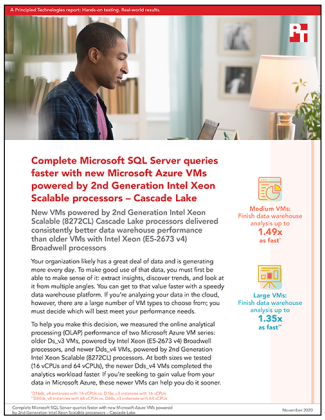

The science behind the report:

Complete Microsoft SQL Server queries faster with new Microsoft Azure VMs powered by 2nd Generation Intel Xeon Scalable processors – Cascade Lake

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Complete Microsoft SQL Server queries faster with new Microsoft Azure VMs powered by 2nd Generation Intel Xeon Scalable processors – Cascade Lake.

We concluded our hands-on testing on October 27, 2020. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on October 11, 2020 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

Table 1: Medium VM results. Source: Principled Technologies.

D16_Series v3 vs v4 (30GB database)			
Time to complete in seconds	v3	v4	v4 times as fast
1 stream	29	21	1.38
2 streams	46	34	1.35
3 streams	63	44	1.43
4 streams	82	55	1.49

Table 2: Large VM results. Source: Principled Technologies.

D64_Series v3 vs v4 (100GB database)			
Time to complete in seconds	v3	v4	v4 times as fast
1 stream	36	31	1.16
2 streams	55	44	1.25
3 streams	73	54	1.35
4 streams	89	66	1.35
5 streams	105	78	1.35

System configuration information

Table 3: Detailed information on the systems we tested.

VM configuration information	D16s_v3	D64s_v3	D16ds_v4	D64ds_v4
Tested by	Principled Technologies	Principled Technologies	Principled Technologies	Principled Technologies
Test date	10/13/2020	10/13/2020	10/13/2020	10/13/2020
CSP/Region	Microsoft Azure East US (Zone 1)	Microsoft Azure East US (Zone 1)	Microsoft Azure East US (Zone 1)	Microsoft Azure East US (Zone 1)
Workload & version	HammerDB v3.3 TPC-H-like	HammerDB v3.3 TPC-H-like	HammerDB v3.3 TPC-H-like	HammerDB v3.3 TPC-H-like
WL specific parameters	CCI, MAXDOP 16, Lock Pages in Memory, 90% Reserved SQL Memory	CCI, MAXDOP 64, Lock Pages in Memory, 90% Reserved SQL Memory	CCI, MAXDOP 16, Lock Pages in Memory, 90% Reserved SQL Memory	CCI, MAXDOP 64, Lock Pages in Memory, 90% Reserved SQL Memory
Iterations and result choice	3 runs, median	3 runs, median	3 runs, median	3 runs, median
Server platform	D16s_v3	D64s_v3	D16ds_v4	D64ds_v4
BIOS name and version	Microsoft Corporation Hyper-V UEFI Release v4.1, 4/2/2020	Microsoft Corporation Hyper-V UEFI Release v4.1, 4/2/2020	Microsoft Corporation Hyper-V UEFI Release v4.0, 3/12/2019	Microsoft Corporation Hyper-V UEFI Release v4.0, 3/12/2019
Operating system name and version/build number	Microsoft Windows Server 2019 Datacenter 10.0.17763 / Build 17763	Microsoft Windows Server 2019 Datacenter 10.0.17763 / Build 17763	Microsoft Windows Server 2019 Datacenter 10.0.17763 / Build 17763	Microsoft Windows Server 2019 Datacenter 10.0.17763 / Build 17763
Date of last OS updates/ patches applied	10/09/2020	10/09/2020	10/09/2020	10/09/2020
Processor				
Number of processors	1	2	1	2
Vendor and model	Intel® Xeon® CPU E5-2673 v4	Intel Xeon CPU E5-2673 v4	Intel Xeon Platinum 8272CL	Intel Xeon Platinum 8272CL
Core count (per processor)	20	20	24	24
Core frequency (GHz)	2.30	2.30	2.60	2.60
Stepping	1	1	7	7
Hyper-Threading	Yes	Yes	Yes	Yes
Turbo	Yes	Yes	Yes	Yes
Number of vCPU per VM	16	64	16	64
Memory module(s)				
Total memory in system (GB)	64	256	64	256
NVMe memory present?	No	No	No	No
Total memory (DDR+NVMe RAM)	64	256	64	256

VM configuration information	D16s_v3	D64s_v3	D16ds_v4	D64ds_v4
General hardware				
Storage: Network or Direct attached	Network	Network	Network	Network
Network bandwidth per VM	8,000 Mbps	30,000 Mbps	8,000 Mbps	30,000 Mbps
Storage bandwidth per VM	384 MB/s	1,200 MB/s	384 MB/s	1,200 MB/s
Local storage (OS)				
Number of drives	1	1	1	1
Drive size (GB)	127	127	127	127
Drive information (speed, interface, type)	Standard HDD	Standard HDD	Standard HDD	Standard HDD
Local storage (data drive)				
Number of drives	1	1	1	1
Drive size (GB)	64	128	64	128
Drive information (speed, interface, type)	Premium SSD (P6)	Premium SSD (P10)	Premium SSD (P6)	Premium SSD (P10)
Local storage (temporary drive)				
Number of drives	1	1	1	1
Drive size (GB)	128	512	600	2,400
Network adapter				
Vendor and model	Microsoft Hyper-V Network Adapter	Microsoft Hyper-V Network Adapter	Microsoft Hyper-V Network Adapter	Microsoft Hyper-V Network Adapter
Number and type of ports	1x 40Gb	1x 50Gb	1x 50Gb	1x 50Gb

How we tested

Creating the Windows Server 2019 baseline image

This section contains the steps we took to create our baseline image.

Using our methodology to aid your own deployments

While the methodology below describes in great detail how we accomplished our testing, it is not a deployment guide. However, because we include many basic installation steps for operating systems and testing tools, reading our testing methodology may help with your own installation.

Creating the baseline image VM

1. Log into the Azure Portal, and navigate to the Virtual Machines service.
2. To open the Add VM wizard, click Add
3. On the Basics tab, set the following:
    a. Choose your Subscription from the dropdown menu.
    b. Choose your Resource group from the dropdown menu.
    c. Name the Virtual Machine.
    d. Choose your Region from the dropdown menu.
    e. Leave the Availability options set to No infrastructure redundancy required.
    f. From the Image dropdown menu, choose Windows Server 2019 Datacenter.
    g. Leave Azure Spot instance set to No.
    h. Select the instance size you wish to use. We used Standard B4ms.
    i. Choose a new Username and Password for the Administrator account.
    j. Leave Public inbound ports set to Allow selected ports.
    k. For Select inbound ports, choose SSH (22).
4. On the Disks tab, set the following:
    a. For the OS disk type, choose Standard HDD.
    b. Leave the default Encryption type.
5. On the Networking tab, set the following:
    a. Choose your Virtual network from the dropdown menu.
    b. To create a new public IP, choose Create new.
    c. Leave the rest of the settings at their defaults.
6. On the Management tab, set the following:
    a. From the dropdown menu, choose your diagnostics storage account.
    b. Leave the rest set to defaults.
7. On the Advanced tab, leave all defaults.
8. On the Tags tab, add any tags you wish to use.
9. On the Review + create tab, review your settings, and click Create.

Configuring Windows Server 2019

1. Open Server Manager, and click Local Server.
2. Disable IE Enhanced Security Configuration.
3. Change the time zone to your local time zone.
4. Change the name of your server. When prompted, reboot.
5. Open Server Manager again, and click Local Server.
6. Click the link to run updates.
7. Run updates, rebooting when prompted, until the server shows no new updates to install.

Installing Microsoft SQL Server 2019 Enterprise

1. Download or copy the ISO to the server, and unzip it.
2. Double-click the Setup application.
3. Click InstallationàNew SQL Server Standalone installation or add features to an existing installation.
4. Choose the trial version, and click Next.
5. Check the I accept the license terms and Privacy Statement box, and click Next.
6. Check the Use Microsoft Update to check for updates (recommended) box, and click Next.
7. On the Install Rules page, click Next.
8. Check the boxes for the following features, and click Next:
    a. Database Engine Services
    b. Full-Test and Semantic Extractions for Search
    c. Client Tools Connectivity
    d. Client Tools Backwards Compatibility
9. Leave the Default instance, and click Next.
10. Leave the default Service Accounts, and click Next.
11. On the Server Configuration tab, choose Mixed Mode, and enter and confirm a Password for the SQL Server system administrator (sa) account.
12. To specify the SQL Server administrators, click Add Current User.
13. Click Next.
14. Once you've passed the rule check, click Next.
15. Click Install.
16. When the install is finished, go back to the SQL Server Installation Center, and click Install SQL Server Management Tools.
17. Download the SSMS file, and install with defaults.
18. Reboot the server when prompted.
19. Run Windows Update one more time to ensure there aren't any new updates for SQL (make sure Windows Updates are set to get updates for other Microsoft products).
20. Once you've installed all available updates, disable Windows Update service by performing the following actions:
    a. Click the Start button.
    b. To open the Services list, type `services`
    c. Disable the Windows Update service.

Locking pages in memory

1. Click Start, and type `Local Security Policy`
2. Open the program when it pops up in the search.
3. Expand Local Policies, and click on User Rights Assignment.
4. In the right-hand pane, scroll down, and double-click Lock pages in memory.
5. Click Add User or Group, type `NT Service\MSSQLSERVER`, and click OK.
6. To close the Properties window, click OK.
7. Close the Local Security Policy window.

Installing HammerDB 3.3

1. Download HammerDB from here: https://hammerdb.com/download.html.
2. Double-click the .exe file, choose English, and click OK.
3. Click Yes.
4. Click Next.
5. Chose a destination location, and click Next.
6. Click Next.
7. Click Finish.

Creating a snapshot of your baseline VM

1. In your Azure portal, navigate to the Snapshots service.
2. To open the Snapshot wizard, click Add
3. On the Basics tab, set the following:
    a. Choose your Subscription.
    b. Choose your Resource group.
    c. Enter a name for your snapshot.
    d. Choose your Region.
    e. Select Full - make a complete read-only copy of the selected disk for the Snapshot type.
    f. Choose the OS disk from your baseline VM.
    g. For the Storage type, choose Standard HDD.
4. On the Encryption tab, leave all defaults.
5. On the Tags tab, add any tags you wish to use.
6. On the Review + create tab, review your settings, and click Create.

Creating your image with the baseline snapshot

To create an image, you must first have a Shared Image Gallery. The steps below will walk you through the creation of the gallery as well as the image creation steps. Once you have created your gallery, you will not need to do so again to add new images.

1. In your Azure portal, navigate to the Shared image galleries service.
2. To open the Add gallery wizard, click Add.
3. On the Basics tab, set the following:
    a. Choose your Subscription.
    b. Choose your Resource.
    c. Name your gallery.
    d. Choose your Region.
    e. Enter a description if you'd like.
4. On the Tags tab, add any tags you wish to use.
5. On the Review + create tab, review your settings, and click Create.
6. Click your new image gallery, and click Add new image definition to open the wizard.
7. On the Basics tab, set the following:
    a. Set the Operating System to Windows.
    b. Set the VM generation to Gen 2.
    c. Set the Operation system state to Specialized.
    d. Enter whatever you wish for the Publisher, Offer, and SKU entries.
8. Skip the Version tab.
9. Skip the Publishing options tab.
10. On the Tags tab, add any tags you wish to use.
11. On the Review + create tab, review your settings, and click Create.
12. Click the image definition you've created, and click Add version to open the wizard.
13. On the Basics tab, set the following:
    a. Enter a version number such as 1.0.0.
    b. From the dropdown menu, choose the OS disk snapshot of the baseline VM you created.
    c. Leave the rest as defaults.
14. On the Encryption tab, leave defaults.
15. On the Tags tab, add any tags you wish to use.
16. On the Review + create tab, review your settings, and click Create.

Creating the VMs under test

In this section, we list the steps required to create a VM from the image we created previously.

Creating the VMs from the specialized image

1. Open the Azure Portal, and navigate to the Share image galleries service.
2. Click on the Shared image gallery you created.
3. Navigate to the image version you created (we used 1.0.0 above), and click Create VM.
4. On the Basics tab, set the following:
    a. Choose your Subscription.
    b. Choose your Resource group.
    c. Enter a Virtual machine name.
    d. Select Availability Zone, and set the Zone you desire.
    e. Select the instance size you want.
    f. Under Licensing, select Windows server.
    g. Leave the rest as defaults.
5. On the Disks tab, set the following:
    a. Change the OS disk type to Standard HDD.
    b. Click Create, and attach a new disk.
        i. In the Create a new disk wizard, click Change size, and pick the size of Premium SSD that matches your VM type. We chose P6 SSDs for the 16vCPU VMs, and P10 SSDs for the 64vCPU VMs
        ii. Leave the rest as defaults, and click OK.
6. Skip the Networking, Management, and Advanced tabs.
7. On the Tags tab, assign any tags you wish to use.
8. On the Review + create tab, review your settings, and click Create.
9. Once the VM creation is finished, click Go to resource (or navigate to the virtual machine service and click on the new VM).
10. Click ConnectàRDP, and download the RDP file.
11. Double-click the RDP file, and log in with the user and password you set.
12. Right-click the Windows Start button, and click Disk Management.
13. At the GPT partition popup window, click OK.
14. Right-click the Premium SSD you added, and follow the prompts to create a new NTFS volume for the database.

Configuring Microsoft SQL Server on the VMs under test

In this section, we list the various SQL settings that we changed and the steps to do so.

Setting the SQL Server memory reserve and max degree of parallelism (MAXDOP)

1. Open the SQL Server Management Studio.
2. Right-click on the SQL Instance, and click Properties.
3. Click Advanced node, scroll down to the Max Degree of Parallelism, and change the value to match the number of vCPUs on the system you are testing. Click OK.
4. Right-click the SQL Server VM again, and go to Memory.
5. Set the Max Memory to 90% of the total memory in the system. Click OK, and close the Properties window.
6. Right click the SQL Server VM, and restart the service. Click Yes when prompted.

Configuring the tempdb database

1. Open the SQL Server Management Studio.
2. Expand Databases and System databases, and right-click tempdb.
3. Add files, and change the starting size as necessary.
4. Right-click the SQL Server VM, and restart the service. When prompted, click Yes.
5. To move the tempdb to the database drive, open a new Query, and run the following command for the number of tempdb files your system has:

```
USE [master]
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = tempdev , FILENAME = 'E:\TempDB\tempdb.mdf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp2 , FILENAME = 'E:\TempDB\tempdb_mssql_2.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp3 , FILENAME = 'E:\TempDB\tempdb_mssql_3.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp4 , FILENAME = 'E:\TempDB\tempdb_mssql_4.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp5 , FILENAME = 'E:\TempDB\tempdb_mssql_5.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp6 , FILENAME = 'E:\TempDB\tempdb_mssql_6.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp7 , FILENAME = 'E:\TempDB\tempdb_mssql_7.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = temp8 , FILENAME = 'E:\TempDB\tempdb_mssql_8.ndf' )
GO
ALTER DATABASE tempdb MODIFY FILE ( NAME = templog , FILENAME = 'E:\TempDB\templog.ldf' )
GO
```

6. Right-click the SQL Server VM, and restart the service. When prompted, click Yes.

Running the tests

In this section, we list the steps to run the HammerDB TPC-H-like test on the VMs under test. For the maximum number of streams we ran, we followed HammerDB TPC-H recommendations for the size database we were testing. Additionally, to show the scaling of each VM pair, we ran with fewer streams. Note that for each test we ran a single-stream test first to cache the database into memory before running the second test (normally multi-stream, the exception being the 1-stream test).

1. On the VM you're testing, restore the database under test to so that the database and log files reside on the Premium SSD.
2. Make sure your SQL settings and tempdb are configured properly according to the instructions above and the instance you're running on.
3. Open HammerDB.
4. Select OptionsàBenchmark.
5. Choose MSSQL Server and TPC-H.
6. Expand SQl ServeràTPC-HàSchema Build.
7. Double-click Options, change the driver to ODBC Driver 17 for SQL Server, set the scale to match your database, set MAXDOP to match that of SQL Server, and check the box for Clustered Columnstore. Click OK.
8. Expand Driver Script, double-click Options, and click OK to load.
9. Expand Virtual User, and double-click Options.
10. Choose 1 user.
11. Check the boxes for Show Output, Log Output to Temp, and Use Unique Log Name.
12. Click OK.
13. To load the driver script, double-click Double-click Load.
14. Double-click Create users.
15. To capture performance metrics on the system, start Performance monitor and set to record CPU, Memory, and drive usage information.
16. To begin the run, click Start.
17. When the run finishes, stop Perfmon, and save the HammerDB results file and Perfmon output.
18. Stop the HammerDB user.
19. Double-click User options again, and set the number of users to the appropriate count for the multi-stream test.
20. Double-click Create users.
21. To capture performance metrics on the system, start Performance monitor set to record CPU, Memory, and drive usage information.
22. To begin the run, click Start on HammerDB.
23. When the run finishes, stop Perfmon, and save the HammerDB results file and Perfmon output.
24. Reboot the VM.
25. Repeat the test two more times for a total of three runs at each user count, and record the median run.

Determining CPU vulnerability mitigation

The following figures show the Intel processor mitigation settings on the Azure instances.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ptadmin> Get-SpeculationControlSettings
For more information about the output below, please refer to https://support.microsoft.com/help/4074629

Speculation control settings for CVE-2017-5715 [branch target injection]

Hardware support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is enabled: False
Windows OS support for branch target injection mitigation is disabled by system policy: True
Windows OS support for branch target injection mitigation is disabled by absence of hardware support: True

Speculation control settings for CVE-2017-5754 [rogue data cache load]

Hardware requires 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 PCID performance optimization is enabled: True [not required for security]

Speculation control settings for CVE-2018-3639 [speculative store bypass]

Hardware is vulnerable to speculative store bypass: True
Hardware support for speculative store bypass disable is present: False
Windows OS support for speculative store bypass disable is present: True
Windows OS support for speculative store bypass disable is enabled system-wide: False

Speculation control settings for CVE-2018-3620 [L1 terminal fault]

Hardware is vulnerable to L1 terminal fault: True
Windows OS support for L1 terminal fault mitigation is present: True
Windows OS support for L1 terminal fault mitigation is enabled: True

Speculation control settings for MDS [microarchitectural data sampling]

Windows OS support for MDS mitigation is present: True
Hardware is vulnerable to MDS: True
Windows OS support for MDS mitigation is enabled: True

Suggested actions

 * Install BIOS/firmware update provided by your device OEM that enables hardware support for the branch target injection mitigation.


BTIHardwarePresent                 : False
BTIWindowsSupportPresent           : True
BTIWindowsSupportEnabled           : False
BTIDisabledBySystemPolicy          : True
BTIDisabledByNoHardwareSupport     : True
BTIKernelRetpolineEnabled          : False
BTIKernelImportOptimizationEnabled : False
KVAShadowRequired                  : True
KVAShadowWindowsSupportPresent     : True
KVAShadowWindowsSupportEnabled     : True
KVAShadowPcidEnabled               : True
SSBDWindowsSupportPresent          : True
SSBDHardwareVulnerable             : True
SSBDHardwarePresent                : False
SSBDWindowsSupportEnabledSystemWide : False
L1TFHardwareVulnerable             : True
L1TFWindowsSupportPresent          : True
L1TFWindowsSupportEnabled          : True
L1TFInvalidPteBit                  : 45
L1DFlushSupported                  : False
MDSWindowsSupportPresent           : True
MDSHardwareVulnerable              : True
MDSWindowsSupportEnabled           : True



PS C:\Users\ptadmin>
```

Figure 1: This figure shows the CPU mitigation settings on the DS_v3 series instances powered by Intel E5_v4 processors. Source: Principled Technologies.

```
PS C:\Users\ptadmin> Get-SpeculationControlSettings
For more information about the output below, please refer to https://support.microsoft.com/help/4074629

Speculation control settings for CVE-2017-5715 [branch target injection]

Hardware support for branch target injection mitigation is present: False
Windows OS support for branch target injection mitigation is present: True
Windows OS support for branch target injection mitigation is enabled: False
Windows OS support for branch target injection mitigation is disabled by system policy: True
Windows OS support for branch target injection mitigation is disabled by absence of hardware support: True

Speculation control settings for CVE-2017-5754 [rogue data cache load]

Hardware requires kernel VA shadowing: False

Speculation control settings for CVE-2018-3639 [speculative store bypass]

Hardware is vulnerable to speculative store bypass: True
Hardware support for speculative store bypass disable is present: False
Windows OS support for speculative store bypass disable is present: True
Windows OS support for speculative store bypass disable is enabled system-wide: False

Speculation control settings for CVE-2018-3620 [L1 terminal fault]

Hardware is vulnerable to L1 terminal fault: False

Speculation control settings for MDS [microarchitectural data sampling]

Windows OS support for MDS mitigation is present: True
Hardware is vulnerable to MDS: False

Suggested actions

 * Install BIOS/firmware update provided by your device OEM that enables hardware support for the branch target injection mitigation.


BTIHardwarePresent                 : False
BTIWindowsSupportPresent           : True
BTIWindowsSupportEnabled           : False
BTIDisabledBySystemPolicy          : True
BTIDisabledByNoHardwareSupport     : True
BTIKernelRetpolineEnabled          : False
BTIKernelImportOptimizationEnabled : False
KVAShadowRequired                  : False
KVAShadowWindowsSupportPresent     : True
KVAShadowWindowsSupportEnabled     : False
KVAShadowPcidEnabled               : False
SSBDWindowsSupportPresent          : True
SSBDHardwareVulnerable             : True
SSBDHardwarePresent                : False
SSBDWindowsSupportEnabledSystemWide : False
L1TFHardwareVulnerable             : False
L1TFWindowsSupportPresent          : True
L1TFWindowsSupportEnabled          : False
L1TFInvalidPteBit                  : 0
L1DFlushSupported                  : False
MDSWindowsSupportPresent           : True
MDSHardwareVulnerable              : False
MDSWindowsSupportEnabled           : False


PS C:\Users\ptadmin> _
```

Figure 2: This figure shows the CPU mitigation settings on the Dds_v4 series instances powered by Intel 2nd Generation Xeon processors. Source: Principled Technologies.

Read the report at http://facts.pt/IMBAPC9 ▶

This project was commissioned by Intel.

Principled Technologies®

Facts matter.®