The science behind the report:

Complete online analytics processing work faster with Google Cloud Platform N2 standard VM instances featuring 3rd Generation Intel Xeon Scalable Processors

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 online analytics processing work faster with Google Cloud Platform N2 standard VM instances featuring 3rd Generation Intel Xeon Scalable Processors.

We concluded our hands-on testing on November 18, 2021. 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 November 9, 2021 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Results of our data analytics tests comparing HammerDB TPROC-H workload performance of Google Cloud Platform N2 standard VM instances featuring 3rd Generation Intel Xeon Scalable processors to N2 standard VM instances featuring 2nd Generation Intel Xeon Scalable processors. All time is in seconds.

	VM instance with 3rd Gen Intel Xeon Scalable CPU	VM instance with 2nd Gen Intel Xeon Scalable CPU
n2-standard-8		
1 stream	15	12
2 streams	23	20
3 streams	30	26
n2-standard-16		
1 stream	21	17
2 streams	33	28
3 streams	45	38
4 streams	57	48
n2-standard-64		
1 stream	30	25
2 streams	44	37
3 streams	56	48
4 streams	67	59
5 streams	76	68

System configuration information

Table 2: Detailed information on the 2nd Generation Intel Xeon Scalable processor-supported N2 standard VM instances we tested.

System configuration information	n2-standard-8	n2-standard-16	n2-standard-64
Tested by	Principled Technologies	Principled Technologies	Principled Technologies
Test date	11/16/2021	11/16/2021	11/17/2021
CSP / Region	us-central1-a	us-central1-a	us-central1-a
Workload & version	HammerDB v4.2 TPROC-H	HammerDB v4.2 TPROC-H	HammerDB v4.2 TPROC-H
WL specific parameters	CCI, MAXDOP 8, 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
Server platform	n2-standard-8	n2-standard-16	n2-standard-64
BIOS name and version	Google 01/01/2011	Google 01/01/2011	Google 01/01/2011
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
Date of last OS updates/ patches applied	11/09/2021	11/09/2021	11/09/2021
Processor			
Number of processors	2	2	2
Vendor and model	Intel® Xeon® Cascade Lake	Intel Xeon Cascade Lake	Intel Xeon Cascade Lake
VM core count (per processor)	4	8	32
Core frequency (GHz)	2.80	2.80	2.80
Stepping	7	7	7
Hyper-Threading	Yes	Yes	Yes
Turbo	Yes	Yes	Yes
Total number of vCPUs per VM	8	16	64
Memory module(s)			
Total memory in system (GB)	32	64	256
NVMe memory present?	No	No	No
Total memory (DDR+NVMe RAM)	32	64	256
General HW			
Storage: NW or Direct Att / Instance	NW	NW	NW
Network BW / Instance	16 Gbps	32 Gbps	32 Gbps
Storage BW / Instance	6,400 Mbps	9,600 Mbps	9,600 Mbps

System configuration information	n2-standard-8	n2-standard-16	n2-standard-64
Local storage			
OS			
Number of drives	1	1	1
Drive size (GB)	10	10	10
Drive information (speed, interface, type)	SSD persistent disk	SSD persistent disk	SSD persistent disk
Data drive			
Number of drives	1	1	1
Drive size (GB)	25	60	180
Drive information (speed, interface, type)	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
Number and type of ports	1x 100Gb	1x 100Gb	1x 100Gb

Table 3: Detailed information on the 3rd Generation Intel Xeon Scalable processor-supported N2 standard VM instances we tested.

System configuration information	n2-standard-8	n2-standard-16	n2-standard-64
Tested by	Principled Technologies	Principled Technologies	Principled Technologies
Test date	11/16/2021	11/16/2021	11/18/2021
CSP / Region	us-central1-a	us-central1-a	us-central1-a
Workload & version	HammerDB v4.2 TPROC-H	HammerDB v4.2 TPROC-H	HammerDB v4.2 TPROC-H
WL specific parameters	CCI, MAXDOP 8, 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
Server platform	n2-standard-8	n2-standard-16	n2-standard-64
BIOS name and version	Google 01/01/2011	Google 01/01/2011	Google 01/01/2011
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
Date of last OS updates/ patches applied	11/09/2021	11/09/2021	11/09/2021

System configuration information	n2-standard-8	n2-standard-16	n2-standard-64
Processor			
Number of processors	2	2	2
Vendor and model	Intel Xeon Ice Lake	Intel Xeon Ice Lake	Intel Xeon Ice Lake
VM core count (per processor)	4	8	32
Core frequency (GHz)	2.60	2.60	2.60
Stepping	6	6	6
Hyper-Threading	Yes	Yes	Yes
Turbo	Yes	Yes	Yes
Total number of vCPUs per VM	8	16	64
Memory module(s)			
Total memory in system (GB)	32	64	256
NVMe memory present?	No	No	No
Total memory (DDR+NVMe RAM)	32	64	256
General HW			
Storage: NW or Direct Att / Instance	NW	NW	NW
Network BW / Instance	16 Gbps	32 Gbps	32 Gbps
Storage BW / Instance	6,400 Mbps	9,600 Mbps	9,600 Mbps
Local storage			
OS			
Number of drives	1	1	1
Drive size (GB)	10	10	10
Drive information (speed, interface, type)	SSD persistent disk	SSD persistent disk	SSD persistent disk
Data drive			
Number of drives	1	1	1
Drive size (GB)	25	60	180
Drive information (speed, interface, type)	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
Number and type of ports	1x 100Gb	1x 100Gb	1x 100Gb

How we tested

Testing overview

We tested Google Cloud Platform VM instances featuring 3rd Generation Intel Xeon Scalable processors and compared them to VM instances featuring 2nd Generation Intel Xeon Scalable processors. We ran the TPROC-H workload from HammerDB on Microsoft SQL Server 2019 to show the time to complete savings for analytic databases that customers can expect to see using VM instances with newer processors vs. older ones.

Creating the Windows Server 2019 baseline image

Creating the baseline image

1. Log into Google Cloud, and click Go to console.
2. Click Compute engine, and click VM instances.
3. Click the Create button.
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. We used us-central1.
    d. Zone: Select your desired zone.
    e. Machine Configuration:
    f. Machine family: General-purpose
    g. Series: N2
    h. Machine type: n2-standard-4
    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
        ii. Version: Windows Server 2019 Datacenter
        iii. Boot disk type: SSD 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. Download the VM instance RDP file, and connect to the instance.
2. Open Server Manager, and click Local Server.
3. Disable IE Enhanced Security Configuration.
4. Change the time zone to your local time zone.
5. Change the name of your server.
6. When prompted, reboot the server.
7. Open Server Manager again, and click Local Server.
8. Click to run updates.
9. Run updates, rebooting when prompted, until the server shows no new updates to install.

Installing 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 box for I accept the license terms and Privacy Statement, and click Next.
6. Check the box for Use Microsoft Update to check for updates (recommended), 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. 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 the TempDB tab.
14. Set the number of tempdb files to 8, with a file size of 1024MB each.
15. Set the log file to a size of 1024MB.
16. Click Next.
17. Once you've passed the rule check, click Next.
18. Click Install.
19. When the installation is complete, go back to the SQL Server Installation Center, and click Install SQL Server Management Tools.
20. Download the SSMS file, and install with defaults.
21. When prompted, reboot the server.
22. To ensure there aren't any new updates for SQL Server, run Windows Update one more time (make sure Windows Updates are set to get updates for other Microsoft products).
23. Once you've installed all available updates, to disable the Windows Update service, click the Start button, type `services` to open the Services list, and disable the Windows Update service.

Locking pages in memory

1. Click Start, and type `Local Security Policy`. Open the program.
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, and close the Local Security Policy window.

Installing HammerDB 4.2

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, and click Snapshots.
3. At the top of the page, click the Create snapshot button.
4. Enter a snapshot Name.
5. Optionally, enter a Description of the snapshot.
6. From the drop-down menu, select the Source disk. This is the boot disk for the VM instance you 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-central1.
10. Add any appropriate labels.
11. Leave everything else as default.
12. To create the snapshot, click Create.

Creating your Image with the baseline snapshot

1. Log into Google Cloud, and click Go to console.
2. Click Compute engine, and click Images.
3. At the top of the page, click the Create image button.
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 we created in the previous step.
6. Specify the Location at which to store your image. We chose us-central1.
7. Specify a family, if desired.
8. Enter a description, if desired.
9. Add any appropriate labels.
10. Leave the default encryption choice.
11. To create the image, click Create.

Creating the VM instances under test

In this section we list the steps required to create a VM instance from the image we created previously. For the list of VM instances and SSDs we used, see Table 4, and follow the steps using the proper specifications for the VM instance you wish to create. For our testing, we used the us-central1 region and Zone a.

Creating the VM instances from the specialized image

1. Log into Google Cloud, and click Go to Console.
2. Click Compute engine, and click Images.
3. Click your baseline image.
4. Click Create Instance.
5. Add the following information:
    a. Name: Name your VM instance.
    b. Labels: Use any appropriate labels.
    c. Region: Select your desired region. We used us-central1.
    d. Zone: Select your desired zone.
    e. Machine Configuration:
    f. Machine family: General-purpose
    g. Series: N2
    h. Machine type: n2-standard-{8,16,64}
    i. CPU platform: {Cascade Lake, Ice Lake} or above
    j. Keep Turn on display device unchecked.
    k. Keep Confidential VM Service and Container unchecked.
    l. Boot Disk, click Change:
        i. Operating System: Ubuntu
        ii. Version: Ubuntu 20.04 LTS
        iii. Boot disk type: SSD persistent disk
        iv. Size: 10GB
        v. Click Select
    m. Identity and API access: App Engine default service account.
    n. Firewall: Check Allow HTTP traffic and Allow HTTPs traffic.
    o. Expand Networking, Disks, Security, Management, Sole-Tenancy
    p. Expand Disks
    q. Click Add New Disk:
        i. Name: Name the disk
        ii. Disk source type: Blank disk
        iii. Disk type: SSD persistent disk
        iv. Size: {25,60,180}GB
        v. Labels: add appropriate label
        vi. Mode: Read/write
        vii. Deletion rule: Delete disk
        viii. Click Save.
    r. Click Create.

Configuring SQL Server 2019 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. To see the exact settings for each VM instance, please refer to Table 4.

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

1. Open the SQL Server Management Studio.
2. Right-click the SQL Instance, and click Properties.
3. Click Advanced node, scroll down to the Max Degree of Parallelism, and change the value. Click OK.
4. Right-click the SQL Instance, and go to Memory.
5. Set the Max Memory to 90 percent of the total memory in the system. Click OK, and close the Properties window.
6. Right-click the SQL instance, and restart the service. When prompted, click Yes.

Running the tests

In this section, we list the steps to run the HammerDB TPROC-H test on the VM instances under test. As each VM instance had different hardware and database sizes, please refer to Table 4 to see the number of users to run on each VM. To determine the maximum number of users to run, we followed TPC-H recommendations for the size database we were testing. Additionally, to show the scaling of each VM pair, we ran with fewer users. Note that for each test, we first ran a single-stream test 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 instance under test, restore the database under test to so that the database and log files reside on the data disk.
2. Make sure your SQL 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 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 SQL's, and check the box for Clustered Columnstore. Click OK.
8. Expand Driver Script, and double-click Options. To load, click OK.
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 Load.
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. To begin the test 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, 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. In HammerDB, to begin the run, click Start.
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.

Table 4: Configuration information for the VM instances we tested.

Instance type	n2-standard-8	n2-standard-16	n2-standard-64
Number of vCPU	8	16	64
Memory (GB)	32	64	256
Data disk (GB)	25	60	180
TPROC-H database scale	10	30	100
Max number of users	3	4	5
MAXDOP	8	16	64

Mitigations

n2 (CLX)

```
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
```

n2 (ICX)

```
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: 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: 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: False
Speculation control settings for MDS [microarchitectural data sampling]
Windows OS support for MDS mitigation is present: True
Hardware is vulnerable to MDS: False
```

Read the report at https://facts.pt/5qbfLud ▶

This project was commissioned by Intel.

Principled Technologies®

Facts matter.®