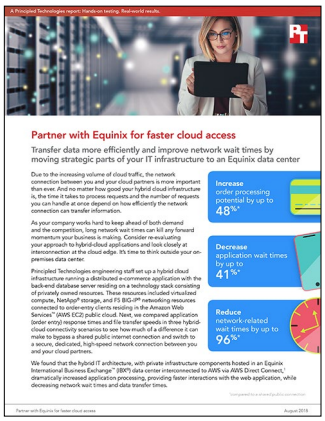


The science behind the report:

Partner with Equinix for faster cloud access

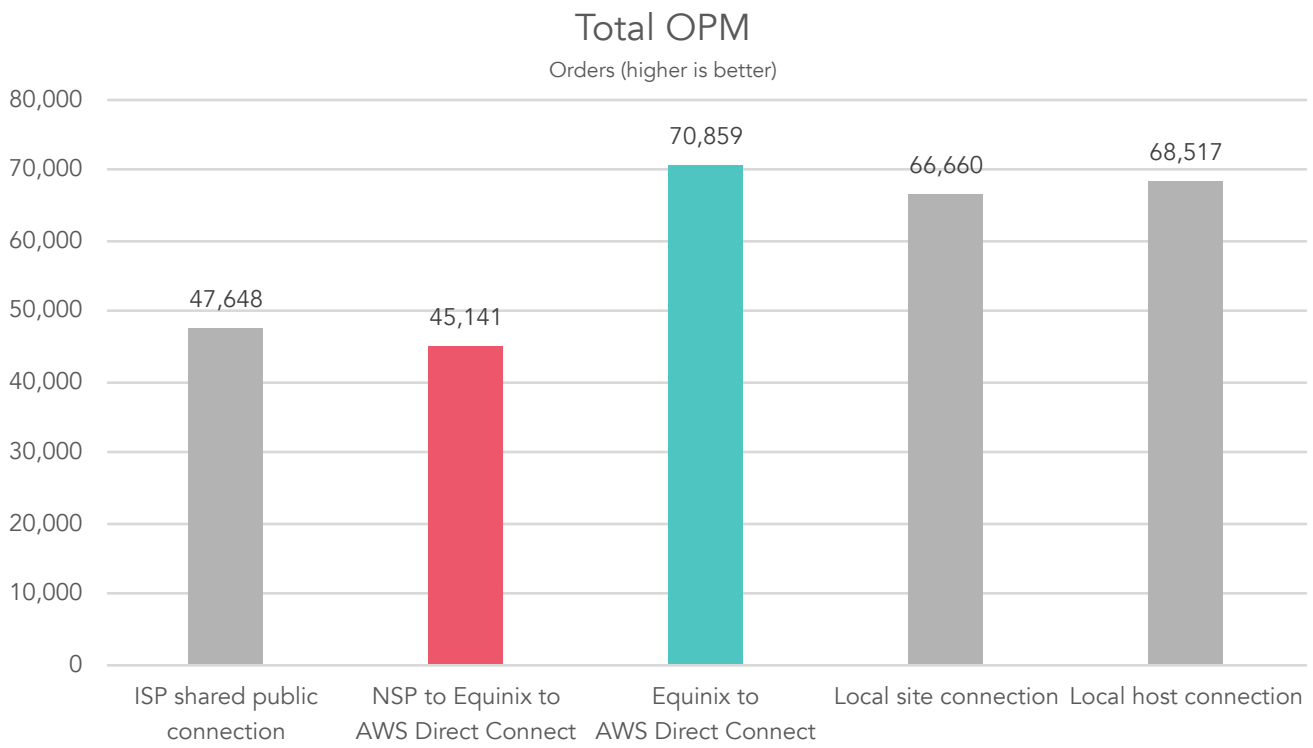
This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report "Partner with Equinix for faster cloud access".

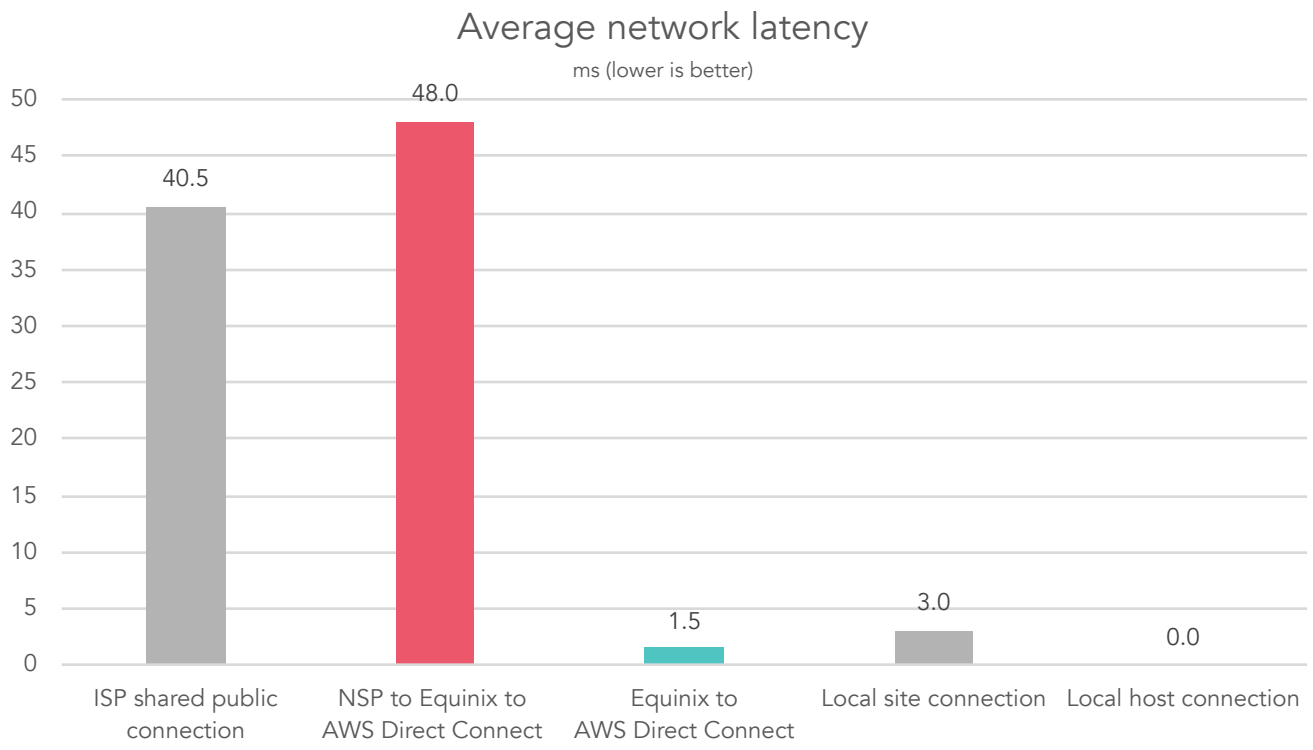
On March 15, 2018, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. Cloud resources reside on shared equipment that is not dedicated to specific workloads. On any given day, variations in resource consumption on shared equipment can produce variability and anomalies in workload performance. We concluded hands-on testing on March 21, 2018.

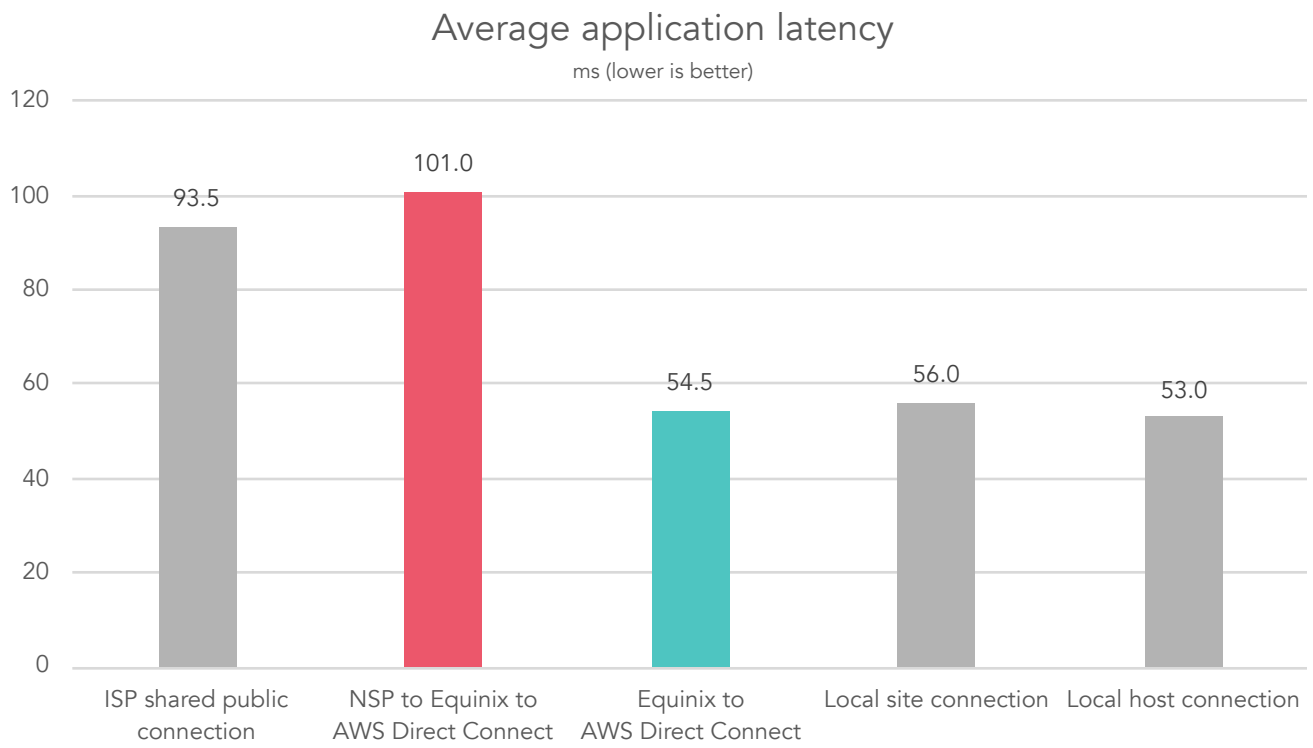
Appendix A: Our results

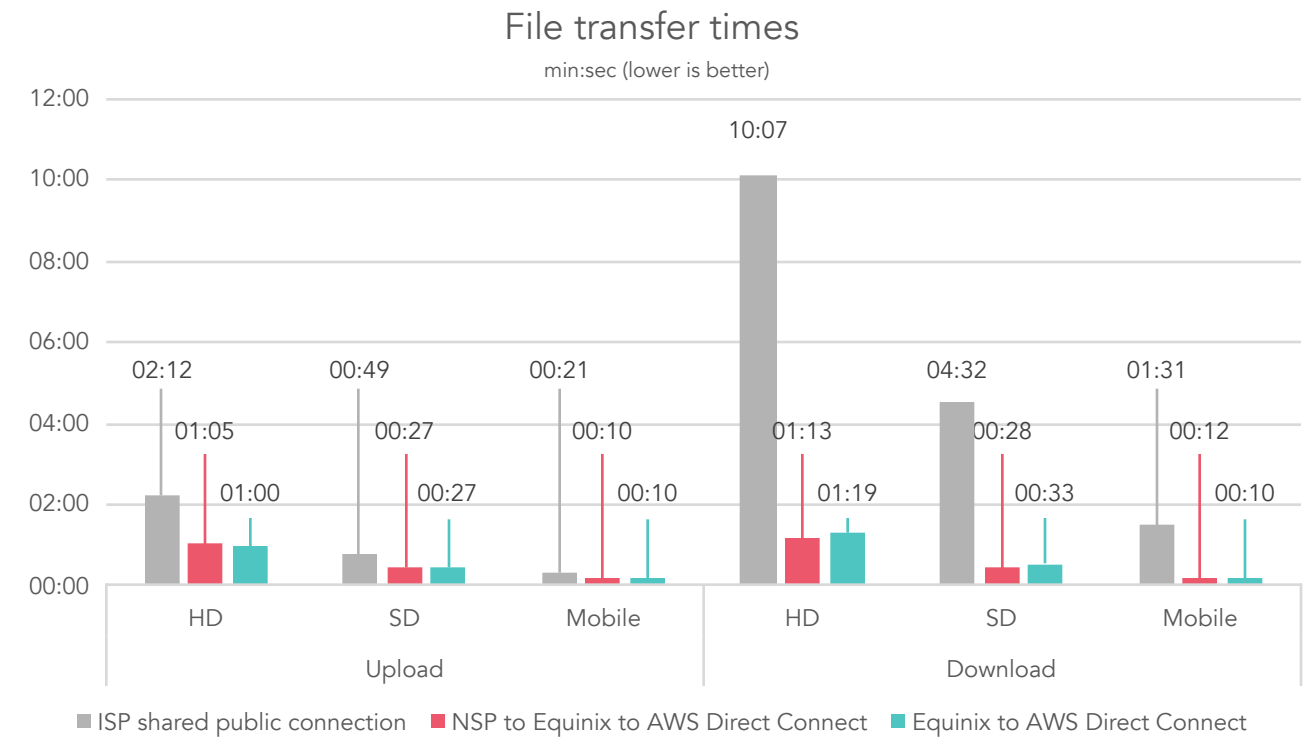
Results with local comparison

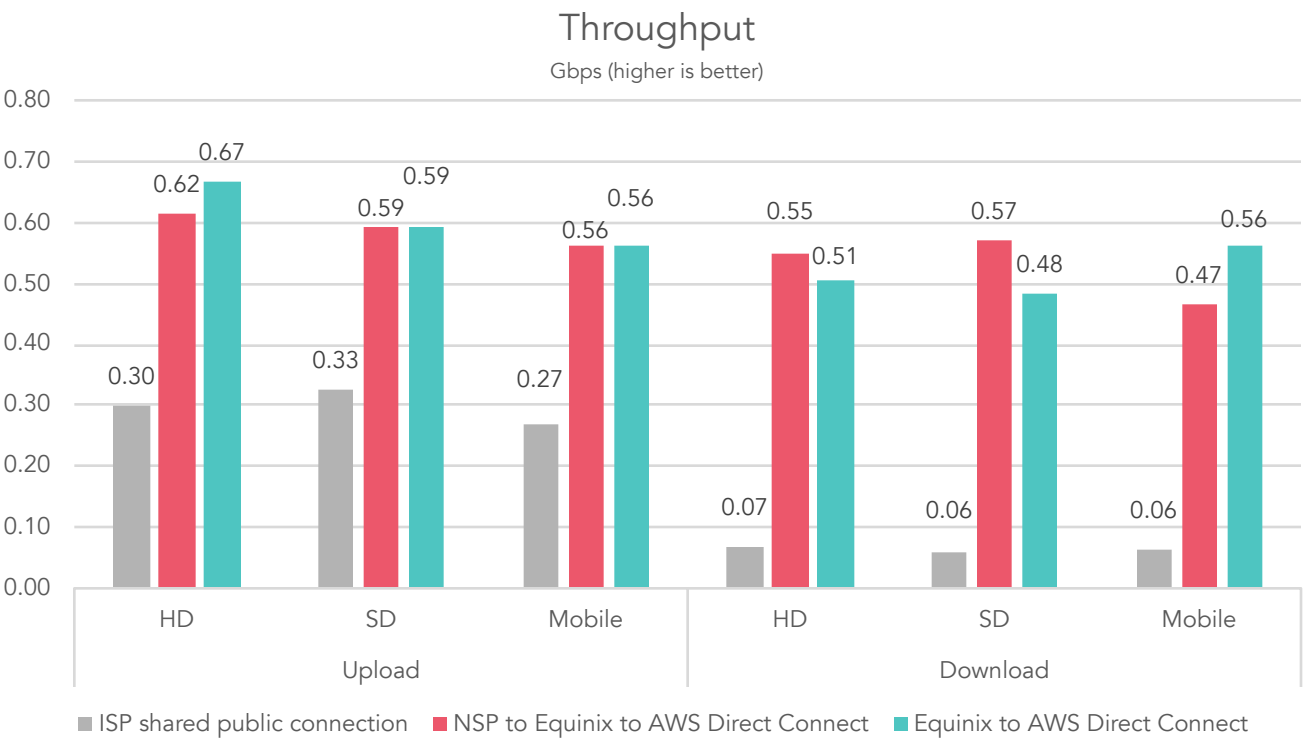
For these tests, we measured both dual-server and single-server connections to determine the amount of latency produced solely by the application. We subtracted the single-server application latency from other test cases to arrive at our average network latency number.




Average network latency
ms (lower is better)
50
45
40
35
30
25
20
15
10
5
0
40.5
48.0
1.5
3.0
0.0
ISP shared public connection
NSP to Equinix to AWS Direct Connect
Equinix to AWS Direct Connect
Local site connection
Local host connection


Average application latency
ms (lower is better)
120
100
80
60
40
20
0
93.5
101.0
54.5
56.0
53.0
ISP shared public connection
NSP to Equinix to AWS Direct Connect
Equinix to AWS Direct Connect
Local site connection
Local host connection


File transfer times
min:sec (lower is better)
12:00
10:00
08:00
06:00
04:00
02:00
00:00
02:12
01:05
01:00
00:49
00:27
00:27
00:21
00:10
00:10
10:07
01:13
01:19
04:32
00:28
00:33
01:31
00:12
00:10
HD
SD
Mobile
HD
SD
Mobile
Upload
Download
ISP shared public connection
NSP to Equinix to AWS Direct Connect
Equinix to AWS Direct Connect


Throughput
Gbps (higher is better)
0.80
0.70
0.60
0.50
0.40
0.30
0.20
0.10
0.00
0.30
0.62
0.67
0.33
0.59
0.59
0.27
0.56
0.56
0.07
0.55
0.51
0.06
0.57
0.48
0.06
0.47
0.56
HD
SD
Mobile
HD
SD
Mobile
Upload
Download
ISP shared public connection
NSP to Equinix to AWS Direct Connect
Equinix to AWS Direct Connect

Appendix B: System configuration information

Server under test

Server configuration information	Dell EMC™ PowerEdge™ R730xd
BIOS name and version	Dell™ 2.0.2
Non-default BIOS settings	Virtualization enabled
Operating system name and version/build number	VMware® ESXi™ 6.0.0 build-3620759
Date of last OS updates/patches applied	06/13/17
Power management policy	Balanced
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® E5-2690 v3
Core count (per processor)	12
Core frequency (GHz)	2.60
Memory module(s)	
Total memory in system (GB)	128
Number of memory modules	16
Vendor and model	Hynix HMA41GR7MFR4N-TF
Size (GB)	8
Type	PC4-17000
Speed (MHz)	2,133
Speed running in the server (MHz)	2,133
Storage controller	
Vendor and model	Dell PERC H730 MINI
Cache size (GB)	2
Firmware version	24.4.2.0001
Driver version	1.0.1
Local storage	
Number of drives	14
Drive vendor and model	Seagate® ST3000NM0023
Drive size (GB)	3000
Drive information (speed, interface, type)	7.2K, 6Gb SAS, HDD
Network adapter	
Vendor and model	Broadcom® NetXtreme® BCM5720 Gigabit Ethernet PCIe
Number and type of ports	4 x 1Gb RJ45

Server configuration information	Dell EMC PowerEdge R730xd
Cooling fans	
Vendor and model	Dell internal system fan
Number of cooling fans	6
Power supplies	
Vendor and model	Dell 0HTRH4A01
Number of power supplies	2
Wattage of each (W)	750

Storage solution

Storage configuration information	NetApp® FAS3240
Controller software version	NetApp Release 8.3RC1
Number of storage controllers	2
Number of storage shelves	1
Number of drives per shelf	24
Drive vendor and model number	Seagate ST3600057SS
Drive size (GB)	600
Drive information (speed, interface, type)	15K, 6Gb SAS, HDD

Network switch

Network switch configuration information	F5 BIG-IP® 4200
Firmware revision	BIG-IP 12.1.2 Build 0.0.249 Final
Number and type of ports	8 x RJ45 1Gb Ethernet
Number and type of ports used in test	4 x RJ45 1Gb Ethernet

Appendix C: How we tested

Configuring NetApp FAS3240 and DS4240

Deploying storage

1. Rack the NetApp disk shelf and controller.
2. Cable the solution appropriately. For more information, see http://docs.netapp.com/documentation/docweb/index.html?productID=30340&language=en-US.
3. Power on the disk shelf.
4. Plug a serial console cable into the console port on the top controller in the FAS3240.
5. Plug the other end of the serial console cable into your laptop.
6. Start a terminal emulator (Putty, OS X® Terminal, etc.) on the laptop.
7. Power on the FAS4240.
8. Wait until prompted to escape into the bootloader.
9. On the bootloader prompt, type the following commands:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.factory_init_completed true
setenv bootarg.init.clearvarfsnvram true
```

10. Type: `bye`
11. Click Enter.
12. To start NetApp boot menu, press Control-C.
13. At the boot menu, instead of providing a number, type: `wipeconfig`, and click enter. The system will reboot.
14. At the prompt, to clean configuration and initialize all disks, select 4. The system will reboot again.
15. Perform steps 1 through 14 on the bottom controller in the FAS3240.
16. Follow the initial CLI startup wizards on both controllers.
17. Download and launch the NetApp configuration utility on your laptop. The application will discover the NetApp FAS3240 array and lead you through cluster creation and configuration. The NetApp CLI is now available at the cluster IP address, and the Web UI is available as well.

Configuring storage

Deploying Dell EMC PowerEdge R730xd

1. Connect the iDRAC and NIC1 to the Top-of-Rack (ToR) management switch.
2. Connect NIC2 to the F5 BIG-IP 4000 series port 1.1.
3. Connect NIC4 to the F5 BIG-IP 4000 series port 1.6.
4. Connect the Fibre Channel port 1 to the Brocade 300 Fibre Channel switch.
5. Power on the server.
6. To start system setup, press F2.
7. Configure the system with the performance profile. Save the changes, and exit to reboot.
8. To run the RAID configuration utility, press CTRL-R when prompted.
9. On the VD Mgmt page, select PERC H730P Mini, and press F2.
10. Select Create New VD, and click Enter.
11. Configure the new virtual disk with the following information, and click OK:
    - RAID-1
    - Select two physical disks
    - VD Name = OS
12. Click F2.
13. Select Create New VD, and press Enter.
14. Configure the new virtual disk with the following information, and click OK:
    - RAID-10
    - Select the remaining physical disks
    - VD Name = data

15. Set each virtual disk to fast initialize:
    - Select the virtual disk name, and click F2
    - Select initialization→Fast Init→OK
16. To exit the controller configuration utility, click Esc.
17. Reboot the server.

Installing VMware ESXi on Dell EMC PowerEdge R730xd

1. Insert the VMware vSphere® installation media, and power on the server.
2. Select the standard vSphere installer, and allow the files to copy into memory.
3. At the welcome screen, press F11.
4. At the keyboard language selection screen, click Enter.
5. Provide a password twice for the root user, and click Enter.
6. Select the mirrored disk volume you created as the installation target.
7. Allow the installer to finish installing vSphere, and reboot the server.
8. At the home screen, press F2, and provide your credentials.
9. Select Configure Management Network.
10. Select IP Configuration.
11. Provide your static IP information, and click Enter.
12. Select DNS Configuration.
13. Provide a hostname, and click Enter.
14. Click Esc-Y to restart the management network.

Deploying VMware vCenter Server®

Use the steps below to install the vCenter Server Appliance™ onto a VMware ESXi or vCenter server outside of the testing environment. For the deployment outlined here, your server or VM must have at least two processors and 8 GB of RAM. On a Windows server or VM, locate the installer image VMware-VCSA-all-6.0.0-3040890.iso.

1. Mount the image, navigate to the vcsa folder, and launch VMware-ClientIntegrationPlugin-6.0.0.exe.
2. In the wizard that appears, click Next.
3. Accept the terms of the license agreement, and click Next.
4. Leave the default installation directory, and click Next.
5. Click Install.
6. Click Finish.
7. In the mounted image's top directory, open vcsa-setup.html.
8. When prompted, click Allow.
9. Click Install.
10. Accept the terms of the license agreement, and click Next.
11. Provide the FQDN or IP address of the host where you are deploying the vCenter Server Appliance.
12. Provide a username and password for the system in question, and click Next.
13. Accept the certificate of the host you chose to connect to by clicking Yes.
14. Select the appropriate data center, and click Next.
15. Select the appropriate resource, and click Next.
16. Provide a name and password for the virtual machine, and click Next.
17. Select Install vCenter Server with an Embedded Platform Services Controller, and click Next.
18. Select Create a new SSO domain.
19. Provide a password, and confirm it.
20. Provide an SSO Domain name and SSO Site name, and click Next.
21. Set an appropriate Appliance Size, and click Next.
22. Select an appropriate datastore, and click Next.
23. Select Use an embedded database (PostgreSQL), and click Next.
24. At the Network Settings page, configure the network settings as appropriate for your environment, and click Next.
25. Review your settings, and click Finish.
26. When installation completes, click Close.

Deploying Microsoft® SQL Server® virtual machine

Installing Microsoft Windows Server® 2016

1. Set the installation ISO file as the virtual media device for the virtual machine, click connect at power on, and start the server.
2. Select any key when prompted to boot from DVD.
3. When the installation screen appears, leave language, time/currency format, and input method as default, and click Next.
4. Click Install Now.
5. When the installation prompts you, provide the product key.
6. Select Windows Server 2016 Standard Edition (Server with a GUI), and click Next.
7. Check I accept the license terms, and click Next.
8. Click Custom: Install Windows only (advanced).
9. Select Drive 0 Unallocated Space, and click Next, at which point Windows begins automatically, and restarts automatically after completing.
10. When the Settings page appears, fill in the Password and Reenter Password fields with the same password.
11. Log in with the password you set up previously.

Installing Microsoft SQL Server 2016

1. Mount the installation DVD for SQL Server 2016.
2. Click Run SETUP.EXE. If Autoplay does not begin the installation, navigate to the SQL Server 2016 DVD, and double-click it.
3. In the left pane, click Installation.
4. Click New SQL Server stand-alone installation or add features to an existing installation.
5. Select Enter the Product Key Radio, provide the product key, and click Next.
6. Click the checkbox to accept the license terms, and click Next.
7. Click Use Microsoft Update to check for updates, and click Next.
8. Click Install to install the setup support files.
9. If there are no failures displayed, click Next.
10. At the Setup Role screen, choose SQL Server Feature Installation, and click Next.
11. At the Feature Selection screen, select Database Engine Services, Full-Text and Semantic Extractions for Search, Client Tools Connectivity, Client Tools Backwards Compatibility, Management Tools – Basic, and Management Tools – Complete, and click Next.
12. At the Installation Rules screen, after the check completes, click Next.
13. At the Instance configuration screen, leave the default selection of default instance, and click Next.
14. At the Server Configuration screen, choose NT Service\SQLSERVERAGENT for SQL Server Agent, and choose NT Service\MSSQLSERVER for SQL Server Database Engine.
15. Change the Startup Type to Automatic, and click Next.
16. At the Database Engine Configuration screen, select the Mixed Mode authentication method.
17. Provide and confirm a password for the system administrator account.
18. Click Add Current user. This may take several seconds.
19. Click the Data Directories tab to relocate the system, user, and tempdb files.
20. Change the location of the root directory to the D:\ volume.
21. Click Next.
22. At the Error and usage reporting screen, click Next.
23. At the Installation Configuration Rules screen, check that there are no failures or relevant warnings, and click Next.
24. At the Ready to Install screen, click Install.
25. After installation completes, click Close.
26. Close the installation window.
27. Open SQL Server 2016 Configuration Manager, and expand Protocols for MSSQLSERVER.
28. Right-click Named Pipes, and choose Enabled.
29. Click OK, and restart the SQL service.

Configuring F5 BIG-IP 4000

This is the configuration of our F5 BIG-IP 4000 as shown in the bigip.conf file:

```
#TMSH-VERSION: 12.1.2
apm report default-report {
    report-name sessionReports/sessionSummary
    user /Common/admin
}
ltm default-node-monitor {
    rule /Common/icmp
}
ltm node /Common/SQL {
    address 192.168.0.30
}
ltm pool /Common/SQL_Pool {
    members {
        /Common/SQL:0 {
            address 192.168.0.30
            monitor /Common/gateway_icmp
        }
    }
    monitor /Common/gateway_icmp
}
ltm virtual /Common/InboundFromAWS-DirectConnect {
    destination /Common/192.168.0.0:0
    ip-forward
    mask 255.255.255.0
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
    source 0.0.0.0/0
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}
ltm virtual /Common/JPerf {
    destination /Common/66.57.81.14:5001
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/SQL_Pool
    profiles {
        /Common/tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm virtual /Common/Outbound {
    destination /Common/0.0.0.0:0
    ip-forward
    mask any
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
    source 192.168.0.0/24
    translate-address disabled
    translate-port disabled
```

```
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}
apm report default-report {
    report-name sessionReports/sessionSummary
    user /Common/admin
}
ltm default-node-monitor {
    rule /Common/icmp
}
ltm node /Common/SQL {
    address 192.168.0.30
}
ltm pool /Common/SQL_Pool {
    members {
        /Common/SQL:0 {
            address 192.168.0.30
            monitor /Common/gateway_icmp
        }
    }
    monitor /Common/gateway_icmp
}
ltm virtual /Common/InboundFromAWS-DirectConnect {
    destination /Common/192.168.0.0:0
    ip-forward
    mask 255.255.255.0
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
    source 0.0.0.0/0
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}
ltm virtual /Common/JPerf {
    destination /Common/66.57.81.14:5001
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/SQL_Pool
    profiles {
        /Common/tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm virtual /Common/Outbound {
    destination /Common/0.0.0.0:0
    ip-forward
    mask any
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
```

```
    source 192.168.0.0/24
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}

apm report default-report {
    report-name sessionReports/sessionSummary
    user /Common/admin
}
ltm default-node-monitor {
    rule /Common/icmp
}
ltm node /Common/SQL {
    address 192.168.0.30
}
ltm pool /Common/SQL_Pool {
    members {
        /Common/SQL:0 {
            address 192.168.0.30
            monitor /Common/gateway_icmp
        }
    }
    monitor /Common/gateway_icmp
}
ltm virtual /Common/InboundFromAWS-DirectConnect {
    destination /Common/192.168.0.0:0
    ip-forward
    mask 255.255.255.0
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
    source 0.0.0.0/0
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}
ltm virtual /Common/JPerf {
    destination /Common/66.57.81.14:5001
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/SQL_Pool
    profiles {
        /Common/tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm virtual /Common/Outbound {
    destination /Common/0.0.0.0:0
    ip-forward
```

```
    mask any
    profiles {
        /Common/apm-forwarding-fastL4 { }
    }
    source 192.168.0.0/24
    translate-address disabled
    translate-port disabled
    vlans {
        /Common/VLAN169
        /Common/http-tunnel
        /Common/internal
        /Common/socks-tunnel
    }
    vlans-enabled
}
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm virtual /Common/PSEXEC-445 {
    destination /Common/66.57.81.14:445
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/SQL_Pool
    profiles {
        /Common/tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
}
ltm virtual /Common/SQL_inbound {
    destination /Common/66.57.81.14:1433
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/SQL_Pool
    profiles {
        /Common/tcp { }
    }
    source 0.0.0.0/0
    translate-address enabled
    translate-port enabled
}
ltm virtual-address /Common/0.0.0.0 {
    address any
    arp disabled
    icmp-echo disabled
    mask any
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/10.209.0.0 {
    address 10.209.0.0
    arp disabled
    icmp-echo disabled
    mask 255.255.0.0
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/65.57.81.1 {
    address 65.57.81.1
    arp enabled
    icmp-echo enabled
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
```

```
}
ltm virtual-address /Common/65.57.81.14 {
    address 65.57.81.14
    arp enabled
    icmp-echo enabled
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/66.57.81.0 {
    address 66.57.81.0
    arp disabled
    icmp-echo disabled
    mask 255.255.255.240
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/66.57.81.1 {
    address 66.57.81.1
    arp enabled
    icmp-echo enabled
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/66.57.81.13 {
    address 66.57.81.13
    arp enabled
    icmp-echo enabled
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
}
ltm virtual-address /Common/66.57.81.14 {
    address 66.57.81.14
    arp enabled
    icmp-echo enabled
    mask 255.255.255.255
    traffic-group /Common/traffic-group-local-only
}
ltm virtual-address /Common/192.168.0.0 {
    address 192.168.0.0
    arp disabled
    icmp-echo disabled
    mask 255.255.255.0
    traffic-group /Common/traffic-group-1
}
net route /Common/external_default_gateway {
    interface /Common/VLAN169
    network default
}
net ipsec ike-daemon /Common/ikedaemon { }
pem global-settings analytics { }
security dos udp-portlist /Common/dos-udp-portlist {
    list-type exclude-listed-ports
}
security firewall config-change-log {
    log-publisher /Common/local-db-publisher
}
sys ecm cloud-provider /Common/aws-ec2 {
    description "The aws-ec2 parameters"
    property-template {
        account { }
        availability-zone {
            valid-values { a b c d }
        }
        instance-type {
            valid-values { t2.micro t2.small t2.medium m3.medium m3.large m3.xlarge
m3.2xlarge c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge r3.large r3.xlarge
r3.2xlarge r3.4xlarge r3.8xlarge }
        }
```

```
        region {             valid-values { us-east-1 us-west-1 us-west-2 sa-east-1 eu-
west-1 eu-central-1 ap-southeast-2 ap-southeast-1 ap-northeast-1 }
        }
    }
}
sys ecm cloud-provider /Common/dnet {
    description "The dnet parameters"
}
sys ecm cloud-provider /Common/vsphere {
    description "The vsphere parameters"
    property-template {
        cloud-host-ip { }
        dhcp-network-name { }
        end-point-url { }
        node-name { }
    }
}
sys software update {
    auto-check enabled
    auto-phonehome enabled
    frequency weekly
}
wom endpoint-discovery { }
```

Configuring DVD Store 2

For our testing, we generated the data using the Install.pl script included with DVD Store version 2.1 (DS2). This provided the parameters for our 20GB database size and the Microsoft SQL Server 2016 platform. We ran the Install.pl script on a utility system running Linux®. The Install.pl script also generated the database schema.

After processing the data generation, we transferred the data files and schema creation files to a Windows-based system running SQL Server 2016. We built the 4GB database in SQL Server 2016, and then performed a full backup, storing the backup file on the C: drive for quick access. We used that backup file to restore the server between test runs.

The only modification we made to the schema creation scripts were the specified file sizes for our database. We explicitly set the file sizes higher than necessary to ensure that no file-growth activity would affect the outputs of the test. Besides this file size modification, we created and loaded the database schema according to the DVD Store documentation. Specifically, we followed the steps below:

1. We generated the data and created the database and file structure using database creation scripts in the DS2 download. We made size modifications specific to our 20GB database, and the appropriate changes to drive letters.
2. We transferred the files from our Linux data generation system to a Windows system running SQL Server.
3. We created database tables, stored procedures, and objects using the provided DVD Store scripts.
4. We set the database recovery model to bulk-logged to prevent excess logging.
5. We loaded the data we generated into the database. For data loading, we used the import wizard in SQL Server Management Studio. Where necessary, we retained options from the original scripts, such as Enable Identity Insert.
6. Using the database-creation scripts, we created indices, full-text catalogs, primary keys, and foreign keys.
7. We updated statistics on each table according to database-creation scripts, which sample 18 percent of the table data.
8. On the SQL Server instance, we created a ds2user SQL Server login using the following Transact-SQL (T-SQL) script:

```
USE [master]
GO
CREATE LOGIN [ds2user] WITH PASSWORD=N'',
DEFAULT_DATABASE=[master],
DEFAULT_LANGUAGE=[us_english],
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF
GO
```

9. We set the database recovery model back to full.
10. Using SQL Server Management Studio, we created the necessary full text index.
11. We created a database user, and mapped this user to the SQL Server login.
12. We performed a full backup of the database. This backup allowed us to restore the databases to a pristine state relatively quickly between tests.

Configuring the database workload client

For our testing, we used virtual clients for the Microsoft SQL Server client. To create these clients, we installed Windows Server 2016 on Amazon® EC2 instances, assigned a static IP address, and installed .NET 3.5.

Running the DVD Store tests

For our testing, we created a series of batch files, SQL scripts, and shell scripts to automate the complete test cycle. DVD Store outputs an orders-per-minute (OPM) metric, which is a running average calculated throughout the test. In this report, we document the last OPM reported by each client/target pair, as well as the application latency.

Each complete test cycle consisted of the following general steps:

1. Clean up prior outputs from the target system and the client driver system.
2. Drop the database from the target.
3. Restore the database on the target.
4. Shut down the target.
5. Reboot the host and client system.
6. Wait for a ping response from the server under test and the client system.
7. Let the test server idle for 10 minutes.
8. Start the DVD Store driver on the client.

We used the following DVD Store parameters for testing:

```
ds2sqlserverdriver.exe --target=<target_IP> --ramp_rate=10 --run_time=30 --n_threads=32
--db_size=20GB --think_time=50 --warmup_time=5 --report_rate=1 --csv_output=<drive path>
```

Running the file transfer tests

For our testing, we created three different video files to test file transfer times using Windows Explorer. Using a stopwatch, we timed the transfer duration copying to and from the AWS cloud-based VMs with each size of files. For the public internet connection, we tested at different times of day to find a median for performance comparison. We rotated the file tests to ensure that disk caching wasn't reusing the previous copy data.

Running the test cycles:

1. Copy the local source file.
2. To paste while simultaneously starting the timer, select the cloud-based target folder, and type `Ctrl-V`.
3. When the copy finishes, stop the timer.
4. Repeat the process with the next file, until all three have been tested.
5. Reverse the process, copying all three files individually from the cloud folder to a local folder.
6. Delete the local and remote copies of the files.
7. To determine median values, repeat these steps with the original source files a total of three times.

Read the report at http://facts.pt/6dvksi ▶

This project was commissioned by Equinix.

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.