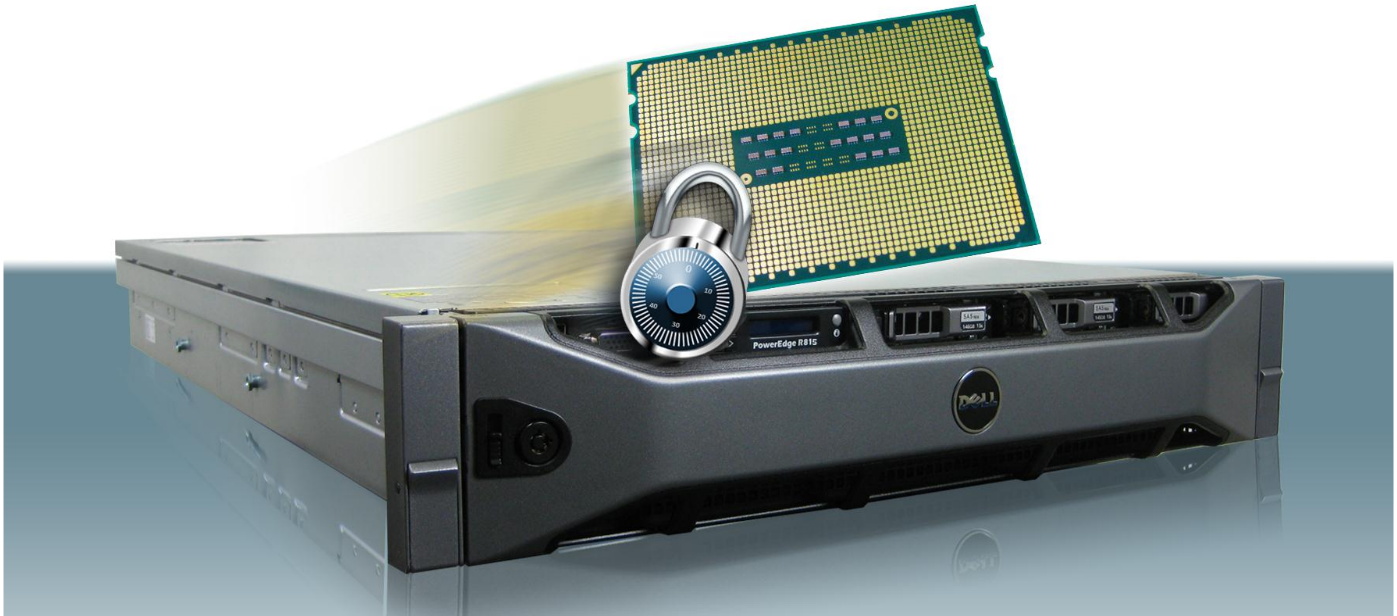
Dell™ PowerEdge™ R815 servers with AMD Opteron™ 6200 Series processors: Data protection with full disk encryption



Risk mitigation with outstanding performance

Protecting your company's data is a key part of maintaining your corporate reputation. It is a given that you want the strongest security you can find for your server's hard drives, and full disk encryption (FDE) is a great way to secure this data. FDE has traditionally hurt server performance, such that the combination of stringent encryption and strong performance has not been possible until now.

Thankfully, the Dell PowerEdge R815 server powered by the new AMD Opteron 6200 Series processors can handle FDE with only a minimal performance hit. This is because these AMD processors support the Advanced Encryption Standard New Instructions (AES-NI), which improve application speed when using the AES standard to run FDE. You can now secure data on your server's disks while also enjoying good performance.

We confirmed this when we tested an AMD Opteron processor Model 6276-powered Dell PowerEdge R815 server in our labs. Full disk encryption using AES-NI decreased database performance by only 2.1 percent, with a difference of only 2.3 percent processor utilization compared to the same server with no encryption. These results demonstrate the value of a Dell server with an AMD processor that supports AES-NI. You get the best of both worlds: strong performance and secure data protection.

A PRINCIPLED TECHNOLOGIES TEST REPORT
Commissioned by Dell Inc. December 2011

PROTECT YOUR DATA, MAINTAIN SOLID PERFORMANCE

We live in an era of high-profile data breaches. Loss of sensitive company data is an increasingly common occurrence, one that likely gives CEOs everywhere nightmares. Whether due to hacking, as befell Heartland Payment Systems and its customers in 2009,[1] or employee oversight, as was the case with the National Archive and Records Administration in 2009,[2] the threat is one that all companies must combat with vigilance.

There are numerous ways to protect against such data loss. Full disk encryption is a particularly effective method to ensure that unauthorized parties cannot access confidential data on lost or stolen server disks. This high level of security has come with a price: performance impact. Any server disk using FDE has been simultaneously encrypting and decrypting data while running applications, which places a greater strain on the server's disks and processor.

Not anymore! The capability of the latest AMD processors, including the new Opteron processor Model 6276, to run AES-NI greatly improves server performance when using FDE. We found that a Dell PowerEdge R815 server powered with this new AMD processor could deliver FDE in a production database environment with only a minimal performance drop.

We compared database performance of the server in two scenarios: with FDE with AES-NI and without FDE.

Figure 1 shows our results. The AMD Opteron processor Model 6276-powered Dell PowerEdge R815 server performed nearly as well when running FDE as when running without it, with a performance decrease of only 2.1 percent, and an increase in Total Percentage Processor Time (processor utilization) of only 2.3. Higher orders per minute (OPM) and lower processor utilization are better.

In addition to loss of customer confidence, here is another reason to protect against data loss: increasingly stringent regulations.

- **Health Insurance Portability and Accountability Act of 1996 requires the encryption of health data. Penalties include a 10-year prison sentence and $25,000 maximum yearly fine.**
- **The Health Information Technology for Economic and Clinical Health Act of 2009 sets encryption standards for data. The act requires companies to notify the media and government when a breach of unencrypted data occurs.**
- **Sarbanes-Oxley Act enacts strict security guidelines, and defines company best practices. Penalties include a 10-year prison sentence and $15,000,000 maximum fine.**
- **Payment Card Industry Data Security Standard requires encryption of card and account numbers. Penalties include fines up to $500,000.**

[1] http://www.nytimes.com/2009/08/18/technology/18card.html?ref=heartlandpaymentsystemsinc
[2] http://www.scmagazineuk.com/lost-hard-drive-could-affect-70-million-us-military-veterans/article/151478/

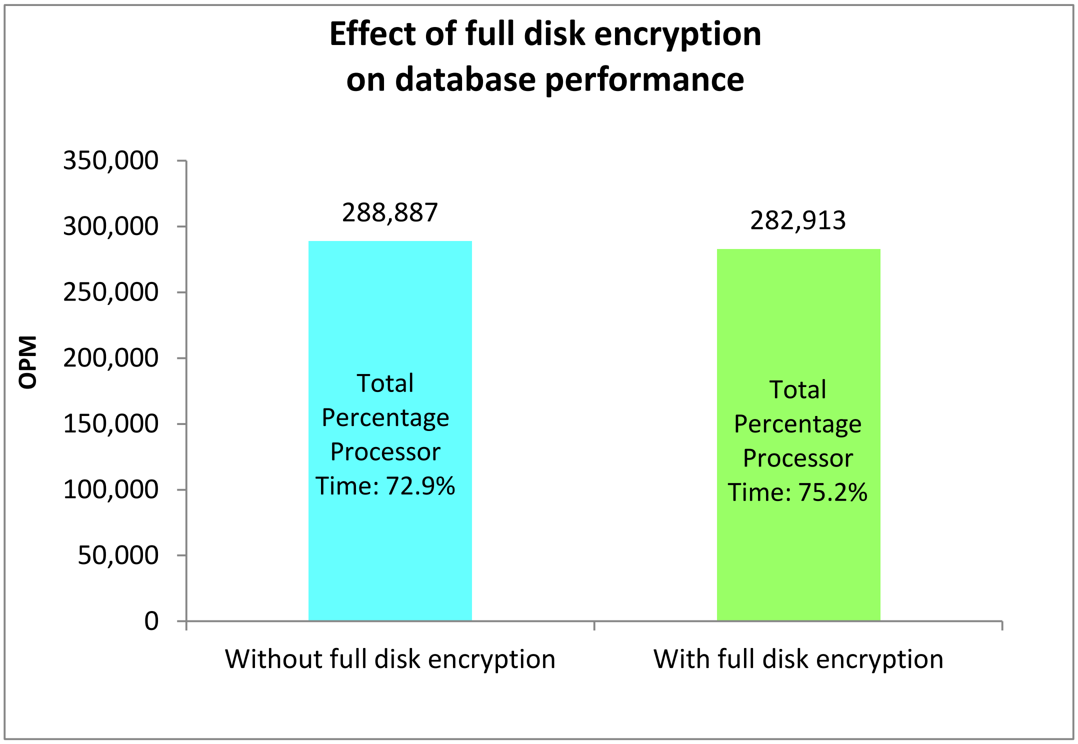


Figure 1: The AMD Opteron processor Model 6276-based Dell PowerEdge R815 database performance with FDE was comparable to that without FDE.

WHAT IS AES-NI, AND HOW DOES IT HELP YOU?

Plaintext
DATA IN PLAINTEXT FORM
Key→
AES-NI
block cipher
encryption
●●☒●☒●●☒●☒●
Ciphertext

AES-NI speeds up AES encryption.

By the mid-1990s, the need for a global encryption standard was increasingly apparent to governments worldwide. In 1996, the US Federal Government began an exhaustive five-year encryption standardization process. Adoption of the Advanced Encryption Standard happened in 2001, and in 2002, the US Federal Government began using it to protect its data.

AES uses an algorithm that employs a symmetric block cipher method to convert data to an unreadable ciphertext; AES then decrypts this ciphertext and converts it into readable plaintext. AES offers a variety of key lengths, the highest of which (192 and 256) are strong enough that the National Security Agency uses them to protect its top-secret data. An additional advantage of AES is that it makes effective use of computing resources, offering high speed with minimal RAM usage.

New instructions improve AES performance

AES-NI is a series of seven new instructions designed to speed up applications that are using AES to carry out encryption and decryption. Specifically, it is an extension to the x86 instruction set architecture for certain newer processors, including the AMD Opteron processor Model 6276.

Each of the seven instructions speeds up the encryption and decryption process by better using the processor’s hardware to execute certain AES algorithms. One instruction accelerates carry-less multiplication, two improve key generation and matrix manipulation, and four improve encryption and decryption.

In addition to speeding up the encryption and decryption process, AES-NI makes servers less vulnerable to attacks that exploit certain types of data stored in AES software, such as memory cache. This is because AES-NI executes its instructions in the hardware.

ADDITIONAL TEST RESULTS

We ran two different tests in our labs. The first was a database test using the DVD Store 2.1 workload, which reports its results in OPM. We tested the disk performance of the AMD Opteron processor Model 6276-based Dell PowerEdge R815 server while it ran a simulated database. In this scenario, we ran each client twice: once running 256-bit full disk encryption using Microsoft® BitLocker® with the help of AES-NI, and once without FDE or BitLocker. Doing so allowed us to determine the impact FDE had on the server's performance. To determine the amount of stress placed on the processor we measured the total percentage processor time. The Total Percentage Processor Time is the sum of all 64 cores during testing.

We present the overall results from this test in Figure 1, and more detailed results in Figure 2. Higher OPM results are better. The average Total Percentage Processor Time shows the average processor utilization during the last 10 minutes of peak performance. Lower processor utilization is better.

DVD Store results		
Client	**Without FDE**	**With FDE (using BitLocker)**
1	37,689	36,783
2	37,369	37,039
3	35,146	34,177
4	37,455	34,344
5	35,250	35,239
6	35,528	33,999
7	34,482	35,970
8	35,968	35,362
Total OPM	**288,887**	**282,913**
Average Total Percentage Processor Time	**72.9%**	**75.2%**

Figure 2: DVD Store results with and without FDE. Higher OPM and lower Total Percentage Processor Time are better.

The second test we ran, the TrueCrypt internal benchmark, measured the encryption performance of the AMD Opteron processor Model 6276-powered Dell PowerEdge R815 with AES-NI and without it. For the "without AES-NI" test, we configured the benchmark to ignore the AES-NI instruction set. We did not encrypt the server's drive with TrueCrypt, but instead used TrueCrypt to test how fast the server's processor could handle encrypting different file sizes. We did so to confirm that the AES-NI instruction speeds up the processor of FDE.

Figure 3 shows the overall throughput results from the TrueCrypt benchmarking test. Higher numbers show better throughput and the ability to encrypt files faster. When using the AES-NI instruction set, the server delivered more than twice the performance—an improvement of 151.3 percent—than when not using AES-NI.

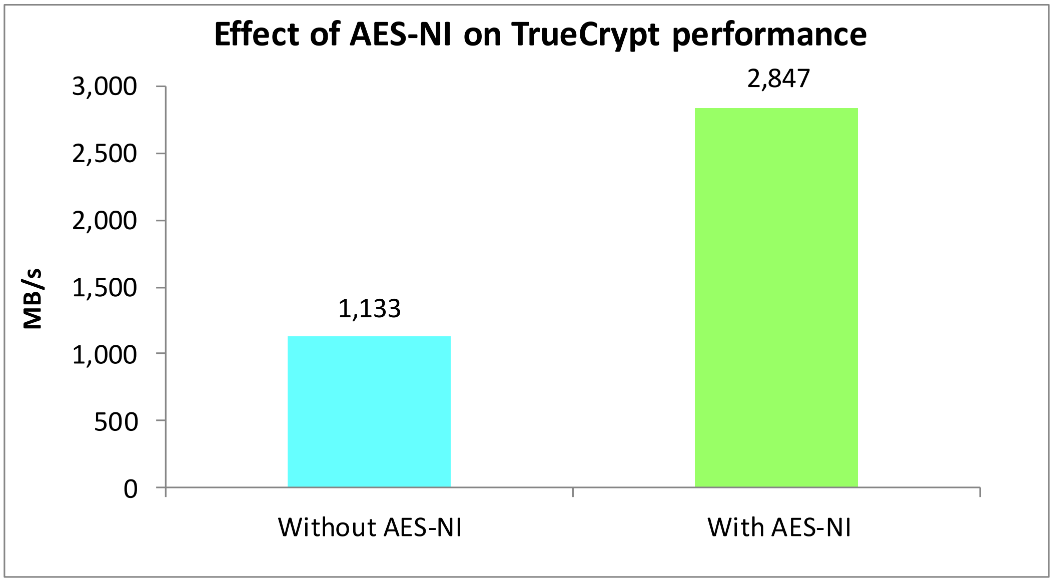


Figure 3: The AMD Opteron processor Model 6276-based Dell PowerEdge R815 delivered superior encryption performance using AES-NI.

Figure 4 shows the median results from the TrueCrypt benchmark tests for different buffer sizes. The results show the mean of both encryption and decryption times. Higher numbers are better.

Median TrueCrypt benchmark results		
	Without AES-NI	With AES-NI
Buffer size	**Results (in MB/s)**	**Results (in MB/s)**
100 KB	209	206
500 KB	302	1,024
1 MB	318	1,229
5 MB	671	1,434
10 MB	1,126	2,355
50 MB	1,843	3,789
100 MB	1,946	4,608
200 MB	1,946	4,608
500 MB	1,331	4,608
1 GB	1,638	4,608
Average MB/s	**1,133**	**2,847**
Percentage improvement with AES-NI		**151.3%**

Figure 4: TrueCrypt benchmark results, in MB/s, with and without AES-NI. Higher numbers are better.

The TrueCrypt benchmark shows the throughput results in MB/s or GB/s. To calculate the results for each system, we converted the GB/s to MB/s. We averaged the results from all buffer sizes to get a comparable result.

We present the test results from each run in Appendix A, our system specs in Appendix B, our test tools in Appendix C, and our test methodology in Appendix D.

FINAL THOUGHTS

Using servers powered by processors that support AES-NI means you no longer need to choose between good performance and robust data protection. A Dell PowerEdge R815 server powered by the AMD Opteron processor Model 6276 delivers strong database performance while protecting your data with full disk encryption.

In our tests, database performance while running FDE with AES-NI was comparable to that without FDE: performance decreased only 2.1 percent and processor utilization increased only 2.3 percent. The results of our TrueCrypt testing confirm that the added throughput using the AES-NI processor instruction set minimizes the impact of FDE on your server's load.

APPENDIX A – COMPLETE TEST RESULTS

Figures 5 and 6 show the DVD Store testing results from each run without FDE and with FDE (using BitLocker). Higher OPM numbers are better.

DVD Store results without FDE			
Client	**Run 1**	**Run 2**	**Run 3**
1	36,004	38,639	37,689
2	35,364	37,548	37,369
3	36,781	36,799	35,146
4	36,692	36,634	37,455
5	34,797	35,836	35,250
6	37,003	35,963	35,528
7	34,930	36,100	34,482
8	34,816	35,621	35,968
Total OPM	**286,387**	**293,140**	**288,887**

Figure 5: DVD Store results without FDE. Higher OPM is better.

DVD Store results with FDE using AES-NI (using BitLocker)			
Client	**Run 1**	**Run 2**	**Run 3**
1	34,854	36,047	36,783
2	34,079	35,384	37,039
3	33,732	34,723	34,177
4	34,146	34,655	34,344
5	34,412	35,314	35,239
6	33,695	36,275	33,999
7	34,410	34,524	35,970
8	35,265	36,004	35,362
Total OPM	**274,593**	**282,926**	**282,913**

Figure 6: DVD Store results with FDE (using BitLocker). Higher OPM is better.

Figures 7 through 9 show the results from each run using the TrueCrypt benchmark, both with AES-NI and without AES-NI. Higher numbers are better. In the body of this report, we present the median of the three runs.

Run 1 results running TrueCrypt processor encryption						
	Encryption		**Decryption**		**Mean**	
Buffer size	**Without AES-NI**	**With AES-NI**	**Without AES-NI**	**With AES-NI**	**Without AES-NI**	**With AES-NI**
100 KB	209 MB/s	204 MB/s	208 MB/s	207 MB/s	208 MB/s	206 MB/s
500 KB	280 MB/s	1.0 GB/s	297 MB/s	1.0 GB/s	288 MB/s	1.0 GB/s
1 MB	310 MB/s	1.2 GB/s	326 MB/s	1.2 GB/s	318 MB/s	1.2 GB/s
5 MB	688 MB/s	1.4 GB/s	655 MB/s	1.4 GB/s	671 MB/s	1.4 GB/s
10 MB	1.1 GB/s	2.0 GB/s	1.2 GB/s	1.7 GB/s	1.2 GB/s	1.9 GB/s
50 MB	1.7 GB/s	3.7 GB/s	1.8 GB/s	3.7 GB/s	1.8 GB/s	3.7 GB/s
100 MB	1.9 GB/s	4.1 GB/s	2.0 GB/s	4.0 GB/s	1.9 GB/s	4.1 GB/s
200 MB	1.9 GB/s	4.2 GB/s	2.0 GB/s	4.2 GB/s	1.9 GB/s	4.2 GB/s

Run 1 results running TrueCrypt processor encryption						
	Encryption		Decryption		Mean	
Buffer size	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI
500 MB	1.3 GB/s	4.1 GB/s	1.4 GB/s	4.1 GB/s	1.3 GB/s	4.1 GB/s
1 GB	1.6 GB/s	4.2 GB/s	1.6 GB/s	4.2 GB/s	1.6 GB/s	4.2 GB/s

Figure 7: TrueCrypt results with and without AES-NI. Higher numbers are better.

Run 2 results running TrueCrypt processor encryption						
	Encryption		Decryption		Mean	
Buffer size	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI
100 KB	198 MB/s	224 MB/s	220 MB/s	170 MB/s	209 MB/s	197 MB/s
500 KB	296 MB/s	1,012 MB/s	307 MB/s	1,008 MB/s	302 MB/s	1,010 MB/s
1 MB	311 MB/s	1.2 GB/s	326 MB/s	1.2 GB/s	318 MB/s	1.2 GB/s
5 MB	659 MB/s	1.4 GB/s	672 MB/s	1.4 GB/s	665 MB/s	1.4 GB/s
10 MB	1.1 GB/s	2.3 GB/s	1.2 GB/s	2.3 GB/s	1.1 GB/s	2.3 GB/s
50 MB	1.7 GB/s	4.3 GB/s	1.8 GB/s	4.6 GB/s	1.8 GB/s	4.4 GB/s
100 MB	1.9 GB/s	4.6 GB/s	2.0 GB/s	4.9 GB/s	1.9 GB/s	4.7 GB/s
200 MB	1.9 GB/s	4.5 GB/s	2.0 GB/s	4.5 GB/s	2.0 GB/s	4.5 GB/s
500 MB	1.3 GB/s	4.5 GB/s	1.3 GB/s	4.6 GB/s	1.3 GB/s	4.5 GB/s
1 GB	1.6 GB/s	4.5 GB/s	1.6 GB/s	4.6 GB/s	1.6 GB/s	4.5 GB/s

Figure 8: TrueCrypt results with and without AES-NI. Higher numbers are better.

Run 3 results running TrueCrypt processor encryption						
	Encryption		Decryption		Mean	
Buffer size	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI	Without AES-NI	With AES-NI
100 KB	215 MB/s	222 MB/s	220 MB/s	222 MB/s	218 MB/s	222 MB/s
500 KB	295 MB/s	1.0 GB/s	309 MB/s	1.0 GB/s	302 MB/s	1.0 GB/s
1 MB	535 MB/s	1.2 GB/s	549 MB/s	1.2 GB/s	542 MB/s	1.2 GB/s
5 MB	673 MB/s	2.2 GB/s	700 MB/s	2.2 GB/s	687 MB/s	2.2 GB/s
10 MB	1.1 GB/s	2.6 GB/s	1.2 GB/s	2.4 GB/s	1.1 GB/s	2.5 GB/s
50 MB	1.4 GB/s	3.7 GB/s	1.5 GB/s	3.7 GB/s	1.4 GB/s	3.7 GB/s
100 MB	1.6 GB/s	4.5 GB/s	1.3 GB/s	4.6 GB/s	1.4 GB/s	4.5 GB/s
200 MB	1.3 GB/s	4.5 GB/s	1.4 GB/s	4.5 GB/s	1.4 GB/s	4.5 GB/s
500 MB	1.3 GB/s	4.6 GB/s	1.3 GB/s	4.6 GB/s	1.3 GB/s	4.6 GB/s
1 GB	1.4 GB/s	4.5 GB/s	1.6 GB/s	4.6 GB/s	1.5 GB/s	4.6 GB/s

Figure 9: TrueCrypt results with and without AES-NI. Higher numbers are better.

APPENDIX B – SERVER CONFIGURATION INFORMATION

Figure 10 provides detailed configuration information about the Dell PowerEdge R815 servers we used for testing.

System	Dell PowerEdge R815
Power supplies	
Total number	2
Vendor and model number	Dell L1100A-S0
Wattage of each (W)	1,100
Cooling fans	
Total number	6
Vendor and model number	San Ace 60 9GA0612P1K611
Dimensions (h x w) of each	2-3/8” x 2-1/2”
Volts	12
Amps	0.95
General	
Number of processor packages	4
Number of cores per processor	16
Number of hardware threads per core	1
System power management policy	Balanced
CPU	
Vendor	AMD
Name	Opteron
Model number	6276
Stepping	B2
Socket type	Socket G34
Core frequency (GHz)	2.30
Bus frequency (MT/s)	6.4
L1 cache	48 KB (per core)
L2 cache (KB)	1,000 (per core)
L3 cache (MB)	16
Platform	
Vendor and model number	Dell PowerEdge R815
Motherboard model number	Dell Inc. 06JC9T
Motherboard chipset	AMD SR5650
BIOS name and version	Dell Inc. 2.3.0 (10/18/2011)
BIOS settings	Default
Memory module(s)	
Total RAM in system (GB)	128
Vendor and model number	Samsung M393B1K70BH1-CH9
Type	PC3-10600R
Speed (MHz)	1,333
Speed running in the system (MHz)	1,333
Size (GB)	8

System	**Dell PowerEdge R815**
Number of RAM module(s)	16 x 8 GB
Chip organization	Double-sided
Rank	Dual
Hard disk	
Hard disk type 1	
Vendor and model number	Dell ST9146852SS
Number of disks in system	2
Size (GB)	146
Buffer size (MB)	16
RPM	15,000
Type	6Gb/s SAS
Hard disk type 2	
Vendor and model number	Pliant LB 150S
Number of disks in system	4
Size (GB)	150
Buffer size (MB)	N/A
RPM	N/A
Type	SAS
Disk Controller	
Vendor and model	Dell PERC H700 Integrated
Controller cache (MB)	512
Controller driver	Dell 4.31.1.64 (08/09/2010)
Controller firmware	12.10.1-0001
RAID configuration	RAID 0
Operating system	
Name	Windows Server® 2008 R2 Enterprise
Build number	7601
Service pack	1
File system	NTFS
Kernel	ACPI x64-based PC
Language	English
Graphics	
Vendor and model number	Matrox® G200eW
Graphics memory (MB)	8
Driver	Microsoft 6.1.7600.16385 (06/21/2006)
Ethernet	
Vendor and model number	Broadcom® BCM5709C NetXtreme® II GigE
Type	Integrated
Driver	Broadcom 6.2.9.0 (02/04/2011)

System	Dell PowerEdge R815
Optical drive(s)	
Vendor and model number	TEAC DV-28SW
Type	DVD-ROM
USB ports	
Number	6
Type	2.0

Figure 10: Configuration information for the AMD processor-based Dell server.

APPENDIX C – THE TEST TOOLS WE USED

In this section, we discuss the tools we used in our tests.

DVD Store

To build the workload, we used DVD Store Version 2.1 (DS2), an open-source simulation of an online e-commerce DVD store. DS2 has database components and Web server components, and includes driver programs that place heavy loads on these components. A new feature of DVD Store Version 2.1 uses the ability to target multiple databases from one source client. We used this functionality in order to record the orders per minute output from each specific database target.

The goal of this test was to show the advantage of the AMD Opteron processor Model 6276's AES-NI instruction with FDE. Therefore, we needed to ensure the test database did not become cached in memory, requiring constant reads and writes to the hard drives to give maximum encryption activity.

The Dell PowerEdge R815 server ran four Microsoft SQL Server® 2008 R2 instances, with two databases per instance to ensure that the database load was greater than the 128 GB of system memory. We configured each SQL Server 2008 R2 instance database with two 20GB databases.

The main DS2 metric is orders per minute, which the driver program calculates and records to a text file on the client machines. The DVD Store client application outputs OPM at 10-second intervals. We ran this workload on the server for 30 minutes and report the last OPM score the benchmark reported.

A DS2 order consists of a customer login; a search for movies by title, actor, or category; and a purchase. The workload also performs other actions, such as adding new customers, to exercise a wide range of database functions.

As we note above, because our goal was to isolate and test database server performance, we did not use the front-end Web client component of DS2. Instead, we ran a compiled driver on client machines directly via its command-line interface. We used the default DS2 parameters and setup configuration, with the exceptions we note in the Setting up DVD Store version 2.1 sections in the detailed test methodology in Appendix D.

Each client machine ran two instances of DS2, with 16 threads each to simulate a heavily loaded environment; the load-generating client machines ran with no think time, processing requests as quickly as the servers were able.

For more details about the DS2 tool, see http://www.delltechcenter.com/page/DVD+Store.

BitLocker

Microsoft includes BitLocker full disk Drive Encryption with the following operating systems: Ultimate and Enterprise editions of Windows Vista® and Windows 7, and Windows Server 2008 and Windows Server 2008 R2. BitLocker uses 128-bit or 256-bit key AES encryptions, and allows you to easily and transparently encrypt entire volumes, either on a single drive or across multiple drives, and to encrypt removable drives. BitLocker automatically encrypts any new files you add to a drive (or drives), and checks the drive(s) for security threats each time you start up the computer. Note that BitLocker locks down the drive if it detects a security hazard, and you must then use a recovery key in gain access to your data. Like all FDE methods, BitLocker exacts a performance hit on any drive that uses it. We used 256-bit AES encryption for testing.

To learn more about BitLocker, visit http://windows.microsoft.com/en-US/windows7/products/features/bitlocker.

TrueCrypt

TrueCrypt is a free, open-source disk encryption program. It supports the following operating systems: Windows (XP, Vista, and 7), Mac OS® X, and Linux. TrueCrypt enables “on-the-fly” encryption, which means that it automatically encrypts data just before it is saved and then decrypts it just after it is loaded, so that there is no need for the user to handle this manually. Additionally, TrueCrypt can encrypt an entire partition or storage device (i.e., USB flash drive), can encrypt at the pre-boot authentication level (i.e., a partition or drive where Windows is installed), and can create a virtual encrypted disk inside a file that it then mounts as a real disk. TrueCrypt also allows for parallelization and pipelining, which it claims allows data to be read and written as fast as it would be if the drive were not encrypted. TrueCrypt includes a benchmark to test the encryption speed of your system’s processor and memory. We used this included benchmark for our testing.

To learn more about TrueCrypt, visit http://www.truecrypt.org/.

APPENDIX D – DETAILED TEST METHODOLOGY

Here, we explain the detailed steps we followed to set up our test scenario.

Setting up the servers for DVD Store

Our DVD Store test bed consisted of a Dell PowerEdge R815 as the server under test and four Dell PowerEdge 1850 servers as clients. Each Dell PowerEdge 1850 had two processors, 2 GB of system memory, and a Gigabit network card in default configurations. We connected the systems via one Gigabit network switch.

We configured two internal SAS hard drives as RAID 0 arrays for the operating system and SQL Server 2008 R2 installations on the Dell PowerEdge R815. We installed a fresh copy of Windows Server 2008 R2 Enterprise Edition on the server.

Installing Windows Server 2008 R2 Enterprise Edition

1. Boot the server, and insert the Windows Server 2008 R2 installation DVD in the DVD-ROM drive.
2. At the Language Selection screen, click Next.
3. Click Install Now.
4. Select Windows Server 2008 R2 Enterprise (Full Installation), and click Next.
5. Click the I accept the license terms check box, and click Next.
6. Click Custom.
7. At the Where to Install Windows screen, click Drive options (advanced).
8. Ensure you select the proper drive, and click New.
9. Enter the partition size, and click Apply. (We used the entire disk.)
10. At the pop-up informing you Windows will create additional partitions, click OK.
11. At the Where to Install Windows screen, click Next.
12. At the User's password must be changed before logging on warning screen, click OK.
13. Enter a password as the new password in both fields, and click the arrow to continue.
14. At the Your password has been changed screen, click OK.

Setting up the network configuration on the server

1. Click Start→Control Panel→Network and Internet→Network and Sharing Center, and click Change Adapter Settings.
2. Right-click on the network adapter, and select Properties from the drop-down menu.
3. Select Internet Protocol Version 4 (TCP/IPv4), and click Properties.
4. At the Internet Protocol Version 4 (TCP/IPv4) Properties screen, select the Use the following IP address radio button.
5. Enter a valid static IP address, subnet mask, and default gateway.
6. Click OK to close the window.
7. At the Local Area Connection Properties window, click Close.
8. Close the Network Connection window.

Installing system updates in Windows Server 2008 R2

We installed all critical updates as of 11/21/2011 on the server using the Windows Update feature.

Installing SQL Server 2008 R2 on the server

1. Insert the installation DVD for SQL Server 2008 R2 into the DVD drive.
2. If Autoplay does not begin the installation, navigate to the SQL Server 2008 DVD, and double-click.
3. If prompted with a .NET installation prompt, click OK to enable the .NET Framework Core role.
4. At the SQL Server Installation Center screen, click Installation.

5. Click New installation or add features to an existing installation.
6. At the Setup Support Rules screen, click OK.
7. At the Product Key screen, specify the free Enterprise Edition evaluation, and click Next.
8. At the License Terms screen, accept the license terms, and click Next.
9. At the Setup Support Files screen, click Install.
10. At the Setup Support Rules screen, click Next.
11. At the Setup Role screen, choose SQL Server Feature Installation, and click Next.
12. At the SQL Server 2008 R2 Feature Selection screen, select the following features: Database Engine Services, Full-Text Search, Client Tools Connectivity, Client Tools Backwards Compatibility, Management Tools – Basic, Management Tools – Complete; and click Next.
13. At the Installation Rules screen, click Next.
14. At the Instance Configuration screen, leave the defaults, and click Next.
15. At the Disk Space Requirements screen, click Next.
16. At the Server Configuration screen, change SQL Server Agent and SQL Server Database Engine to NT AUTHORITY\SYSTEM, and click Next.
17. At the Database Engine Configuration screen, select Mixed Mode, fill in a password for the system administrator (sa) account, click Add Current User, and click Next.
18. At the Error Reporting screen, click Next.
19. At the Installation Configuration Rules screen, click Next.
20. At the Installation screen, click Install.
21. At the Complete screen, click Close.
22. Important: Repeat the installation process three more times to create four total instances of SQL Server 2008 R2.
23. Install SQL Server 2008 R2 Service Pack 1, and patch all instances.

Configuring SQL Server 2008 R2

After installing SQL Server 2008 R2, we enabled the SQL Server Browser and TCP/IP. We followed this process for these configurations:

1. Click Start→Administrative Tools→Services.
2. In the right-hand pane, right-click SQL Server Browser, and select Properties from the drop-down menu.
3. At the Startup type drop-down menu, select Automatic, and click OK.
4. Close the Services window.
5. Click Start→All Programs→Microsoft SQL Server 2008 R2→Configuration Tools→SQL Server Configuration Manager.
6. Select SQL Server Services in the left pane.
7. In the right pane, right-click SQL Server Browser, and select Start from the drop-down menu.
8. In the left pane, expand SQL Server Network Configuration, and select Protocols for MSSQLSERVER (where MSSQLSERVER is the name of the first SQL Server instance).
9. In the right pane, right-click TCP/IP, and select Enable from the drop-down menu.
10. Repeat Step 9 for the remaining three SQL Server instances.
11. In the left pane, select SQL Server Services.
12. In the right pane, right-click SQL Server (MSSQLSERVER), and select Restart from the drop-down menu.
13. Repeat step 12 for the remaining three SQL Server instances.

Installing and configuring the database clients

For the DS2 scripts, we used four Dell PowerEdge 1850 servers as clients to simulate a number of users putting a load on the server. Each server had a single drive on which we installed a fresh copy of Windows Server 2003 R2 Enterprise Edition. We installed the .NET 3.5 SP1 framework on each client, as the DS2 test executable requires at least

.NET2.0. After the installation, we created two folders on the server, one for each client instance, to store the DS2 executable. We followed this process for each installation:

1. Install Microsoft Windows Server 2003 R2 Enterprise x86 Edition with Service Pack 2 on the client.
2. Assign a computer name of `Clientx` for the database client, where x is the client number.
3. For the licensing mode, use the default setting of five concurrent connections.
4. Enter a password for the administrator logon.
5. Select Eastern Time Zone.
6. Use typical settings for the Network installation.
7. Type `Workgroup` for the workgroup.
8. Install Windows Updates, .NET 3.5 SP1 framework, and copy the DVD Store client executable into each of the two folders.

Creating scripts on the database clients

To simplify testing, we created batch files named test.bat on all four Dell PowerEdge 1850 clients to start the DVD Store executable with the correct parameters. We put the batch files in two folders on the clients: c:\clientshare and c:\clientshare2. The batch files in c:\clientshare contained the text below. The batch files in C:\clientshare2 contained the same text, but the driver and output file pointed to the different directory and had `–database_name=ds2-1`.

```
c:\clientshare\ds2sqlserverdriver.exe --target=192.168.0.100 --ramp_rate=10 --
run_time=30 --n_threads=16 --db_size=20GB --think_time=0 --database_name=ds2 --
detailed_view=Y --warmup_time=1 --pct_newcustomers=5 --
output_path=c:\clientshare\opmoutds2.txt
```

Setting up DVD Store version 2.1

Data generation overview

We generated the data using the Install.pl script included with DVD Store version 2.1, providing the parameters for our 20GB database size and the database platform on which we ran - Microsoft SQL Server. 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 2008 R2 SP1. We built the 20GB database in SQL Server 2008 R2 SP1, and then performed a full backup, storing the backup file on the C: drive for quick access. We used that backup file to restore on the server between test runs.

The only modification we made to the schema creation scripts were the specified file sizes for our database. We deliberately 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, the database schema was created and loaded 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. We created indices, full-text catalogs, primary keys, and foreign keys using the database-creation scripts.
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 (TSQL) 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. We created the necessary full text index using SQL Server Management Studio.
11. We created a database user and mapped this user to the SQL Server login.
12. We then performed a full backup of the database. This backup allowed us to restore the databases to a pristine state relatively quickly between tests.
    Figure 11 shows our initial file size modifications.

Logical name	Filegroup	Initial size (MB)
Database files		
primary	PRIMARY	3
cust1	DS_CUST_FG	2,168
cust2	DS_CUST_FG	2,168
cust3	DS_CUST_FG	2,168
cust4	DS_CUST_FG	2,168
cust5	DS_CUST_FG	2,168
cust6	DS_CUST_FG	2,168
cust7	DS_CUST_FG	2,168
cust8	DS_CUST_FG	2,168
ind1	DS_IND_FG	1,280
ind2	DS_IND_FG	1,280
ind3	DS_IND_FG	1,280
ind4	DS_IND_FG	1,280
ind5	DS_IND_FG	1,280
ind6	DS_IND_FG	1,280
ind7	DS_IND_FG	1,280
ind8	DS_IND_FG	1,280
ds_misc1	DS_MISC_FG	256
ds_misc2	DS_MISC_FG	256

Logical name	Filegroup	Initial size (MB)
ds_misc3	DS_MISC_FG	256
ds_misc4	DS_MISC_FG	256
ds_misc5	DS_MISC_FG	256
ds_misc6	DS_MISC_FG	256
ds_misc7	DS_MISC_FG	256
ds_misc8	DS_MISC_FG	256
orders1	DS_ORDERS	1,536
orders2	DS_ORDERS	1,536
orders3	DS_ORDERS	1,536
orders4	DS_ORDERS	1,536
orders5	DS_ORDERS	1,536
orders6	DS_ORDERS	1,536
orders7	DS_ORDERS	1,536
orders8	DS_ORDERS	1,536
Log files		
ds_log	Not Applicable	20,480

Figure 11. Our initial file size modifications.

Editing the workload script – ds2xdriver.cs module

A new feature of DVD Store version 2.1 is the ability to target multiple targets from one source client. We used this functionality. In order to record the orders per minute output from each specific database target, we modified the ds2xdriver to output this information to log files on each client system. To do this, we used the StreamWriter method to create a new text file on the client system, and the WriteLine and Flush methods to write the relevant outputs to the files during the tests. We also added the capabilities to target differently named databases.

After making these changes, we recompiled the ds2xdriver.cs and ds2sqlserverfns.cs module in Windows by following the instructions in the DVD Store documentation. Because the DS2 instructions were for compiling from the command line, we used the following steps on a system with Visual Studio installed:

1. Open a command prompt.
2. Use the `cd` command to change to the directory containing our sources.
3. Execute the following command:

```
csc /out:ds2sqlserverdriver.exe ds2xdriver.cs ds2sqlserverfns.cs
/d:USE_WIN32_TIMER /d:GEN_PERF_CTRS
```

Setting up disk drives for the database

We installed four Pliant LB 150S SSD drives in the Dell PowerEdge R815 server for the database and log files. We configured the drives in 2 two-disk RAID 0 volumes and named them volume1 (E:) and volume2 (F:). We put the database and logs on different volumes. For example, the database 1 files were on volume1 and the log files were on volume2. We reversed this for the next database, so database 2 files were on volume2 and the log files were on volume1. We repeated these steps for the remaining database instances. This setup ensured equal disk activity on both RAID volumes.

Setting up Windows BitLocker AES 256-bit encryption

By default, Windows uses AES 128-bit with diffuser for its encryption cipher. We used 256-bit encryption for testing. To change to 256-bit, we completed the following steps:

1. Click Start→Run, and type `MMC`
2. Select File menu→Add/remove snap-ins.
3. Select Group policy object→Local computer, and click Finish.
4. Click OK to close the snap-in editor.
5. Expand the left pane: Local computer policy→Computer configuration→Administrative templates→Windows components→BitLocker drive encryption.
6. Select Choose drive encryption method and cipher strength.
7. Enable the setting and select AES 256-bit, and click OK.
8. Close the group policy editor (when BitLocker is turned on later, all encryption will be AES 256).

Enabling BitLocker

1. Click Start→Administrative Tools→Server Manager.
2. In the left pane, click Features.
3. In the right pane, click Add Features.
4. At the Add Features Wizard, select BitLocker Drive Encryption, and click Next.
5. At the Confirm Installation Selections screen, click Install.
6. At the Installation Results screen, click Close to finish the installation and restart the server.
7. At the Do you want to restart now? pop-up, click Yes.
8. After the server reboots, at the Installation Results screen, click Close.

Testing procedure

To perform the DVD Store tests use the following steps:

1. Boot the Dell PowerEdge R815 server and all clients.
2. On the Dell PowerEdge R815, ensure all SQL Server instances are running.
3. On each client, open a command prompt, and change directory to C:\clientshare. (Repeat this step to open a second command prompt window for C:\clientshare2 batch file.)
4. Type `test.bat` in each command prompt (Note: Do not press Enter to start the benchmark until all systems are ready.)
5. Once all clients are ready, wait for 10 minutes to ensure the server under test is idle.
6. Start the perfmon counters on the Dell PowerEdge R815.
   (Note: To measure processor utilization, we used the Total % Processor Time counter. To measure disk utilization, we used the % Idle counter.)
7. Press Enter on each of the client command prompt windows to begin the test. (Note: We staggered the clients by waiting 15 seconds between each one)
8. After the test finishes, stop perfmon and copy off all output files from the clients.
9. Restore all databases on the server under test. (To simplify testing, we created restore scripts for all databases.)
10. Reboot the server and test clients.
    Repeat steps 2 through 10 for the additional runs. (Note: We encrypted and decrypted the hard drives between each run when doing FDE testing. We decrypted the drives, restored the database, and then encrypted the drives each time.)

Encrypting server drives

We encrypted the two database volumes for testing. We did not encrypt the volume holding the operating system. Encrypting the drives takes a while, so we only encrypted database volumes to simplify and speed up testing. All activity is on the database volumes during testing, so this procedure did not alter results in any way. Use the following steps to encrypt the drives:

1. Start→Control Panel→System and Security→Manage BitLocker→Turn on all BitLocker for the system drive.
2. When prompted to start BitLocker, select Yes.
3. At the Choose how you want to unlock this drive window, select Use a password to unlock the drive.
4. Enter a password, and click Next.
5. At the How do you want to store your recovery key screen, select Save the recovery key to a file.
6. At the pop-up, navigate to a folder on the C:, and click Save.
7. At the pop-up asking if you want to store the key on this computer, click Yes.
8. At the How do you want to save your recovery key, click Next.
9. At the Are you ready to encrypt this drive screen, click Start Encrypting.
10. Repeat steps 1 through 9 for the second database disk volume.
11. Ensure that you encrypt all drives before beginning the test.

Decrypting server drives

After the DVD Store test is finished, we decrypted the drives before restoring the database. This insured consistent results for testing by starting with the same database and encryption each time.

1. Start→Control Panel→System and Security→Manage BitLocker.
2. Turn off BitLocker for all drives.

Setting up the server for TrueCrypt

The TrueCrypt benchmark runs on the server under test, so we did not use any clients for this testing. We began setting up the Dell PowerEdge R815 by installing a fresh copy of Windows Server 2008 R2 as outlined in the Installing Windows Server 2008 R2 Enterprise Edition section. We configured two internal SAS hard drives as RAID 0 arrays for the operating system.

Installing TrueCrypt 7.1

We downloaded TrueCrypt 7.1 from http://www.truecrypt.org/downloads. We completed the following steps for installation:

1. Double-click installation executable to begin the installation.
2. At the Please read the license terms screen, accept the license agreement, and click Next.
3. At the Wizard Mode screen, select Install, and click Next.
4. At the Setup Options screen, keep the default, and click Install.
5. At the TrueCrypt has been successfully updated screen, click Finish.

Running TrueCrypt 7.1

The TrueCrypt benchmark runs the test in memory. It does not require disk encryption, so we did not encrypt the server's hard drives for testing. We used the following steps for testing:

1. Double-click the TrueCrypt desktop shortcut.
2. Select Settings→Performance.
3. At the Performance Options screen, click Benchmark. (Note: We checked and unchecked the Accelerate AES encryption/decryption by using the AES instructions of the processor to enable or disable the AES hardware accelerator for testing.)
4. At the Encryption Algorithm Benchmark screen, select the correct buffer size, and click Benchmark.
5. The results are shown in the same window after the benchmark finishes. We recorded those numbers in the Test results section and in Appendix A of this report.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

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.