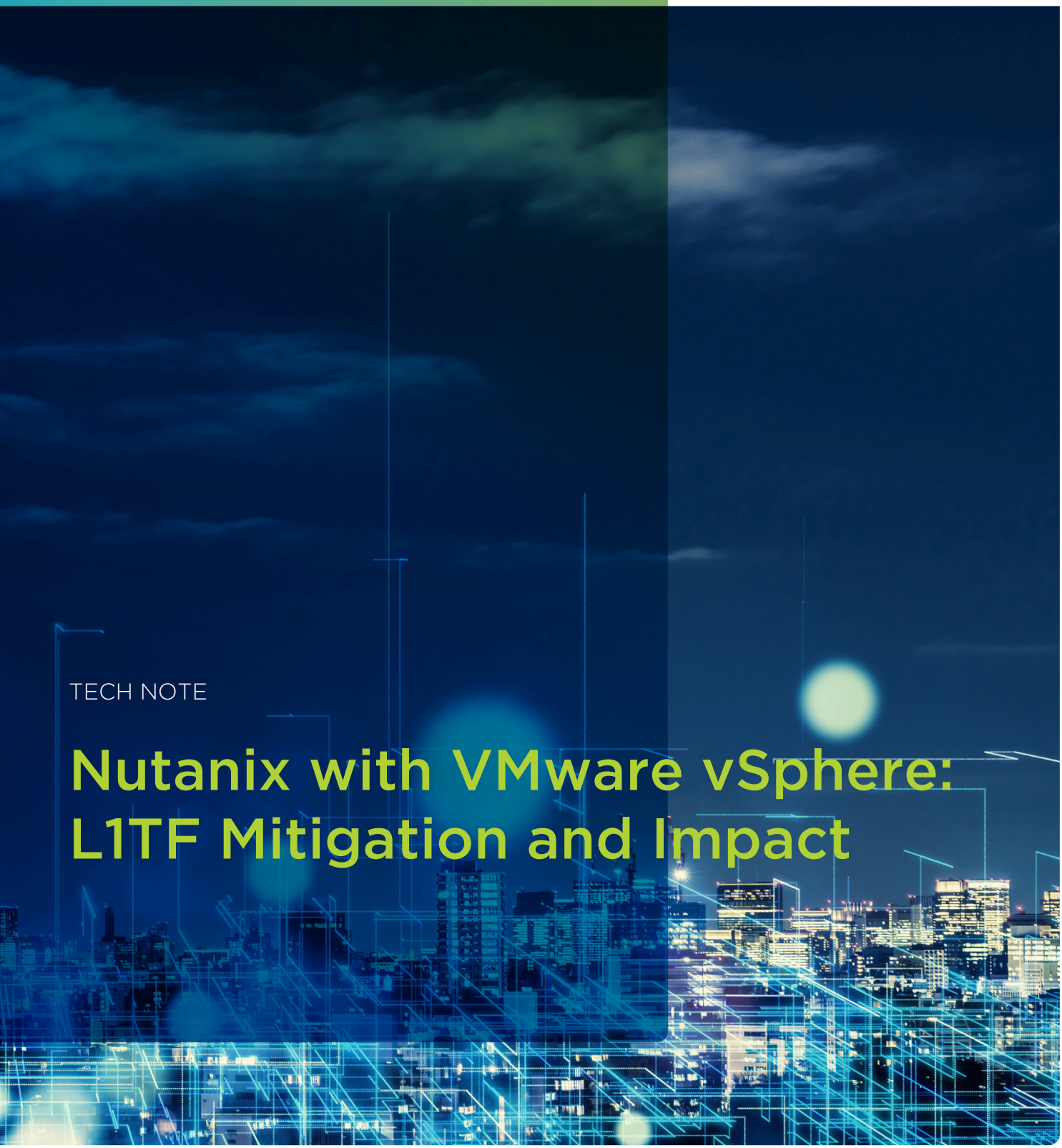
v1.1 | March 2022 | TN-2143



TECH NOTE

Nutanix with VMware vSphere: L1TF Mitigation and Impact

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary....4

2. Introduction....5
- Audience....5
- Purpose....5
- Document Version History....5

3. L1TF Vulnerability Mitigations for vSphere....6
- SCA V2 L1TF Vulnerability Mitigation for vSphere....6
- Performance Testing....7

4. Conclusion....11

5. Resources....12

Appendix....13
- About Nutanix....13

1. Executive Summary

Nutanix is a highly resilient converged compute and storage platform designed to support virtual environments like VMware vSphere. The Nutanix architecture runs a storage controller in the Nutanix Controller VM (CVM). The CVM runs on every Nutanix server node in a Nutanix cluster to form a highly distributed, shared-nothing infrastructure.

All CVMs actively work together to aggregate storage resources into a single global pool that user VMs running on the Nutanix server nodes can consume. The Nutanix distributed storage fabric manages storage resources to preserve data and system integrity in the event of node, disk, application, or hypervisor software failure. The distributed storage fabric also delivers data protection and high availability that keep critical data and VMs protected.

Because of its hyperconverged architecture, the Nutanix platform can have any number of storage controllers—a huge advantage compared to traditional shared storage platforms that must have either two or four. As a result, it's much less complex to design, build, and scale a solution to service all datacenter requirements with Nutanix.

2. Introduction

Audience

This document is part of the Nutanix Solutions Library. We wrote it to show the performance impact of L1TF mitigations on a Nutanix cluster running VMware vSphere as validated by the Nutanix Performance Engineering team. As per the VMware EULA, we don't publish actual performance numbers in this document.

Purpose

This report covers the following subject areas:

- Steps for mitigating L1TF.
- L1TF mitigation performance testing.
- Recommendations for optimal performance with L1TF mitigations.

Document Version History

Version Number	Published	Notes
1.0	August 2020	Original publication.
1.1	February 2022	Refreshed content.

3. L1TF Vulnerability Mitigations for vSphere

CVE-2018-3646 details an Intel microprocessor vulnerability that impacts hypervisors, L1 Terminal Fault (L1TF). The L1TF vulnerability may allow a malicious VM running on a given CPU core to copy the hypervisor content or the privileged information of another VM in the same core's L1 data cache. CVE-2018-3646 currently has two known attack vectors: Sequential-Context and Concurrent-Context.

You can find the Nutanix response to the L1TF vulnerability in Nutanix Security Advisory #10 on the Nutanix Security Advisories list. The ESXi Side Channel Aware Scheduler (ESXi | L1TF vulnerability mitigation) KB from Nutanix might also be useful. You can read VMware's official recommendation for vSphere in VMware KB 55636 and their official performance impact analysis for example workloads in their Performance of vSphere 6.7 document.

To enable L1TF mitigation (SCA V1 and V2) from the command line interface on all the hosts running vSphere, complete the following steps:

- Use SSH to sign on to any CVM in the Nutanix cluster.
- Run the following commands:

```
$ hostssh esxcli system settings kernel set -s hyperthreadingMitigation -v TRUE
$ hostssh esxcli system settings kernel set -s hyperthreadingMitigationIntraVM -v
 TRUE
```

- Once you've applied the mitigation settings, run the following commands to verify the changes:

```
$ hostssh esxcli system settings kernel list -o hyperthreadingMitigation
$ hostssh esxcli system settings kernel list -o hyperthreadingMitigationIntraVM
```

SCA V2 L1TF Vulnerability Mitigation for vSphere

Internal testing suggests that enabling the SCA V2 L1TF mitigation has an impact similar to enabling the SCA V1 mitigation for similar workloads. If

you want to enable the SCA V2 mitigation, be aware that it impacts CPU performance for all VMs up to 30 percent and consider scaling out the compute requirements to meet performance objectives.

If you can't add any compute capacity, mission-critical workloads and other large workloads might experience performance degradation, because enabling the SCA V2 mitigation has a direct impact on the I/O operations that the CVM and other VMs can process.

Performance Testing

We conducted the following tests to validate the performance impact of enabling the SCA V2 L1TF mitigation:

- HammerDB testing (to simulate SQL and database workloads).
- MS Exchange Jetstress testing (to simulate 50,000 users on Nutanix running on VMware vSphere).

The cluster specifications used for both the tests are as follows:

- 4 Dell R740-XD 24-drive nodes
  - 2 Intel Xeon Gold 6148 2.40 GHz 20-core processors
  - 768 GB of RAM
  - 4 x 2.9 TB NVMe drives
  - 20 x 1.92 TB SSD drives
  - 2 x 25 GB Mellanox NICS connected to redundant Dell 5148F 25 GB switches

The system tested had the following software specifications:

- VMware vSphere 6.7 U3b
- Nutanix AOS 5.11.2.3
- 10 vCPU for the CVM
- 32 GB of RAM for the CVM

- Local storage for CVM on each node configured with Foundation
- Inline compression enabled

As per VMware documented performance testing, if a server uses all of its cores at or near full capacity, the loss of hyperthreads results in a noticeable decrease in performance—up to 30 percent, depending on the workload.

The testing done by Nutanix Performance Engineering showed results consistent with VMware's. The decrease in performance was between 15 percent and 25 percent, observed when the server was loaded and running at 75 percent or more CPU utilization.

Hammer DB Test: SQL Server on Windows

HammerDB is an open-source database benchmark used to validate and test various database workloads. It supports most databases in the market, including Oracle, SQL, and PostgreSQL. For this test, we followed the recommendations in the Nutanix SQL Server best practice guide for optimal VM performance. We used SQL Server 2016 running on Windows Server 2016 and the following VM configuration:

- 10 vCPU
- 192 GB of RAM
- 1 x 100 GB system drive
- 4 x 400 GB database drives
- 1 x 200 GB log drive
- 1 x 200 GB temp DB drive

We ran the test using the Transaction Processing Performance Council (TPC) TPC-C benchmark (for online transaction processing) from HammerDB. We ran two SQL VMs per node. To keep the results consistent, we used a similar user profile for all the tests, with 10 users and 100 warehouses per VM. These parameters gave us a total of 80 users and 800 warehouses for the TPC-C workload profile.

The VMware EULA does not permit publication of actual performance numbers, but the following table summarizes the performance changes for the HammerDB test.

Table: HammerDB SQL Server Performance Results

Test Criteria	Baseline CPU Performance	L1TF Mitigation	CPU Performance Change
TPC-C	1 x	SCA V2 mitigation applied	15% decrease in performance
TPC-C	1 x	SCA V1 mitigation applied	26% decrease in performance

MS Exchange Jetstress: Windows Server 2016

The MS Exchange Jetstress tool simulates the Exchange 2016 disk I/O load on a server to verify the performance and stability of the disk subsystem. Because the Nutanix CVM is a multipurpose VM that also acts as a storage controller, L1TF impacts the performance of the disk subsystem, which is directly related to the CPU performance.

The Jetstress configuration selected simulates 50,000 users with a 500 MB mailbox size running on eight Exchange Server VMs. Each Exchange Server VM (Jetstress VM) had the following specifications:

- 10 vCPU
- 192 GB of RAM
- 1 x 100 GB system drive
- 10 x 600 GB Exchange data drives
- 10 x 100 GB Exchange log drives

We ran the user workload simulation twice, for 24 hours each time, to ensure that the I/O performance was measured accurately, as CPU activity was not very high for the Jetstress VMs.

Table: MS Exchange I/O Performance Results

Test Criteria	Baseline I/O Performance	L1TF Mitigation	I/O Performance Change
Exchange Jetstress	1 x	SCA V2 mitigation applied	20% decrease in performance
Exchange Jetstress	1 x	SCA V1 mitigation applied	29% decrease in performance

Combined HammerDB and Jetstress Testing

To ensure consistency in both CPU and I/O performance profiles with the L1TF mitigations, we tested the HammerDB VMs and the Jetstress VMs together. We used Distributed Resource Scheduler (DRS) rules to keep the workloads on the same nodes and push the cluster to the maximum CPU utilization, with all physical cores allocated and 90 percent of the RAM allocated to the VMs. We only enabled the SCA V2 L1TF mitigation for simplicity.

The cluster consisted of the following:

- 8 Dell R740XD nodes running Nutanix AOS 5.11.2.3 and vSphere 6.7 U3b.
- 8 Windows Server 2016 VMs with SQL 2016 (10 cores and 192 GB of RAM).
- 16 Windows Server 2016 VMs with Jetstress 2016 (10 cores and 192 GB of RAM).

The following tables show the results.

Table: HammerDB CPU Performance Results

Test Criteria	TPC-C
CPU performance change	22% decrease in performance

Table: Exchange Jetstress I/O Performance Results

Test Criteria	Exchange Jetstress
I/O performance change	24% decrease in performance

4. Conclusion

Enabling SCA V2 mitigations can cause performance decreases up to 30 percent. To resolve this issue, we recommend that you scale your compute resources by adding approximately 30 percent more to meet the performance requirements.

5. Resources

- Nutanix third-party hardware compatibility lists
- VMware Compatibility Guide (including guest OS options supported on VMware ESXi)
- Nutanix Software Documents (including release notes)
- Nutanix End of Life Information
- VMware vSphere with Nutanix best practice guide
- VMware vSphere Networking with Nutanix best practice guide

Appendix

About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

