Abstract
This document introduces the NetApp® HCI solution to infrastructure administrators and provides important design paradigms to consider when using NetApp HCI solutions for VMware Horizon. The document talks about VMware End-User Computing, VMware Horizon View, and hyper converged infrastructure (HCI) and it discusses architectural considerations for Horizon View that runs in the context of NetApp HCI. By following the guidelines in this document, you can learn how to effectively design and implement VMware Horizon View on NetApp HCI. This updated document also has added data on the sizing of the NetApp HCI H700E nodes, instant clones, and the impact of patching to address the Spectre and Meltdown vulnerabilities.
TABLE OF CONTENTS

1 NetApp HCI Introduction ........................................................................................................ 5
   1.1 NetApp HCI Quality of Service ....................................................................................... 5
   1.2 Enterprise Scale ............................................................................................................ 5
   1.3 Streamlined Operations ................................................................................................. 5
   1.4 Configuration ................................................................................................................ 6

2 Transforming from VDI to End-User Computing ................................................................. 7
   2.1 VMware Horizon and Instant Clones ............................................................................. 8
   2.2 VMware App Volumes ................................................................................................. 9
   2.3 Workspace ONE ........................................................................................................... 9

3 NetApp HCI Solution Configuration .................................................................................... 10
   3.1 HCI Infrastructure ........................................................................................................ 10
   3.2 NetApp Deployment Engine ......................................................................................... 11
   3.3 Compute Configuration ............................................................................................... 11
   3.4 Storage Configuration .................................................................................................. 11
   3.5 Virtual Machine Configuration .................................................................................... 13
   3.6 Windows Desktop Template ....................................................................................... 14

4 About Login VSI .................................................................................................................. 18
   4.1 Objective testing with Login VSI ................................................................................. 18
   4.2 How Login VSI works ................................................................................................. 19

5 VMware Horizon View DesktopTesting with Login VSI ....................................................... 19
   5.1 Testing Objectives ....................................................................................................... 19
   5.2 Tests and Results ......................................................................................................... 19
   5.3 VMware Horizon View Common Maintenance Operations ........................................... 23
   5.4 Storage Sizing .............................................................................................................. 24

6 Additional Performance Analysis ......................................................................................... 24
   6.1 Large NetApp HCI H700E Compute Node Performance Validation .............................. 24
   6.2 Instant Clone Scalability ............................................................................................... 25
   6.3 Spectre and Meltdown Performance Analysis .............................................................. 26

Acknowledgments .................................................................................................................. 32

Where to Find Additional Information .................................................................................. 32

Version History ...................................................................................................................... 32

LIST OF TABLES
Table 1) NetApp HCI configuration compute nodes. ................................................................. 6
Table 2) NetApp HCI configuration storage nodes. ................................................................. 6
Table 3) Compute configuration for testing. ........................................................................... 10
Table 4) Storage configuration for testing. ............................................................................. 10
Table 5) Infrastructure VMs. ................................................................................................. 13
Table 6) H300E single–compute node test Login VSI metrics. ............................................. 20
Table 7) H300E six–compute node test Login VSI metrics .................................................... 21
Table 8) H300E seven–compute node test Login VSI metrics .............................................. 22
Table 9) VMware Horizon maintenance operations. .............................................................. 24
Table 10) Linked-clone density based on the Login VSI knowledge worker load. ................. 25
Table 11) Instant Clone density based on the Login VSI knowledge worker load. ................. 26
Table 12) Differences between Spectre and Meltdown testing and previous testing. .......... 27
Table 13) Prepatch and postpatch software versions. ............................................................... 27
Table 14) Spectre and Meltdown prepatch and postpatch test result summary. ...................... 32

LIST OF FIGURES

Figure 1) Minimum configuration. ......................................................................................... 6
Figure 2) VMware EUC solution with Workspace ONE. ........................................................ 8
Figure 3) App Volumes solution. ............................................................................................ 9
Figure 4) NetApp HCI hardware configuration for testing. .................................................... 10
Figure 5) NetApp Deployment Engine. .................................................................................. 11
Figure 6) NetApp HCI vCenter plug-in for storage management. ........................................... 12
Figure 7) Creating a datastore. ............................................................................................. 12
Figure 8) Edit vCenter Server advanced settings. ................................................................. 14
Figure 9) Updating the VMware OSOT template. ................................................................. 17
Figure 10) VMware OSOT before optimizations. ................................................................. 17
Figure 11) VMware OSOT after successful optimizations. .................................................. 18
Figure 12) H300E single–compute node test VSI max v4 graph. ........................................... 21
Figure 13) H300E six–compute node test VSI max v4 graph ................................................ 22
Figure 14) H300E seven–compute node test VSI max v4 graph .......................................... 23
Figure 15) Login VSI metrics across the three tests. .............................................................. 23
Figure 16) H700E single–compute node test VSI max v4 graph .......................................... 25
Figure 17) H300E Instant Clone density results. .................................................................... 26
Figure 18) H700E Instant Clone density results. .................................................................... 26
Figure 19) Example of unpatched Windows 10 operating system Speculation Control output. ........................................................................................................................................... 28
Figure 20) Example of patched Windows 10 operating system Speculation Control output. ........................................................................................................................................... 28
Figure 21) Patch testing methodology. .................................................................................. 29
Figure 22) H300E Login VSI results before patching for Spectre and Meltdown. ................. 30
Figure 23) H300E Login VSI results after patching for Spectre and Meltdown. .................... 30
Figure 24) H700E Login VSI results before patching for Spectre and Meltdown. ................. 31
Figure 25) H700E Login VSI results after patching for Spectre and Meltdown.
1 NetApp HCI Introduction

NetApp HCI is an enterprise-scale hyper converged infrastructure (HCI) solution that is well suited for customers who are looking to break free from first-generation HCI limitations.

As a NetApp HCI customer, you can run multiple applications with guaranteed performance to confidently deploy resources across your entire data center. By simplifying management, the architecture enables you to easily deploy your infrastructure, and you can independently scale both compute and storage resources. NetApp HCI is Data Fabric ready out of the box, for easy access to all your data across any public, private, or hybrid cloud. By moving to NetApp HCI, your IT organization can transform your data center, driving operational efficiencies and reducing costs.

Data Fabric is a software-defined approach from NetApp for data management that enables you to connect disparate data management and storage resources. NetApp HCI can streamline data management between on-premises and cloud storage for enhanced data portability, visibility, and protection.

1.1 NetApp HCI Quality of Service

A common challenge for a data center is to deliver predictable performance, which is complicated even more by running multiple applications that share the same infrastructure. An application that interferes with other applications creates performance degradations, causing IT administrators to spend valuable time on troubleshooting the environment. When they are deployed in a shared environment, mainstream applications, such as virtual desktop infrastructure (VDI) and database applications, have unique I/O patterns that can affect one another’s performance during normal operations.

The NetApp HCI quality-of-service (QoS) feature enables fine-grained control of performance for every application, eliminating noisy neighbors, meeting unique performance needs, allowing higher utilization of infrastructure, and satisfying agreed-upon performance SLAs. The storage architecture, which is part of the NetApp HCI solution, eliminates performance variance in the context of data locality because the data is distributed across all the nodes in the HCI cluster.

1.2 Enterprise Scale

Unlike previous generations of HCI that have fixed resource ratios, NetApp HCI scales compute and storage resources independently. Independent scaling avoids costly and inefficient overprovisioning and simplifies capacity and performance planning. Running on innovative NetApp SolidFire® Element® OS technology and delivered on a NetApp designed architecture, NetApp HCI is an enterprise-scale HCI solution. NetApp HCI comes in 2RU 4-node building blocks (chassis) in small, medium, and large storage and compute configurations that can be mixed and matched. You can scale HCI to rapidly meet your changing business needs on your terms.

1.3 Streamlined Operations

A common goal of IT organizations is to automate all routine tasks. Such automation helps eliminate the risk of user errors that are associated with manual operations and allows valuable resources to be focused on higher-value priorities that drive business efficiencies. The NetApp Deployment Engine (NDE) streamlines day 0 installation from hours to minutes, and simple centralized management through the vCenter plug-in gives you full control over managing your entire infrastructure through an intuitive UI. A robust suite of APIs enables additional seamless integration into higher-level management, orchestration, backup, and disaster recovery tools.
1.4 Configuration

NetApp HCI is available with configuration options of small, medium, or large for both compute and storage. The nodes are similar to a small blade that sits inside a chassis. A minimum starting configuration must have four storage nodes and two compute nodes (Figure 1).

![Figure 1) Minimum configuration.](image)

As the configuration information in Table 1 shows, 16 to 36 CPU cores and 384GB to 768GB of RAM are available for compute nodes. From a storage node perspective, depending on the configuration size, a storage node can deploy from 5.5TB to 44TB of effective capacity, as shown in Table 2.

Table 1) NetApp HCI configuration compute nodes.

<table>
<thead>
<tr>
<th></th>
<th>H300E (Small)</th>
<th>H500E (Medium)</th>
<th>H700E (Large)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU</td>
<td>1RU, half-width</td>
<td>1RU, half-width</td>
<td>1RU, half-width</td>
</tr>
<tr>
<td>Cores for VMs</td>
<td>16</td>
<td>24</td>
<td>36</td>
</tr>
<tr>
<td>CPU</td>
<td>E5-2620 v4: 8C at 2.1GHz</td>
<td>E5-2650 v4: 12C at 2.2GHz</td>
<td>E5-2695 v4: 18C at 2.1GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>384GB</td>
<td>512GB</td>
<td>768GB</td>
</tr>
<tr>
<td>Boot device</td>
<td>1 x 240GB MLC</td>
<td>1 x 240GB MLC</td>
<td>1 x 240GB MLC</td>
</tr>
<tr>
<td>Base networking</td>
<td>4 x 25/10GbE SFP28/SFP+ 2 x 1GbE RJ-45</td>
<td>4 x 25/10GbE SFP28/SFP+ 2 x 1GbE RJ-45</td>
<td>4 x 25/10GbE SFP28/SFP+ 2 x 1GbE RJ-45</td>
</tr>
</tbody>
</table>

Table 2) NetApp HCI configuration storage nodes.

<table>
<thead>
<tr>
<th></th>
<th>H300S (Small)</th>
<th>H500S (Medium)</th>
<th>H700S (Large)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU</td>
<td>1RU, half-width</td>
<td>1RU, half-width</td>
<td>1RU, half-width</td>
</tr>
<tr>
<td>CPU</td>
<td>E5-2620 v4: 8C at 2.1GHz</td>
<td>E5-2650 v4: 12C at 2.2GHz</td>
<td>E5-2695 v4: 18C at 2.1GHz</td>
</tr>
<tr>
<td>Boot device</td>
<td>1 x 240GB MLC</td>
<td>1 x 240GB MLC</td>
<td>1 x 240GB MLC</td>
</tr>
</tbody>
</table>
For example, for a minimum-size starting solution, a configuration with two small compute and four small storage nodes could have 36 cores with 768GB of memory and from 22TB to 44TB of effective capacity. As requirements change, you can add more compute or storage nodes of any size to the chassis independently of each other. This flexibility in adding only compute or only storage nodes enables unique scalability options for building an efficient and agile cloud in your data center for various use cases.

2 Transforming from VDI to End-User Computing

Despite the many advantages of End-User Computing (EUC) solutions—centralized management, increased security, and easy accessibility, to name a few—many organizations have been slow to adopt them. User expectations can be difficult to satisfy, and the complexity and cost of deploying and scaling VDI and virtualized application solutions often derail projects before they get started.

By untethering the digital workspace and by enabling collaboration, EUC is an important enabler of digital transformation. VDI is only the first step on the path to a complete EUC environment. To promote user productivity, you must also accelerate the key applications and databases on which users rely, matching the efficiency of virtual desktops. However, this more comprehensive approach to EUC creates some significant business and technical challenges.

Addressing unpredictable user workloads in a complicated EUC environment can require painful re-architecting. By introducing new workloads, you might rob resources from existing workloads, leaving users unhappy. You need a better approach to infrastructure for EUC. With NetApp HCI, you can mix the different workloads within an EUC environment while protecting user applications and user data from desktop workloads.

With solutions to improve the end-user experience and usability, NetApp and VMware can help in your digital transformation from VDI to EUC. The following sections present some of the VMware technologies that are a critical part of this transformation.
2.1 VMware Horizon and Instant Clones

VMware Horizon 7 introduced Instant Clone virtual desktops to the market in 2016. These clones significantly improved the provisioning time of virtual desktops, allowing customers to move to a Just-in-Time provisioning model. VMware Instant Clones provide the administrator and customers with many benefits, some of which are listed in the following subsections.

Administrative Benefits

As a benefit to administrators, this technology:

- Reduces the time and effort that are associated with deployment and patching of virtual desktops
- Reduces the need for spare desktops that run on the infrastructure
- Eliminates boot storms and refresh, recompose, and rebalance maintenance operations
- Eliminates the need for a View Composer server and an associated database
-Eliminates the need to perform space reclamation on Virtual Machine Disks (VMDKs)
- Eliminates the need for Content-Based Read Cache (CBRC) digest re-creation

End-User Benefits

End users benefit because:

- Instant clones are immediately available for users to log in to.
- Users can get a new desktop each time that they log in.

You can find more information about Instant Clone technology:

- [VMware Instant Clone Technology for Just-In-Time Desktop Delivery in Horizon 7 Enterprise Edition](#)
- [Get Started with VMware Instant Clone Technology in VMware Horizon 7](#)
2.2 VMware App Volumes

App Volumes (Figure 3) is a set of user management and application delivery solutions. App Volumes is designed to simplify user management and to provide the user with faster application delivery as well as a customizable and persistent user experience.

App Volumes uses a read-only VMDK that contains one or more preinstalled applications, known as an AppStack. Each AppStack can be attached to one or more virtual machines (VMs) based on the user’s entitlements.

The second component of App Volumes is known as a Writable Volume. This component is a read/write VMDK that is provisioned to an individual user and is attached to the user’s virtual desktop. The Writable Volume is used to store the user’s data, the user’s profiles (desktop settings such as wallpaper and a screensaver), and user-installed applications.

To provide the user with a faster experience, App Volumes is often used in conjunction with VMware Instant Clones. A VMware Instant Clone is dynamically created when the user logs in, then an AppStack is attached. A Writable Volume is then attached to provide the user with a customizable and persistent experience.

![App Volumes solution](image)

2.3 Workspace ONE

VMware Workspace ONE is a unified enterprise platform that manages and secures delivery of any application on any device. Workspace ONE integrates identity, application, and enterprise mobile device management. With the Workspace ONE unified platform, administrators can easily manage user access and endpoints, all from a single interface. It provides single sign-on (SSO) and multifactor authentication (MFA) so that users can securely access their entitled applications. These applications are presented in a catalog that can contain any mobile, web, cloud, or Microsoft Windows applications, including hosted applications. All these features help improve the security and the compliance of a user’s digital environment.

Key Values of Workspace ONE

Workspace ONE provides the following key benefits:

- Encryption
- Passcodes
• Data loss prevention
• Remote lock and wipe
• Patch management

3 NetApp HCI Solution Configuration

3.1 HCI Infrastructure

To prove the value of NetApp HCI, we performed testing. For our testing, we used three NetApp HCI chassis (6RU), for a total of 12 nodes (Figure 4). Eight small compute nodes were logically divided into two different vSphere clusters to serve the desktops and the infrastructure VMs. We created a third cluster and used it to host the unused ESXi nodes during the different phases of the testing.

Figure 4) NetApp HCI hardware configuration for testing.

![NetApp HCI hardware configuration for testing.](image)

We isolated the infrastructure ESXi host so that we could accurately measure the virtual desktop density. Because Element OS has advanced QoS capabilities to protect the infrastructure from the desktops during activities such as boot and login storms, NetApp does not normally recommend splitting the desktops from the infrastructure. Table 3 and Table 4 contain the compute and storage configurations, respectively, for this testing, and they list the compute, memory, network, and storage capacities of the configurations.

Table 3) Compute configuration for testing.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Type</th>
<th>Node Count</th>
<th>CPU</th>
<th>Memory</th>
<th>Network (Used)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktops</td>
<td>H300E</td>
<td>7</td>
<td>235.2GHz</td>
<td>2688GB</td>
<td>2 x 25GbE*</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>H300E</td>
<td>1</td>
<td>33.6GHz</td>
<td>384GB</td>
<td>2 x 25GbE*</td>
</tr>
</tbody>
</table>

* The compute nodes have four 10/25GB network interfaces, but only two were used in this testing.

Table 4) Storage configuration for testing.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Type</th>
<th>Node Count</th>
<th>Drives (per Node)</th>
<th>Effective Capacity</th>
<th>Network (per Node)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All workloads</td>
<td>H300S</td>
<td>4</td>
<td>6 x 480GB</td>
<td>5.5TB–11TB</td>
<td>2 x 25GB</td>
</tr>
</tbody>
</table>
3.2 NetApp Deployment Engine

The NetApp Deployment Engine (NDE, Figure 5) enables you to quickly deploy NetApp HCI. As part of the deployment process, you can optionally deploy VMware vCenter Server. You can also let the NetApp Deployment Engine automatically set many of the networking configuration details for you, or you can control networking configuration at the advanced level. For more information about the NetApp Deployment Engine, consult the HCI NDE User Guide.

Figure 5) NetApp Deployment Engine.

3.3 Compute Configuration

For our testing, VMware vSphere 6.0 was installed on the compute nodes by the NetApp Deployment Engine. These nodes were then configured to support multiple virtual LANs (VLANs) for the desktops to be isolated from the infrastructure VMs. No other configuration was needed beyond the additional VLANs.

3.4 Storage Configuration

We used four small HCI storage nodes for this test. The system was sized to deliver 5.5TB of effective capacity, assuming 5 times the storage efficiency with up to 200,000 IOPS of storage performance. We used the HCI storage cluster for both the desktops and the infrastructure VMs.

Volume Configuration

For all the storage management tasks, we used the NetApp HCI vCenter plug-in (Figure 6). This plug-in enables the desktop or the server administrator to perform all the necessary day-to-day tasks like creating datastores as seen in Figure 6 and Figure 7.
When the volumes are created, capacity and QoS settings must be provided. For this testing, we set a very high maximum QoS so that the performance of the desktops was not limited. The purpose, as mentioned in section 5.1, Testing Objectives, was to determine the desktop density and performance for the compute, because the storage was able to serve more desktops than the provided compute.

**Linked Clone Desktop Volume Sizing**

In our testing, the 480 virtual desktops were evenly spread across 10 HCI storage volumes, with 48 desktops per volume. We provided each volume with a round 2TB of storage for this exercise.
To help calculate the space that is required for production desktop deployments, VMware uses the following formula for creating linked clones at 50% utilization:

\[
\text{Volume Size} = \text{number of VMs} \times (0.5 \times \text{replica disk size} + \text{size of .vswp file per virtual desktop}) + 2 \times \text{replica disk size}
\]

By using the values from our test deployment, we get the following result:

\[
\text{Volume Size} = 48 \text{ VMs} \times (16\text{GB} + 4\text{GB}) + 64\text{GB} = 1024\text{ GB}
\]

Additionally, to maintain a maximum fullness threshold of 80%, we added 20% more capacity to each datastore for overhead, which increased the total usable size for each desktop datastore:

\[
\text{Volume Size (20% overhead)} = 1024\text{ GB} \times 1.2 = \text{TB}
\]

These values do not take into consideration the fact that compression and deduplication are also used on the storage controller.

### 3.5 Virtual Machine Configuration

We used the VMs that are listed in Table 5 to support the VDI deployment in our test example. A 2TB volume was created and attached to support these management VMs. A Windows 2016 server was cloned, and the software was loaded for the different server components to support this testing. There was very little customization of the software beyond the basic configuration. The areas that we modified are described in the following sections. For specific installation and configuration information, consult [VMware Horizon 7 Installation](#) and the [Login VSI Installation Guide](#).

**Note:** For a production environment, NetApp recommends that you implement load balancing and Horizon View security servers and that you confirm that the infrastructure servers make use of high availability.

**Table 5) Infrastructure VMs.**

<table>
<thead>
<tr>
<th>Server</th>
<th>Software Version</th>
<th>Guest OS Version</th>
<th>CPU</th>
<th>Memory</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>vCenter 6.0</td>
<td>vCenter Appliance</td>
<td>4 vCPUs</td>
<td>16GB</td>
<td>185GB</td>
</tr>
<tr>
<td>Horizon View Connection</td>
<td>7.2</td>
<td>Windows 2016</td>
<td>2 vCPUs</td>
<td>4GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Horizon View Composer</td>
<td>7.2</td>
<td>Windows 2016</td>
<td>2 vCPUs</td>
<td>4GB</td>
<td>40GB</td>
</tr>
<tr>
<td>SQL Server (event,</td>
<td>SQL Server 2012</td>
<td>Windows 2016</td>
<td>2 vCPUs</td>
<td>4GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Composer database)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory, DNS,</td>
<td>Windows 2016</td>
<td>Windows 2016</td>
<td>2 vCPUs</td>
<td>8GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Dynamic Host Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol (DHCP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login VSI management</td>
<td>4.1.25</td>
<td>Windows 2016</td>
<td>2 vCPUs</td>
<td>8GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Login VSI launcher</td>
<td>4.1.25</td>
<td>Windows 2016</td>
<td>4 vCPUs</td>
<td>8GB</td>
<td>40GB</td>
</tr>
<tr>
<td>Desktop template (target)</td>
<td></td>
<td>Windows 10,</td>
<td>2 vCPUs</td>
<td>4GB</td>
<td>32GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>version 1703</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The desktop template disk size that we used in the initial testing was 32GB. For the follow-up testing in section 6.3, we created a new template with a 64GB disk. We found that 32GB was not enough to patch the VM with all the software and updates since version 1703 of Windows 10 had
originally been released. A 64GB image provided us with enough space to successfully update the desktop template.

VMware View Advanced Settings

The following optimizations have been made to increase the number of parallel tasks that are initiated by Horizon View. You can find these settings in the Horizon View Administrator web interface under View Configuration > Servers > vCenter Servers > vCenter Server Settings.

The tests in this document use the advanced settings that are shown in Figure 8.

Figure 8) Edit vCenter Server advanced settings.

3.6 Windows Desktop Template

For this testing, we created a Windows 10 template and patched it with the most current patches from Microsoft. Then we installed Office 2016 and the target installation package, which installs Adobe Reader, Adobe Flash Player, Java, and Doro PDF. After the installation, we modified the registry for the View Composer Agent and optimized the desktop by using the VMware OS Optimization Tool.

Fix the Default PDF Application Association

The default PDF application must be modified to use Login VSI with Windows 10. Windows 10 uses the Microsoft Edge browser by default to open PDF documents. To change this default, you must edit the OEMDefaultAssociations.xml file in the Windows System32 directory. A Login VSI blog post describes how to accomplish this task.

If you are using Adobe Acrobat Reader DC, you can use the following instructions to fix the default PDF application association:

1. After you have installed Adobe Acrobat Reader DC, open a PDF file by right-clicking the file and selecting Open With > Choose Another Program.
2. Select Adobe Acrobat Reader DC and select Always Use This App to Open .pdf Files. Click OK.
3. Run the following commands in an administrator command prompt:

   dism.exe /Online /Export-DefaultAppAssociations:c:\AppAssoc.xml
   START /B notepad c:\AppAssoc.xml
   START /B notepad c:\windows\system32\OEMDefaultAssociations.xml

4. Copy the line in the c:\AppAssoc.xml file that contains the PDF. It should be similar to the following line:

   <Association Identifier=".pdf" ProgId="AcroExch.Document.DC" ApplicationName="Adobe Acrobat Reader DC" />

5. Paste the PDF line into the OEMDefaultAssociations.xml file, replacing the existing line that indicates Microsoft Edge for PDFs.

   <Association Identifier=".pdf" ProgId="AppXd4nrz8ff68srnhf9t5a8sbjyar1cr723" ApplicationName="Microsoft Edge" ApplyOnUpgrade="true" OverwriteIfProgIdIs="AppXk660crfho0g7gd9wcnsws708mn7qjr1" />

6. Create a Group Policy Object (GPO) or use the Login VSI Target-V416 GPO and modify Computer Configuration > Administrative Templates > Windows Components > File Explorer > Set a Default Associations Configuration File.

7. Enable the policy and use %systemroot%\system32\OEMDefaultAssociations.xml as the configuration file, as shown in the following screenshot.
Modify View Composer Agent

Because of the constant churn of creating and deleting the Windows desktops, we configured the Horizon Agent to skip the check if Windows is activated. Production environments should skip this step. To modify View Composer Agent on the template:

1. Start the Windows registry editor.
2. Navigate to the key in the following location:
   
   HKEY_LOCAL_MACHINE\System\ControlSet001\Services\vmware-viewcomposer-ga

3. Change the setting SkipLicenseActivation registry value to 1.

This VMware Knowledge Base article outlines the workarounds for the View Composer activation requirement.

Alternatively, you can create a .reg file by using the following text:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmware-viewcomposer-ga]
"SkipLicenseActivation"=dword:00000001
```

Optimize the Desktop OS

We applied desktop OS optimizations to the template VMs that we used in this testing. For this testing, we used the default optimizations. Although it might be possible to run desktops without guest optimizations, you must first understand the impact of not optimizing. Many recommended optimizations address services and features (such as hibernation, Windows updates, and system restores) that do not provide value in a virtual desktop environment. These services and features consume CPU, memory, and storage resources. Therefore, running services and features that do not add value decreases the overall density of the solution and increases cost. A Login VSI blog post quantifies the benefits of optimizing the desktop.

Before you optimize the template, NetApp recommends that you update the Windows Operating System Optimization Tool (OSOT) with the latest Windows 10 optimizations, as shown in Figure 9.
Figure 9) Updating the VMware OSOT template.

Figure 10) VMware OSOT before optimizations.

Figure 10 shows the VMware OSOT that we used to perform the guest optimizations. Figure 11 shows the OSOT after optimizations.

Figure 11) VMware OSOT after optimizations.
You can find more information about the VMware OSOT on the VMware website.

### 4 About Login VSI

The company, Login VSI, provides end-user performance insights for virtualized desktop and server-based computing environments. Enterprise IT departments use its flagship product Login VSI (for scalability testing), and new addition Login PI (for availability testing) in all phases of their virtual desktop deployment—from planning and deployment to change management—to help build and safeguard high performance, high availability, and (as a result) the optimal end-user experience. With minimal configuration, Login VSI’s products work with VMware Horizon View, Citrix XenApp and XenDesktop, Microsoft Remote Desktop Services (Terminal Services), and any other Windows-based virtual desktop solution. For more information, or a free trial, please visit www.loginvsi.com.

Login VSI accepts no responsibility regarding this publication in any way and cannot be held accountable for any damages following from, or related to, any information contained within this publication, or any conclusions that may be drawn from it.

#### 4.1 Objective testing with Login VSI

Login Virtual Session Indexer (Login VSI) is the industry standard load-testing tool for measuring 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 the major hardware and software vendors and is recommended by both leading IT analysts and the technical community. Login VSI is 100% vendor independent and works with standardized user workloads—making all conclusions based on Login VSI test data objective, verifiable, and repeatable.

Login VSI-based test results are used and published in multiple technical white papers and presented at various IT-related conferences by our vendor customers. The product Login VSI is also widely used by end-user organizations, system integrators, hosting providers, and testing companies. It is also the
standard testing tool used in all tests executed in the internationally acclaimed research project VDI Like a Pro (formerly known as Project Virtual Reality Check).

4.2 How Login VSI works

When used for benchmarking, the product measures the total response times of several specific user operations being performed within a desktop workload, in a scripted loop. The baseline is the measurement of the specific operational response times performed in the desktop workload, measured in milliseconds (ms). Two values, in particular, are very important: VSIbase and VSImax.

- **VSIbase**: A score reflecting the response time of specific operations performed in the desktop workload when there is little or no stress on the system. A low baseline indicates a better user experience—resulting in applications responding faster within the environment.
- **VSImax**: The maximum number of desktop sessions attainable on the host before experiencing degradation in both host and desktop performance.

Both values, VSIbase and VSImax, offer undeniable proof (vendor independent, industry standard and easy to understand) to innovative technology vendors of the power, the scalability, and the benefits of their software and hardware solutions, in a virtual desktop environment.

5 VMware Horizon View Desktop Testing with Login VSI

5.1 Testing Objectives

The objectives of our tests were to determine and to demonstrate the desktop density and performance of small NetApp HCI compute nodes. We performed tests on a single server to see how many users of a given Login VSI profile could fit on a single compute node. Then we added six more compute nodes and multiplied the user count by 6 to demonstrate near linear scalability. We added one more node for high availability and did not modify the user count, and we measured the decrease in the Login VSI Average.

Because this architecture was limited on compute, we did not measure storage density and performance. You can find more information about expected storage density in section 5.4, Storage Sizing, of this document.

5.2 Tests and Results

Workload Profile

For these tests, we used Login VSI to simulate a typical desktop user. We selected the knowledge worker, which is a standard workload that many reference architectures use for comparison. The knowledge worker profile uses the following applications: Microsoft Word, Microsoft Outlook, Internet Explorer, Adobe Reader, Microsoft PowerPoint, Microsoft Excel, FreeMind/Java, and Windows Photo Viewer.

Login VSI uses synthetic users who log in to their desktops, perform work, take virtual coffee breaks, talk to their virtual colleagues, and resume work like a typical real user would do. We set up the test by entering benchmark mode to set all the Login VSI parameters to a known good state. We then exited benchmark mode and modified the workload.

We were required to modify the Login VSI knowledge worker workload profile and removed maximize from the workload, as outlined in a Login VSI Knowledge Base article.

You can find more information about Login VSI and the workloads and behaviors in a Login VSI blog post.
Login VSI Metrics

Login VSI Baseline
The Login VSI Baseline is the average of the 13 lowest VSI index calculation response time samples in the entire test.

Login VSI Average
The Login VSI Average is the average response time for a portion of the active users who are logged in to the system.

Login VSI Threshold
The Login VSI Threshold is calculated by adding 1000ms to the VSI baseline.

VSImax v4
The VSImax v4 is the point at which the number of running sessions exceeds the VSI Threshold. For example, if the VSI Baseline is 1000ms, the VSI Threshold is 2000ms. If session 481 crosses the 2000ms threshold, the VSImax is 480. This value is the number of sessions that the infrastructure supports for this workload.

You can find more information about all the Login VSI metrics in a Login VSI blog post and in a Login VSI VSImax webpage.

Single-node Scalability
The purpose of this testing was to determine and to demonstrate the desktop density and performance of a single small NetApp HCI compute node. It is the first step in determining how many desktops a given node type can host. Based on the Login VSI data, the baseline for the end-to-end response time was under 1 second. This response time is very good. By using the knowledge worker profile, 82 desktops were able to run on this single server without exceeding the VSI threshold. Table 6 shows these results in tabular form, and Figure 12 shows VSImax v4 in graphical form.

Table 6) H300E single–compute node test Login VSI metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login VSI Baseline</td>
<td>947ms</td>
</tr>
<tr>
<td>Login VSI Average</td>
<td>1652ms</td>
</tr>
<tr>
<td>Login VSI Threshold</td>
<td>1947ms</td>
</tr>
<tr>
<td>VSImax</td>
<td>82 desktops</td>
</tr>
</tbody>
</table>
Six-Node Scalability

We performed the six-node scalability test to demonstrate linear scalability of the single-node testing. For this test, we added five servers to the desktop cluster (six total) and, for availability and load balancing, we enabled high availability and Distributed Resource Scheduler (DRS) on the cluster.

The six-node scalability VSImax came in at 480 VMs (Table 7). This value is lower than expected because the linear scaling of the single-node test should have been 492 (6*82). The Login VSI average is also slightly higher, suggesting that something might be affecting the overall result. The results are shown in Figure 13.

During the six-server test, DRS was used, and it did migrate VMs around to better balance the load across the ESXi hosts, thus consuming resources that were not part of the first test. In addition, some VMs above the 480 number were powered on and idle, which consumed a slight amount of compute and memory. We performed this test to show the scalability at 100% resource utilization. This test did not take into consideration the CPU and the memory that are required for host failure.

Table 7) H300E six–compute node test Login VSI metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login VSI baseline</td>
<td>921ms</td>
</tr>
<tr>
<td>Login VSI average</td>
<td>1893ms</td>
</tr>
<tr>
<td>Login VSI threshold</td>
<td>1921ms</td>
</tr>
<tr>
<td>VSImax</td>
<td>480 desktops</td>
</tr>
</tbody>
</table>
Seven-Node Scalability

The seven-node scalability test repeated the purpose and the method of the six-node test with an additional node for high availability. The baseline and average were lower in this test (Table 8) because the configuration included additional CPU and memory. Even this configuration, at 480 VMs, is pushing the limits of acceptable utilization. Reducing the VM count slightly from 480 would provide a lower VSI average when in a failure condition. The results are shown in Figure 14.

Table 8) H300E seven–compute node test Login VSI metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login VSI baseline</td>
<td>938ms</td>
</tr>
<tr>
<td>Login VSI average</td>
<td>1408ms</td>
</tr>
<tr>
<td>Login VSI threshold</td>
<td>1937ms</td>
</tr>
<tr>
<td>VSImax</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Collective Metrics

Looking across all the different tests and their respective results, the VSI baseline is quite steady and has less than 1ms end-to-end latency, indicating that the HCI system configuration and networking are optimally configured. Looking at the VSI average, the six-node test pushed the compute infrastructure to the edge, and we can conclude that additional CPU and memory are recommended. The seven-node test demonstrated that adding one node for availability can dramatically reduce the average latency. See Figure 15.

Figure 15) Login VSI metrics across the three tests.

<table>
<thead>
<tr>
<th></th>
<th>Single-Node Test</th>
<th>Six-Node Test</th>
<th>Seven-Node Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login VSI baseline</td>
<td>947</td>
<td>921</td>
<td>938</td>
</tr>
<tr>
<td>Login VSI average</td>
<td>1652</td>
<td>1893</td>
<td>1408</td>
</tr>
<tr>
<td>Login VSI threshold</td>
<td>1947</td>
<td>1921</td>
<td>1937</td>
</tr>
</tbody>
</table>

5.3 VMware Horizon View Common Maintenance Operations

Three common maintenance activities can be performed on the linked clones: refresh, recompose, and rebalance. Each of these maintenance activities has an effect on both the capacity of the storage controller and the performance of the guest VM.
Refresh

In a VM refresh operation, the VM’s OS disk (the delta disk) is reverted back to the state that it was in when it was first provisioned. A refresh operation restores the VM’s storage efficiency, security, and compliance by purging any sensitive or transient data that has been written to the C:\ drive.

Recompose

In a VM recompose operation, the VM’s replica disk is replaced, and the original VM delta disk is deleted and is relinked to the new or the updated replica. This operation is used when the template machine is patched or when software updates are applied, and it can also be used to distribute a new operating system.

Rebalance

In a VM rebalance operation, the VMware View desktops are redistributed evenly across datastores. Because of the HCI architecture and shared-nothing, scale-out nature of the storage platform, this test was not performed. Both performance and capacity can be added to or removed dynamically from the storage.

Table 9 shows the results from our testing of maintenance operations.

Table 9) VMware Horizon maintenance operations.

<table>
<thead>
<tr>
<th>Task</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot 480 virtual desktops and available</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Create 480 virtual desktops</td>
<td>52 minutes</td>
</tr>
<tr>
<td>Refresh all desktops</td>
<td>18 minutes</td>
</tr>
<tr>
<td>Recompose all desktops</td>
<td>62 minutes</td>
</tr>
</tbody>
</table>

5.4 Storage Sizing

Given the configuration that is listed in section 3.1, the architecture was limited on compute nodes. Because of the compute limitations, the storage was not stressed adequately to report storage performance maximums. However, because the NetApp HCI small storage node has the same hardware configuration as the NetApp SF4805 and SF9605 platforms, we can calculate the approximate VM density based on our VDI sizers.

For our example, we did determine sizing based on previous testing and on the similarity of the NetApp HCI nodes to the SF4805 and SF9605 platforms. We determined that four small NetApp HCI storage nodes should be able to support more than 2,000 users with a standard VDI workload of 15 IOPS per user, 20% read and 80% write, and a 16K average block size. Capacity requirements dictate whether additional nodes of different sizes are required.

Note: These read/write ratios and block sizes are based on what can be typically seen from a Login VSI test from the ESXi layer during vscttStats collection.

6 Additional Performance Analysis

6.1 Large NetApp HCI H700E Compute Node Performance Validation

As a part of the additional work that we performed after the original publication of this report, we validated the sizing of a large NetApp HCI H700E compute node. We performed the same single-node validation with Login VSI as we had conducted originally. We determined that a single NetApp HCI H700E compute
node could support 154 linked-clone nonpersistent desktops with the Login VSI knowledge worker workload. Figure 16 shows the test results.

Figure 16) H700E single-compute node test VSImax v4 graph.

![Figure 16](image)

Because you need at least two compute nodes for high availability, NetApp does not recommend this configuration, however. NetApp also does not recommend that you size your configuration based on running the workload at 100% utilization. Table 10 shows the desktops per node at 100% and at 80% for the NetApp HCI H300E and H700E compute nodes, respectively.

Table 10) Linked-clone density based on the Login VSI knowledge worker load.

<table>
<thead>
<tr>
<th>Model</th>
<th>Desktops/Node at 100%</th>
<th>Desktops/Node at 80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp HCI H300E</td>
<td>80</td>
<td>64</td>
</tr>
<tr>
<td>NetApp HCI H700E</td>
<td>154</td>
<td>123</td>
</tr>
</tbody>
</table>

6.2 Instant Clone Scalability

In this performance assessment, we evaluated the use of VMware Instant Clones to measure the user density effects of Instant Clones. To assess these effects, we created an Instant Clone pool of desktops by using an unpatched Windows 10 desktop. We also modified the VMware Horizon Agent to not use the View Composer components and to use the Instant Clone components of the agent. We used the same workload that had been used in all the other Login VSI testing and obtained the results that are shown in Figure 17, Figure 18 and Table 11.
Figure 17) H300E Instant Clone density results.

![H300E Instant Clone density results](image)

Figure 18) H700E Instant Clone density results.

![H700E Instant Clone density results](image)

Table 11) Instant Clone density based on the Login VSI knowledge worker load.

<table>
<thead>
<tr>
<th>Model</th>
<th>Login VSImax</th>
<th>Login VSI Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp HCI H300E</td>
<td>67</td>
<td>973ms</td>
</tr>
<tr>
<td>NetApp HCI H700E</td>
<td>133</td>
<td>843ms</td>
</tr>
</tbody>
</table>

6.3 Spectre and Meltdown Performance Analysis

Since this document’s original publication, two significant security-related CPU vulnerabilities have been discovered that might affect NetApp HCI solution density and application performance. These
vulnerabilities are known as Spectre (CVE-2017-5753/CVE-2017-5715) and Meltdown (CVE-2017-5754). NetApp has created a security advisory Processor Speculated Execution Vulnerability in NetApp Products that addresses these vulnerabilities. Patching these vulnerabilities has been known to affect the performance of servers and virtual desktop machines. The impact can vary dramatically, based on the applications and their usage of system calls. The heavier the use of system calls, the greater the impact on performance is.

Because of the potential effect on performance, we conducted a series of tests to determine the impact of patching NetApp HCI to address the Spectre and Meltdown vulnerabilities. In those tests, we used Login VSI as we had previously to measure the solution density before and after the patches were applied.

**Note:** Patching to remediate these vulnerabilities includes not only patching the guest operating system, but also patching the hypervisor and updating the processor microcode. NetApp HCI compute nodes are deployed using VMware vSphere 6.0 U3 or 6.5 U1. Customers are responsible for patching and maintaining their VMware software levels. Refer to [KB 52245](#) for version specific remediation details.

### Configuration

In this section, we describe the configuration that we used to determine the impact of the hypervisor and operating system patches. Since the original release of this document, many components of the solution have been updated. Table 12 summarizes the difference in the infrastructure between the previous tests and the Spectre and Meltdown tests.

Table 12) Differences between Spectre and Meltdown testing and previous testing.

<table>
<thead>
<tr>
<th>Item</th>
<th>Previous Test (October 2017)</th>
<th>Spectre and Meltdown Test (July 2018)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere version</td>
<td>vSphere 6.0 (NDE 1.0)</td>
<td>vSphere 6.5 (NDE 1.2)</td>
</tr>
<tr>
<td>Element OS</td>
<td>Element OS 10.0</td>
<td>Element OS 10.2</td>
</tr>
<tr>
<td>VMware Horizon</td>
<td>7.2</td>
<td>7.4</td>
</tr>
<tr>
<td>Login VSI</td>
<td>4.1.25</td>
<td>4.1.31</td>
</tr>
<tr>
<td>Adobe Acrobat</td>
<td>Adobe Acrobat Reader X</td>
<td>Adobe Acrobat Reader DC</td>
</tr>
</tbody>
</table>

In these tests, we used the software versions and their patched versions that are shown in Table 12.

Table 13) Prepatch and postpatch software versions.

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi (prepatch)</td>
<td>ESXi 6.5 Update 1 July 27, 2017</td>
</tr>
<tr>
<td></td>
<td>ISO Build 5969303</td>
</tr>
<tr>
<td>ESXi (postpatch)</td>
<td>ESXi 6.5 Update 1 March 20, 2018</td>
</tr>
<tr>
<td></td>
<td>ISO Build 7967591</td>
</tr>
<tr>
<td>Windows 10 Enterprise (prepatch)</td>
<td>1703, OS Build 16299.125</td>
</tr>
<tr>
<td>Windows 10 Enterprise (postpatch)</td>
<td>1709, OS Build 16299.402</td>
</tr>
</tbody>
</table>
Determining Patch Status

To determine whether the patch was applied to the guest operating system, we used a Windows PowerShell Module, Speculation Control (https://gallery.technet.microsoft.com/scriptcenter/Speculation-Control-e36f0050).

To install and to import this module, open PowerShell as an administrator and run the following commands:

```
Install-Module SpeculationControl
Import-Module SpeculationControl
Get-SpeculationControlSettings
```

The following article can help you decipher the output of Get-SpeculationControlSettings:


Figure 19 shows example Get-SpeculationControlSettings output for an unpatched VM.

**Figure 19) Example of unpatched Windows 10 operating system Speculation Control output.**

```
PS C:\Users> Get-SpeculationControlSettings
Hardware support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is enabled: False
Speculation control settings for CVE-2017-5713 [branch target injection]

Hardware required for kernel VA shadowing: True
Windows OS support for kernel VA shadow is present: False
Windows OS support for kernel VA shadow is enabled: False

SUPPORTED ACTIONS
- Install BIOS/firmware update provided by your device OEM that enables hardware support for the branch target injection mitigation.
- Install the latest available updates for Windows with support for speculation control mitigations.
- Follow the guidance for Windows Client support for speculation control mitigations described in https://support.microsoft.com/help/4073119

BITHardwarePresent : False
BITWindowsSupportPresent : False
BITWindowsSupportEnabled : False
BITDisableHyperSystemPolicy : False
BITRestoreHyperSystemSupport : False
PCVAwakeWspEnabled : False
PCVAwakeWindowsSupportEnabled : False
PCVAwakeFullySupported : False
```

Figure 20 shows example Get-SpeculationControlSettings output for a patched VM.

**Figure 20) Example of patched Windows 10 operating system Speculation Control output.**

```
PS C:\Users> Get-SpeculationControlSettings
Hardware support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is enabled: True
Speculation control settings for CVE-2017-5713 [branch target injection]

Hardware required for kernel VA shadowing: True
Windows OS support for kernel VA shadow is present: True
Windows OS support for kernel VA shadow is enabled: True
Windows OS support for BIOS performance optimization is enabled: True [not required for security]

BITHardwarePresent : True
BITWindowsSupportPresent : True
BITWindowsSupportEnabled : True
BITDisableHyperSystemPolicy : False
BITRestoreHyperSystemSupport : True
PCVAwakeWspEnabled : True
PCVAwakeWindowsSupportEnabled : True
PCVAwakeFullySupported : True
```

Testing Methodology

Figure 21 shows the methodology that we used to test prepatch and postpatch performance.
Step 1: Replicate Previous Results

The first step of this validation was to replicate the results of the previous testing. This step was important to confirm that we were working from a known good baseline. We needed to confirm that the differences in the HCI platform (for example, NetApp Deployment Engine, vSphere, and Horizon; see Table 12) software versions didn’t affect the overall results. We also wanted to confirm that what we were measuring was the impact of patching of the hypervisor and of the guest operating system.

Step 2: Patch and Validate Patch Installation

The second step was to patch both the hypervisor and the guest operating system. We used VMware Update Manager to bring the ESXi hosts up to date. These patches included the patches for Spectre and for Meltdown that are listed in KB 52245.

We then patched the master template guest operating system by using Microsoft Windows Update. For this task, we powered on the template VM and rolled back the changes that had been made by the VMware OSOT. We had to take this action because the OSOT includes many “optimizations” that affect the use of Windows Update. We ran through the Check for Updates and allowed it to install updates and to reboot multiple times.

We then ran the `Get-SpeculationControlSettings` PowerShell script to verify that the patches had been applied to mitigate the Spectre and Meltdown vulnerabilities. We then reapplied all the OSOT settings, powered off the VM, and created a VMware snapshot. We disabled the pool, removed all the VMs in the pool, changed the template and the snapshot of the pool, and reenabled the pool. From that point, the desktops were reprovisioned with the Spectre and Meltdown patches and were available in Horizon.

Step 3: Test Patched VMs

The third step was to run Login VSI exactly as we did in step 1 to determine the VSImax difference.

Prepatch and Postpatch Results

Figure 22 through Figure 25 are the Login VSI max graphs for the unpatched and patched tests. Two things are of note in these graphs. One is that the VSI max and VSI base scores were both affected by patching the VMs. Another is that the VSI average and the VSI threshold were also affected, but those effects are due to the changes in the VSI base.
Figure 22) H300E Login VSI results before patching for Spectre and Meltdown.

Figure 23) H300E Login VSI results after patching for Spectre and Meltdown.
In conclusion, the testing that we performed was consistent with other reports in the industry. As explained in section 5.2, the Login VSI Baseline score is the average of the 13 lowest VSI index calculation response time samples in the entire test. Our test results showed an increase in the baseline score after we patched the desktops. The increase in response time implies that there was additional overhead for a patched VM. By looking at the ESXi host resource utilization for both the unpatched and the patched testing, we know that the CPU was the bottleneck in both scenarios. Due to these increased CPU costs, we saw a 6% to 10% reduction in solution density as shown by the Login VSlmax score. Table 14 summarizes the comparison.
Table 14) Spectre and Meltdown prepatch and postpatch test result summary.

<table>
<thead>
<tr>
<th>Model</th>
<th>Login VSI Max</th>
<th>Login VSI Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp HCI H300E Prepatch</td>
<td>80</td>
<td>932ms</td>
</tr>
<tr>
<td>NetApp HCI H300E Postpatch</td>
<td>75</td>
<td>1115ms</td>
</tr>
<tr>
<td>NetApp HCI H700E Prepatch</td>
<td>154</td>
<td>818ms</td>
</tr>
<tr>
<td>NetApp HCI H700E Postpatch</td>
<td>139</td>
<td>861ms</td>
</tr>
</tbody>
</table>

**Acknowledgments**

The authors would like to thank William Arney, Chris Merz, Bobby Oommen, and Aaron Patten for their contributions to this technical report.

**Where to Find Additional Information**

To learn more about the information that is described in this document, see the following document and websites:

- NetApp HCI Datasheet
  [https://kb.vmware.com/s/article/52337](https://kb.vmware.com/s/article/52337)
  [https://kb.vmware.com/s/article/52245](https://kb.vmware.com/s/article/52245)
- The impact of Meltdown and Spectre patches on Windows 10
- Don’t let your user-experience be a “Spectre” of itself after “Meltdown”

**Version History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>October 2017</td>
<td>Initial release.</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>July 2018</td>
<td>Added subsequent testing to the technical report, including NetApp HCI H700E results, Instant Clone results, and Spectre and Meltdown testing.</td>
</tr>
</tbody>
</table>
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 © 1994–2018 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, tapering, 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.