designed to stress the storage infrastructure in order to determine how quickly a virus scan could be performed. To scan the environment, we used virus scan software that was non-VDI-aware and initiated it with the script shown in Figure 67, which starts the virus scan operation on all VMs within a very short period of time.

**Figure 67** Script for starting virus scan on all VMs.

```plaintext
C:\\PSexec.exe -d -accepteula vdi01n01-001 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
C:\\PSexec.exe -d -accepteula vdi01n01-002 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
C:\\PSexec.exe -d -accepteula vdi01n01-003 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
```

**Note:** NetApp does not recommend that customers use this method because there are more VDI-friendly ways of performing a virus scan. In addition, NetApp recommends extending the test to a longer period of time to lessen the impact on the infrastructure.

Table 38 lists the results for the unthrottled virus scan operation.

**Table 38** Results for persistent full-clone unthrottled virus scan operation.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to virus scan 2,000 desktops</td>
<td>~51 min (unthrottled)</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>7.5ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>145,605</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>84,538</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>6.05GB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>4.07GB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>91%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>74%</td>
</tr>
</tbody>
</table>

**Note:** CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.
Throughput, IOPS, and Latency

During the unthrottled virus scan test, the storage controllers had a combined peak of 145,605 IOPS, a throughput of 6.05GB/sec, and an average of 74% CPU utilization per storage controller with an average latency of 7.5ms. Figure 68 shows the throughput, IOPS, and latency for the unthrottled virus scan operation.

Figure 68) Throughput, IOPS, and latency for unthrottled virus scan operations.

Storage Controller CPU Utilization

Figure 69 shows the storage controller CPU utilization across both nodes of the two-node NetApp cluster. The utilization average was 74% with a peak of 91%.

Figure 69) Storage controller CPU utilization for full-clone unthrottled virus scan operation.
Read/Write IOPS

Figure 70 shows the read/write IOPS for the unthrottled virus scan operation.

Figure 70) Read/write IOPS for full-clone unthrottled virus scan operation.

![McAfee Virus Scan of 2,000 Desktops (Unthrottled)](image)

Read/Write Ratio

Figure 71 shows the read/write ratio for the unthrottled virus scan operation.

Figure 71) Read/write ratio for full-clone unthrottled virus scan operation.

![McAfee Virus Scan of 2,000 Desktops (Unthrottled)](image)

Customer Impact (Test Conclusions)

An unthrottled virus scan operation can be performed on all 2,000 desktops in approximately 51 minutes. Although it is possible to run the tests in an unthrottled manner, there is a potential impact to the users' workload. NetApp recommends using a VDI-friendly virus scan solution as well as staggering the schedules of execution over an extended period of time to lessen the impact to the end users.
9.9 Throttled Virus Scan Test

This section describes test objectives and methodology and provides results from throttled virus scan testing.

Test Objectives and Methodology

The throttled virus scan test was designed to perform a virus scan on the infrastructure in a staggered fashion to reduce overall end-user impact. Because the impact to the CPU of the ESXi servers was extremely high in the unthrottled test, only 1,000 desktops were scanned during this test. All 1,000 desktops were located on one node of the storage cluster, so from a storage perspective, the effect was the same as scanning 2,000 desktops across both nodes. Standard physical asset virus scan software was used, and the test was orchestrated by initiating scripts that would remotely execute a full virus scan on each desktop. Ten scripts were run, with each run executing the command and then sleeping for 15 seconds, as set by the choice command. Figure 72 shows the virus scan script.

Figure 72) Virus scan script.

```
C:\\PSexec.exe -d -accepteula \vdi01n01-001 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
choice /T 15 /D y
C:\\PSexec.exe -d -accepteula \vdi01n01-002 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
choice /T 15 /D y
C:\\PSexec.exe -d -accepteula \vdi01n01-003 "C:\Program Files\McAfee\VirusScan Enterprise\scan32.exe" /PRIORITY=LOW /ALL /ALWAYSEXIT
choice /T 15 /D y
```

Note: NetApp does not recommend that customers use this method because there are more VDI-friendly ways of performing virus scan. NetApp also recommends extending the test to a longer period of time to lessen the impact on the infrastructure.

Table 39 lists the results for the throttled virus scan operation.

Table 39) Results for persistent full-clone throttled virus scan operation.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to virus scan 1,000 desktops on one node</td>
<td>~80 min (artificially throtted)</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>1.7ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>46,940</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>35,318</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>2.21GB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>1.66GB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>89%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>71%</td>
</tr>
</tbody>
</table>

Note: CPU and latency measurements are based on the average across both nodes of the cluster. IOPS and throughput are based on a combined total of each.
Throughput, IOPS, and Latency

During the throttled virus scan test, the storage controllers had a combined peak of 46,940 IOPS, a throughput of 2.21GB/sec, and an average of 71% CPU utilization per storage controller with an average latency of 1.7ms. Figure 73 shows the throughput, IOPS, and latency for the throttled virus scan operation.

Figure 73) Throughput, IOPS, and latency for throttled virus scan operations.

Storage Controller CPU Utilization

Figure 74 shows the storage controller CPU utilization across both nodes of the two-node NetApp cluster. The utilization average was 71% with a peak of 89%.

Figure 74) Storage controller CPU utilization for full-clone throttled virus scan operation.
Read/Write IOPS

Figure 75 shows the read/write IOPS for the throttled virus scan operation.

Figure 75) Read/write IOPS for full-clone throttled virus scan operation.

![McAfee Virus Scan of 1,000 Desktops (Throttled for 80-Minute Run)](image)

Read/Write Ratio

Figure 76 shows the read/write ratio for the throttled virus scan operation.

Figure 76) Read/write ratio for full-clone throttled virus scan operation.

![McAfee Virus Scan of 1,000 Desktops (Throttled for 80-Minute Run)](image)

Customer Impact (Test Conclusions)

A throttled virus scan operation can be performed on all 2,000 desktops in 51 minutes.

9.10 Test for Patching 1,000 Desktops on One Node

This section describes test objectives and methodology and provides results from patch testing.

Test Objectives and Methodology

In this test, we patched 1,000 desktops on one node of the storage infrastructure. As with the throttled virus scan test, we were cautious and didn’t want the server hosts become a bottleneck during this unthrottled test. The results for 1,000 desktops on one node were very similar to what would be seen across two nodes at 2,000 desktops for this workload.
For testing, we used Windows Server Update Server (WSUS) to download and install patches to the 1,000 desktops. A total of 118MB of patches were downloaded and installed on each machine. The patch update was initiated from a Windows PowerShell script that directed each VM to find available updates from the WSUS, apply the patches, and reboot the VMs. Table 40 lists the test results for patching 1,000 desktops on one node.

Table 40) Results for patching 1,000 persistent full clones on one node.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to virus scan 2,000 desktops</td>
<td>~23 min</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>14.783ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>74,385</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>20,998</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>2.35GB/sec</td>
</tr>
<tr>
<td>Average throughput</td>
<td>1.01GB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>92%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>61%</td>
</tr>
</tbody>
</table>

**Note:** CPU and latency measurements are based on one node of the cluster.

**Throughput, IOPS, and Latency**

During the patching test, the storage controller had a peak of 74,385 IOPS, a throughput of 2.35GB/sec, and an average of 61% CPU utilization per storage controller with an average latency of 14.783ms. Figure 77 shows the throughput, IOPS, and latency for the patching of 1,000 persistent full clones on one node.

Figure 77) Throughput, IOPS, and latency for patching 1,000 persistent full clones on one node.
Storage Controller CPU Utilization

Figure 78 shows the storage controller CPU utilization of one node of the two-node NetApp cluster. The utilization average was 61% with a peak of 92%.

Figure 78) Storage controller CPU utilization for patching 1,000 persistent full clones on one node.

Read/Write IOPS

Figure 79 shows the read/write IOPS for patching 1,000 persistent full clones on one node.

Figure 79) Read/write IOPS for patching 1,000 persistent full clones on one node.
Read/Write Ratio

Figure 80 shows the read/write ratio for patching 1,000 persistent full clones on one node.

Customer Impact (Test Conclusions)

The patching of 1,000 (or 2,000) virtual desktops with 118MB per VM took approximately 23 minutes to install and reboot the VM. Latency or CPU was not a concern during this test. In production environments, NetApp recommends staggering patching over a longer period of time to reduce latency and CPU utilization.

9.11 Test for Aggressive Deduplication While Patching 2,000 Desktops

This section describes test objectives and methodology and provides results from testing an aggressive deduplication schedule while patching 2,000 desktops.

Test Objectives and Methodology

During this test, 2,000 VMs were deployed and were running on one node of the two-node cluster, which was accomplished by performing an aggregate relocate operation from one node to the other. Then an aggressive deduplication schedule of 5 minutes was set for each of the 10 volumes. WSUS was set up to deploy 9 critical patches to each of the 2,000 Windows 7 VMs. The nine critical patches totaled 111MB for a grand total of 218GB of data. The patch update was initiated from a Windows PowerShell script that directed each VM to find available updates from the WSUS, apply the patches, and reboot the VMs.

Table 41 lists the results of the test for patching 2,000 desktops on one node.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to patch 2,000 desktops</td>
<td>164 min</td>
</tr>
<tr>
<td>Average storage latency (ms)</td>
<td>0.646ms</td>
</tr>
<tr>
<td>Peak IOPS</td>
<td>17,979</td>
</tr>
<tr>
<td>Average IOPS</td>
<td>12,401</td>
</tr>
<tr>
<td>Peak throughput</td>
<td>400MB/sec</td>
</tr>
<tr>
<td>Measurement</td>
<td>Data</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Average throughput</td>
<td>280MB/sec</td>
</tr>
<tr>
<td>Peak storage CPU utilization</td>
<td>59%</td>
</tr>
<tr>
<td>Average storage CPU utilization</td>
<td>42%</td>
</tr>
</tbody>
</table>

**Note:** CPU and latency measurements are based on one node of the cluster.

**Throughput, IOPS, and Latency**

During the test of aggressive deduplication during patching, the storage controllers had a peak of 17,979 IOPS, a throughput of 400MB/sec, and an average of 42% CPU utilization per storage controller with an average latency of 0.646ms. Figure 81 shows the throughput, IOPS, and latency for the test of aggressive deduplication during patching.

**Figure 81**) Throughput, IOPS, and latency for aggressively deduplicating and patching 2,000 persistent full clones on one node.

**Figure 82**) Storage controller CPU utilization for aggressively deduplicating and patching 2,000 persistent full clones on one node.

**Storage Controller CPU Utilization**

Figure 82 shows the storage controller CPU utilization of one node of the two-node NetApp cluster. The utilization average was 42% with a peak of 59%.

**Figure 82**) Storage controller CPU utilization for aggressively deduplicating and patching 2,000 persistent full clones on one node.
Read/Write IOPS

Figure 83 shows the read/write IOPS for aggressively deduplicating and patching 2,000 persistent full clones on one node.

Figure 83) Read/write IOPS for aggressively deduplicating and patching 2,000 persistent full clones on one node.

Read/Write Ratio

Figure 84 shows the read/write ratio for aggressively deduplicating and patching 2,000 persistent full clones on one node.

Figure 84) Read/write ratio for aggressively deduplicating and patching 2,000 persistent full clones on one node.

Customer Impact (Test Conclusions)

The patching of 2,000 virtual desktops with 111MB of patches can be completed over a 2-hour period with excellent storage CPU utilization and latency. These results can all be achieved while aggressively running deduplication every 5 minutes, which allows the storage controller to maintain maximum storage efficiency and consistent performance while applying patches. During this test, the combination of FlexClone technology and deduplication saved 28.07TB, which translates into a 9.87:1, or 90%, storage efficiency.

10 Additional Reference Architecture Testing

Since the release of this document, many new storage technologies have been introduced. This section provides new information about these topics.
10.1 Always-On Deduplication

Typical storage sizing for VDI environments includes sizing for headroom to prevent the end-user experience from being affected in the event of a storage failover. This extra CPU headroom for storage failover is not typically used during normal operations. In the case of VDI, this headroom provides an excellent advantage for storage vendors with true active-active storage systems. When an All-Flash FAS8000 is used, it is possible to use deduplication with a very aggressive deduplication schedule to maintain storage efficiency over time. To eliminate any potential concerns that always-on deduplication might cause additional wear on the SSDs, NetApp provides up to a five-year warranty (a three-year standard warranty, plus the offer of an additional two-year extended warranty, with no restrictions on the number of drive writes) with all SSDs.

Always-On Deduplication Use Case Testing

In the NetApp Solutions Lab, we have performed many tests to determine whether and how to use always-on deduplication. We used a FAS8060 with a shelf and a half of 400GB SSDs. We completely aged the storage system (which has no effect on client latencies with All-Flash FAS). We created four FlexVol® volumes and presented them to the ESXi hosts. We created a storage efficiency policy that scheduled deduplication to run every minute and set the QoS policy to background. We then created 800 Windows 7 VMs and applied 1GB of Windows updates to each VM. We staggered the patch application so that we would patch a new machine every 30 seconds. Figure 85 shows the Add Efficiency Policy user interface.

Figure 85) Configuring efficiency policy for always-on deduplication.

Always-On Deduplication Use Case Findings

In looking at the results, we found that we could save almost 25% of the time over patching and then running postprocess deduplication. We required 56% less space than using postprocess deduplication. The average storage controller latency was under 1ms for the duration of the patch and always-on deduplication tests. The storage controller was able to ingest 250MB/sec to 300MB/sec with a peak ingest rate of 500MB/sec to 600MB/sec. In Figure 86 and Figure 87, the top line represents the four volumes during the patch (rise) and postprocess deduplication (fall) at the 200-minute mark. The bottom line represents the four volumes during patching with postprocess deduplication.
In Figure 87, the latencies are compared between patch and postprocess deduplication in red and always-on deduplication in blue. Average latencies with always-on deduplication were under 1ms.

**Requirements for Always-On Deduplication**

The following components are required in order to use always-on deduplication:

- All-Flash FAS8000
- Data ONTAP 8.2.2 or later

**Best Practice**

- Size the storage controller properly so that users are not affected if a storage failover occurs. NetApp recommends testing storage failover during normal operations.
- Stagger patching activities over a period of time.
- Have at least eight volumes per node for maximum deduplication performance.
- Set the efficiency policy schedule to one minute.
- Set the QoS policy for the storage efficiency policy to background.
- Monitor the storage system performance with OnCommand® Performance Monitor as well as a desktop monitoring utility such as Liquidware Labs Stratusphere UX to measure the client experience.
- Disable deduplication in the event of a storage failover if client latencies increase.
10.2 Inline Zero Detection and Elimination in Data ONTAP 8.3

Data ONTAP 8.3 introduced a storage efficiency technology that provides inline zero detection and elimination. Zeros are written to a storage controller in two different situations. The first is when VMDKs are used on VMFS. Each time a thin or lazy zero thick VM is written to, blocks must be zeroed before the data is written. When NFS is used, only in the case of lazy zero thick are the blocks zeroed before use. With both VMFS and NFS, eager zero thick VMs are zeroed at VMDK creation. The second case is for normal data zeroes. The elimination of any write to media helps to improve performance and extend media lifespan. Table 42 shows VMDK disk types and protocols.

<table>
<thead>
<tr>
<th>VMDK Type</th>
<th>NFS</th>
<th>VMFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thin</td>
<td></td>
<td>Zeroed on use</td>
</tr>
<tr>
<td>Lazy zero thick</td>
<td>Reserved</td>
<td>Reserved and zeroed on use</td>
</tr>
<tr>
<td>Eager zero thick</td>
<td>Reserved and zeroed</td>
<td>Reserved and zeroed</td>
</tr>
</tbody>
</table>

Inline zero elimination is a way to reduce writes to disk; instead of writing the zero and then performing postprocess deduplication, this method involves only a metadata update. Deduplication must be turned on for the volume, at a minimum. Scheduled deduplication does not have to take place. By enabling deduplication, Data ONTAP inline zero elimination provides approximately 20% faster cloning of eager zero thick VMDKs. It eliminates the need to deduplicate the zeroes from the VMs postprocess, thus increasing disk longevity.

**Best Practice**

- Put the templates in the destination datastore.
- Enable deduplication on the volume; a schedule is not required.
- When NFS is used, thin-provisioned disks are best because they provide end-to-end utilization transparency and have no upfront reservation, which drives higher storage utilization.
- When VMFS is used, eager zero thick disks are the best format. Using this format conforms to the VMware best practice for getting the best performance from a virtual infrastructure. Cloning time is faster with eager zero thick provisioning than with thin provisioning on VMFS datastores.

10.3 Advanced Drive Partitioning

Advanced drive partitioning distributes the root file system across multiple disks within an HA pair. It allows higher overall capacity utilization by removing the need for dedicated root and spare disks. This feature is available in Data ONTAP 8.3.

11 Conclusion

In all tests for both persistent and nonpersistent desktop use cases, end-user login time, guest response time, and maintenance activities performance were excellent. The NetApp All-Flash FAS system performed very well for the variety of tests, reaching peak IOPS of 48,181 during login storm with roaming profiles while averaging 50% CPU utilization on the storage node on which the tests were running. All test categories demonstrated that with the 2,000-user workload tested in this solution, the All-Flash FAS8060 storage system could be doubled up to 4,000 users while still being able to fail over in the event of a failure.

For nonpersistent desktops, the following key findings were observed during the reference architecture testing:

- The NetApp All-Flash FAS solution was able to very easily meet all IOPS requirements of the 2,000-user workload (boot, login, steady state, logout) at an ultra-low latency of approximately 1ms, delivering excellent end-user experience. The storage configuration could easily support up to 4,000 users.
• During all login and workload scenarios, the Login VSI VSImax was not reached.
• During boot storm testing, VMware vCenter did not throttle the boot process and produced an excellent boot time of 8 minutes and 13 seconds for all 2,000 VMs.
• HSD and VDI desktops with roaming profiles require more IOPS than desktops with mandatory profiles because a single mandatory profile is kept on the file servers instead of keeping thousands of roaming profiles.

For persistent desktops, the following key findings were observed during the reference architecture testing:
• The NetApp All-Flash FAS solution was able to very easily meet all IOPS requirements of the 2,000-user workload (boot, login, steady state, logout, AV scans, patch storms) at an ultra-low latency of approximately 1ms, delivering an excellent end-user experience. The storage configuration could easily support up to 4,000 users.
• During all login and workload scenarios, the Login VSI VSImax was not reached.
• During boot storm testing, VMware vCenter did not throttle the boot process and produced an excellent boot time of 6 minutes and 34 seconds for all 2,000 VMs.
• For all of the nonfailover tests, almost twice as many users could have been deployed with the same results. Only in the cases of the failed-over boot storm and initial login and workload did the CPU average over 50%.
• Deduplication can be run with an aggressive schedule of 5 minutes to provide near real-time storage efficiency.
• Deduplication and FlexClone technology storage efficiency saved over 28.07TB of storage, which translates into a savings of 9.87:1, or 90%.

12 References
The following references were used in this technical report:
TR-3982: NetApp Clustered Data ONTAP 8.3 and 8.2.x: An Introduction
TR-4138: Citrix XenDesktop on NetApp Storage Solution Guide
http://www.netapp.com/as/media/tr-4138.pdf
Citrix XenDesktop 7.6 Blueprint
Citrix Product Document on XenApp 7.5 and XenDesktop 7.5
Virtual Storage Console 5.0 for VMware vSphere: Installation and Administration Guide
https://library.netapp.com/ecm/ecm_get_file/ECMP1392339

13 Acknowledgements
The authors thank Bhavik Desai, John George, Abhinav Joshi, Scott Lane, Rob McDonald, and Kim White (NetApp) and Rob Briggs (Citrix) for their contributions to this document.
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, Snap Creator, SnapCopy, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, WAFL and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the Web at http://www.netapp.com/us/legal/netapptmlist.aspx, TR-4342-0415