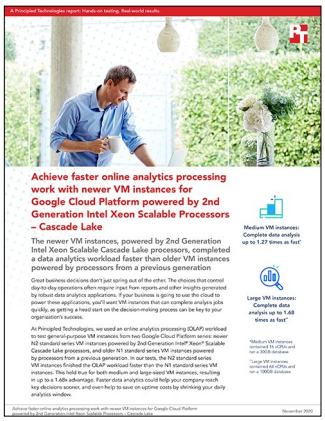

The science behind the report:

Achieve faster online analytics processing work with newer VM instances for Google Cloud Platform 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 Achieve faster online analytics processing work with newer VM instances for Google Cloud Platform powered by 2nd Generation Intel Xeon Scalable Processors – Cascade Lake.

We concluded our hands-on testing on October 29, 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 9, 2020 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

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

n-standard-16 n1 vs. n2 (30GB database)			
Time to complete in seconds	n1	n2	n2 advantage
1 stream	28	22	1.27x
2 streams	43	35	1.23x
3 streams	59	48	1.23x
4 streams	71	58	1.22x

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

n-standard-64 n1 vs. n2 (100GB database)			
Time to complete in seconds	n1	n2	n2 advantage
1 streams	48	30	1.60x
2 streams	71	43	1.65x
3 streams	94	56	1.68x
4 streams	109	67	1.63x
5 streams	114	77	1.48x

System configuration information

Table 3: Detailed information on the system we tested.

Server configuration information	n1-standard-16	n1-standard-64	n2-standard-16	n2-standard-64
Tested by	Principled Technologies	Principled Technologies	Principled Technologies	Principled Technologies
Test date	10/16/2020	10/16/2020	10/16/2020	10/16/2020
CSP / Region	us-east1-b	us-east1-b	us-east1-b	us-east1-b
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	n1-standard-16	n1-standard-64	n2-standard-16	n2-standard-64
BIOS name and version	Google Google, 1/1/2011	Google Google, 1/1/2011	Google Google, 1/1/2011	Google Google, 1/1/2011
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® E5-26XX v4	Intel Xeon E5-26XX v4	Intel Xeon Platinum 82XXCL	Intel Xeon Platinum 82XXCL
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)	60	240	64	256
NVMe memory present?	No	No	No	No
Total memory (DDR+NVMe RAM)	60	240	64	256

Server configuration information	n1-standard-16	n1-standard-64	n2-standard-16	n2-standard-64
General hardware				
Storage: Network or direct-attached	Network	Network	Network	Network
Network bandwidth per VM instance	16 Gbps	16 Gbps	16 Gbps	32 Gbps
Storage bandwidth per VM instance	400 MB/s	400 MB/s	400 MB/s	400 MB/s
Local storage (OS)				
Number of drives	1	1	1	1
Drive size (GB)	50	100	50	120
Drive information (speed, interface, type)	Standard persistent disk	Standard persistent disk	Standard persistent disk	Standard persistent disk
Local storage (data drive)				
Number of drives	1	1	1	1
Drive size (GB)	50	120	50	100
Drive information (speed, interface, type)	SSD persistent disk	SSD persistent disk	SSD persistent disk	SSD persistent disk
Network adapter				
Vendor and model	Google VirtIO Ethernet Adapter	Google VirtIO Ethernet Adapter	Google VirtIO Ethernet Adapter	Google VirtIO Ethernet Adapter
Number and type of ports	1x 100Gb	1x 100Gb	1x 100Gb	1x 100Gb

How we tested

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 Microsoft Windows Server 2019 baseline image

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

Creating the baseline image VM instance

1. Log into Google Cloud and click Go to console.
2. Click on Compute engine, then click VM instances.
3. Click the Create.
4. In the left window, select New VM instance.
5. Add the following information:
    a. Name: Name your VM instance.
    b. Labels: Use any appropriate labels.
    c. Region: Select your desired region.
    d. Zone: Select your desired zone.
    e. Machine Configuration:
    f. Machine family: General-purpose
    g. Series: E2
    h. Machine type: e2-micro
    i. CPU platform: Automatic
    j. Keep Turn on display device unchecked.
    k. Keep Confidential VM Service and Container unchecked.
    l. Boot Disk, click Change.
        i. Operating System: Windows Server
        ii. Version: Windows Server 2019 Datacenter
        iii. Boot disk type: HDD persistent disk
        iv. Size: 50GB
        v. Click Select
    m. Identity and API access: App Engine default service account.
    n. Firewall: Check Allow HTTP traffic and Allow HTTPs traffic.
    o. Click Create.

Configuring Windows Server 2019

1. Open Server Manager, and click on 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, and reboot when prompted.
5. Open Server Manager again, and click on Local Server.
6. Click 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 Installation→New 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. Click Add Current User to Specify the SQL Server administrators.
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 clicking the Start button, typing `services` to open the Services list, and disabling the Windows Update service.

Locking pages in memory

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

1. Log into Google Cloud and click Go to console.
2. Click Compute engine, then click Snapshots.
3. Click the Create snapshot button at the top of the page.
4. Enter a snapshot Name.
5. Optionally, enter a Description of the snapshot.
6. Select the Source disk from the drop-down menu. This is the boot disk for the VM instance created above.
7. Determine your snapshot storage location.
8. Under Location, select whether you want to store your snapshot in a Multi-regional location or a Regional location. We chose Regional.
9. Select which specific region or multi-region that you want to use. To use the region or multi-region that is closest to your source disk, select Based on disk's location (default). We chose us-east1.
10. Add any appropriate labels.
11. Leave everything else default.
12. Click Create to create the snapshot.

Creating your image with the baseline snapshot

1. Log into Google Cloud, and click Go to console.
2. Click Compute engine, then click Images.
3. Click the Create image button at the top of the page.
4. Specify the Name of your image.
5. Specify the Source from which you want to create an image. In our case, we used the snapshot created in the previous step.
6. Specify the Location at which to store your image. We chose us-east1.
7. Specify a family if desired.
8. Enter a description if desired.
9. Add any appropriate labels.
10. Leave default encryption choice.
11. Click Create to create the image.

Creating a standalone boot disk from the custom image

1. Log into Google Cloud, and click Go to console.
2. Click Compute engine, then click Disks.
3. Name the disk.
4. Under Type, select Standard persistent disk.
5. Select your region and zone.
6. Choose No schedule under Snapshot schedule.
7. Choose Image as your Source type.
8. Choose the image created in the previous step as your Source image.
9. Choose a size for the boot disk. Note that estimated performance improves with increasing disk size.
10. Leave encryption as Google-managed key.
11. Add any appropriate labels.
12. Click Create.

Creating the VM instances under test

To create an instance, you must first have a template. The steps below will walk you through the creation of an instance from a template.

1. Log into Google Cloud, and click Go to console.
2. Click Compute engine, then click VM instances.
3. Click the Create instance button at the top of the page.
4. In the left window, select New VM instance.
5. Add the following information:
    a. Name: Name your VM instance.
    b. Labels: Use any appropriate labels
    c. Region: Select your desired region.
    d. Zone: Select your desired zone.
    e. Machine Configuration:
    f. Machine family: General-purpose
    g. Series: <n1 or n2>
    h. Machine type: <machine type>
    i. CPU platform: For n1 series: Intel Broadwell or higher. For n2 series: Default.
    j. Keep Turn on display device unchecked.
    k. Keep Confidential VM Service and Container unchecked.
    l. Boot Disk, click Change.
        i. Select the Existing disks tab
        ii. Choose the disk you created in the previous step and click Select
    m. Identity and API access: App Engine default service account.
    n. Firewall: Check Allow HTTP traffic and Allow HTTPs traffic.
    o. Click Management, security, disks, networking, sole tenancy
        i. Click the Disks tab
        ii. Click Add new disk
        iii. Optionally, enter a name and description for the disk
        iv. Choose the disk type. We chose SSD persistent disk.
        v. Choose a size in GB. We chose 50GB for the 16vCPU VM instances, and 120GB for the 64vCPU VM instances.
        vi. Leave the rest default and click Done.
    p. Click Create.

Configuring SQL Server on the VM instances under test

In this section, we list the various SQL Server 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 the SQL Server instance, and click Properties.
3. Click Advanced node, and scroll down to the Max Degree of Parallelism, and change the value to the number of vCPUs present on the VM instance. Click OK.
4. Right-click the SQL Server instance 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 instance, 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 istance, and restart the service. Click Yes when prompted.
5. To move the tempdb to the database drive, open a new query and run the following, modified 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 Instance, and restart the service. Click Yes when prompted.

Running the tests

In this section, we list the steps to run the HammerDB TPC-H-like test on the VM instances under test. For the maximum number of users we ran, we followed HammerDB TPC-H recommendations for the size database we were testing. Additionally, to show the scaling of each VM instance pair, we ran with fewer users. 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 single-stream test).

1. On the VM instance you're testing, restore the database under test to so that the database and log files reside on the SSD persistent disk.
2. Make sure your SQL Server settings and tempdb are configured properly according to the instructions above and the VM instance you're running on.
3. Open HammerDB.
4. Select Options→Benchmark.
5. Choose MSSQL Server and TPC-H.
6. Expand SQL Server→TPC-H→Schema 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 SQL's, and check the box for Clustered Columnstore. Click OK.
8. Expand Driver Script, and double-click Options, then 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. Double-click Load to load the Driver Script.
14. Double-click Create users.
15. To capture performance metrics on the system, start Performance monitor set to record CPU, Memory, and drive usage information.
16. Click Start to begin the run.
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. Click Start on HammerDB to begin the run.
23. When the run finishes, stop Perfmon and save the HammerDB results file and Perfmon output.
24. Reboot the VM instance.
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 GCP VM instances.

```
PS C:\Windows\system32> 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: True
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: False

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: True
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

 * Follow the guidance for enabling Windows Server support for speculation control mitigations described in https://support.microsoft.com/help/4072698


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


PS C:\Windows\system32>
```

Figure 1: This figure shows the CPU mitigation settings on the N1 standard series VM instances powered by Intel E5_v4 processors. Source: Principled Technologies.

```
PS C:\Windows\system32> 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: True
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: False

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: True
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: False

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

 * Follow the guidance for enabling Windows Server support for speculation control mitigations described in https://support.microsoft.com/help/4072698


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


PS C:\Windows\system32>
```

Figure 2: This figure shows the CPU mitigation settings on the N2 standard series VM instances powered by Intel 2nd Generation Xeon processors. Source: Principled Technologies.

Read the report at http://facts.pt/0u75KOz ▶

This project was commissioned by Intel.

Principled Technologies®

Facts matter.®